Vilniaus universiteto Teisės fakulteto
Viešosios teisės katedra

Gabrielės Radžiūtės,
V kurso, Tarptautinės ir ES teisės
studijų šakos studentės

Magistro darbas

ES Bendrasis duomenų apsaugos reglamentas kaip duomenų apsaugos teisės šaltinis

Vadovas: lekt. dr. Julius Zaleskis

Recenzentė: doc. dr. Indrė Žvaigždinienė

Vilnius

2018

TURINYS

ĮVADAS 3
1. DUOMENŲ APSAUGOS TEISĖ IR JOS REFORMA ES 6
1.1. Duomenų apsaugos teisės samprata ir turinys 6
1.2. Duomenų apsaugos teisės šaltiniai 9
1.3. Duomenų apsaugos teisės reforma ES 14
1.3.1. Poreikio reformai priežastys 15
1.3.2. Reformos tikslai ir priemonės 17
2. BENDRASIS DUOMENŲ APSAUGOS REGLAMENTAS IR JUO ĮGYVENDINAMOS NAUJOVĖS 20
2.1. Reglamento turinys 20
2.2. Duomenų subjekto teisių naujovės 22
2.2.1. Teisė reikalauti ištrinti duomenis (teisė būti pamirštam) 25
2.2.2. Teisė apriboti duomenų tvarkymą 33
2.2.3. Teisė į duomenų perkeliamumą 36
2.3. Pranešimas apie asmens duomenų saugumo pažeidimą 43
2.4. Poveikio duomenų apsaugai vertinimas 45
2.5. Duomenų apsaugos pareigūnas 48
2.5.1. Dabartinis duomenų apsaugos pareigūno reglamentavimas 48
2.5.2. Duomenų apsaugos pareigūno skyrimo pagrindai 50
2.5.3. Duomenų apsaugos pareigūno veiklos principai 53
3. BENDROJO DUOMENŲ APSAUGOS REGLAMENTO VIETA TEISĖS ŠALTINIŲ SISTEMOJE 57
3.1. Valstybėms narėms suteikiama diskrecijos teisė 57
3.2. Reglamentas ir LR duomenų apsaugos įstatymo pakeitimo projektas 59
3.3. Reglamentas ir LR darbo kodeksas 63
3.4. Reglamentas ir 29 straipsnio darbo grupės šaltiniai 66
IŠVADOS 68
LITERATŪROS IR KITŲ ŠALTINIŲ SĄRAŠAS 70
SANTRAUKA 78
SUMMARY 79

ĮVADAS

Duomenų apsauga įgyja vis didesnę svarbą. Teisė į duomenų apsaugą nustatoma Europos Sąjungos pagrindinių teisių chartijoje. Taip pat tai yra viena iš teisių, saugomų kaip Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencijoje įtvirtintos teisės į privatų gyvenimą dalis. Lietuvoje duomenų apsaugą reguliuoja Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas, o Europos Sąjungos lygmeniu duomenų apsauga vis dar yra reglamentuojama 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyvoje 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo (Duomenų apsaugos direktyva). Tačiau nuo šios direktyvos priėmimo praėjo daugiau nei 20 metų, per kuriuos įvyko daugybė pokyčių.

Teisė taip pat turi prisiderinti prie visuomenėje vykstančių pokyčių. Dėl šios priežasties Europos Sąjungoje vyksta duomenų apsaugos teisinio reguliavimo reforma – 2018 m. gegužės 25 d. bus pradėtas taikyti 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). Šis reglamentas bus taikomas tiesiogiai ir taps pagrindiniu duomenų apsaugos teisės šaltiniu visose Europos Sąjungos valstybėse narėse, tarp jų ir Lietuvoje. Todėl šiame darbe bus analizuojamos Bendrojo duomenų apsaugos reglamento naujovės, jų reikšmė duomenų apsaugos teisei bei santykis su kitais duomenų apsaugos teisės šaltiniais.

Temos aktualumas. Šis darbas yra aktualus tuo, jog jame nagrinėjamas naujas Europos Sąjungos teisės aktas – Bendrasis duomenų apsaugos reglamentas, kuris dar tik bus pradėtas taikyti 2018 m. gegužės 25 d. ir taps pagrindiniu duomenų apsaugos teisės šaltiniu Europos Sąjungos mastu. Darbe ypatingai didelis dėmesys skiriamas duomenų subjekto teisėms dėl jų svarbos kiekvienam iš mūsų. Taip pat išsamiai nagrinėjamas duomenų apsaugos pareigūno institutas kaip ypač svarbi duomenų apsaugos teisinio reguliavimo dalis. Dėl šių priežasčių darbas aktualus tiek teoriškai, tiek ir praktiškai.

Tyrimo objektas. Šiame darbe nagrinėjamas Bendrasis duomenų apsaugos reglamentas ir juo įtvirtinamos teisinio reguliavimo naujovės bei duomenų apsaugos teisės šaltinių sistema.

Darbo tikslas. Atskleisti Bendrojo duomenų apsaugos reglamento reikšmę ir įtaką duomenų apsaugos teisei bei nustatyti jo vietą duomenų apsaugos teisės šaltinių sistemoje.

Uždaviniai:

1) išanalizuoti asmens duomenų sampratą;
2) apžvelgti dabartinę duomenų apsaugos teisės sistemą;
3) išsiaiškinti poreikį duomenų apsaugos teisės reformai ES;
4) ištirti pagrindinius naujojo duomenų apsaugos teisinio reguliavimo pokyčius ES bei išanalizuoti jų svarbą ir taikymo ypatumus;
5) atskleisti Bendrojo duomenų apsaugos reglamento santykį su kitais duomenų apsaugos teisės šaltiniais.

Tyrimo metodai. Šiame darbe pagrindiniai naudojami tyrimo metodai yra lyginamasis, sisteminis ir kritinės analizės. Lyginamasis metodas naudojamas lyginant dabartinį duomenų apsaugos teisinį reguliavimą, įtvirtintą Duomenų apsaugos direktyvoje ir ją įgyvendinančiame Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatyme, su naujuoju teisiniu reguliavimu, įtvirtintu Bendrajame duomenų apsaugos reglamente. Sisteminis metodas naudojamas nagrinėjant naujojo teisinio reguliavimo normas kaip sistemą, išskiriant svarbiausius aspektus ir pateikiant apibendrinančias išvadas bei atskleidžiant Bendrąjį duomenų apsaugos reglamentą kaip duomenų apsaugos teisės šaltinių sistemos dalį. Kritinės analizės metodas naudojamas analizuojant naujojo duomenų apsaugos teisinio reguliavimo ypatumus, jų naudą bei galimus įgyvendinimo iššūkius. Taip pat naudojami lingvistinis ir teleologinis metodai aiškinantis pagrindines darbo sąvokas.

Darbo originalumas. Teisės doktrinoje Bendrasis duomenų apsaugos reglamentas nagrinėtas mažai. Christina Tikkinen-Piri, Anna Rohunen ir Jouni Markkula bendrai apžvelgė naujojo reguliavimo pokyčius[1]. Kiti užsienio autoriai tyrė pavienius Bendrojo duomenų apsaugos reglamento aspektus, nedarydami sisteminės analizės. Lietuvoje duomenų apsaugą pagal dabartinį teisinį reguliavimą nagrinėjo Ilona Petraitytė[2], Mindaugas Kiškis[3] ir kiti autoriai. Tačiau Bendrasis duomenų apsaugos reglamentas nebuvo plačiai nagrinėtas. Julius Zaleskis analizavo svarbiausias Bendrojo duomenų apsaugos reglamento naujoves[4] bei nagrinėjo duomenų apsaugos pareigūno veiklos

[1] TIKKINEN-PIRI, Christina; ROHUNEN, Anna; MARKKULA, Jouni. EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law and Security Review*, 2018, t. 34, p. 150. 134-153.
[2] PETRAITYTĖ, Ilona. Asmens duomenų apsauga ir teisė į privatų gyvenimą. *Teisė*, 2011, t. 80, p. 163-174. PETRAITYTĖ, Ilona. Asmens duomenų apsaugos teisinis reguliavimas Lietuvos teisės sistemoje. *Teisė*, 2011, t. 79, p. 125-138. PETRAITYTĖ, Ilona. *Asmens duomenų teisinės apsaugos principai*: daktaro disertacija. Socialiniai mokslai, teisė (01S). Vilnius: Vilniaus universitetas, 2013.
[3] KIŠKIS, Mindaugas. *Data Protection in Lithuania // Data Protection Laws of the World*. London: Sweet & Maxwell, 2007, 12th ed.
[4] ZALESKIS, Julius. ES Bendrasis duomenų apsaugos reglamentas: reikšmė duomenų apsaugos teisei. *Teisė*, 2017, t. 103, p. 45–54.

pagrindus[5]. Justina Dešriūtė analizavo duomenų apsaugos naujoves baudžiamajame procese[6]. Mindaugas Civilka ir Lina Šlapimaitė tyrė tik asmens duomenų sampratą, pateiktą Bendrajame duomenų apsaugos reglamente[7]. Tuo tarpu šiame darbe yra plačiai analizuojamos ir susisteminamos pagrindinės Bendruoju duomenų apsaugos reglamentu įgyvendinamos naujovės ir jų reikšmė naujajam teisiniam reguliavimui bei atskleidžiamas šio reglamento santykis su kitais duomenų apsaugos teisės šaltiniais. Darbas gali būti reikšmingas teisės doktrinai dėl išsamios sisteminės esamojo ir būsimojo duomenų apsaugos teisinio reguliavimo analizės; organizacijoms, siekiančioms prisitaikyti prie Bendruoju duomenų apsaugos reglamentu įtvirtinamų naujovių, dėl praktinių rekomendacijų pateikimo; kiekvienam asmeniui, siekiančiam pasinaudoti savo teisėmis, dėl plačios duomenų subjekto teisių analizės.

Svarbiausi šaltiniai. Rašant darbą pagrindiniai tyrimo šaltiniai buvo Bendrasis duomenų apsaugos reglamentas ir dabar galiojantys duomenų apsaugos norminiai teisės aktai – 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo bei šią direktyvą įgyvendinantis Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas. Taip pat buvo naudojamasi Europos Komisijos komunikatais bei ES 29 straipsnio duomenų apsaugos darbo grupės gairėmis kaip autoritetingais *soft law* šaltiniais, susijusiais su skirtingais Bendrojo duomenų apsaugos reglamento aspektais. Papildomai buvo remiamasi esama Lietuvos ir užsienio moksline doktrina bei Europos Žmogaus Teisių Teismo ir Europos Sąjungos Teisingumo Teismo praktika.

[5] ZALESKIS, Julius. Duomenų apsaugos pareigūno veiklos pagrindai pagal ES bendrąjį duomenų apsaugos reglamentą. *Teisė*, 2017, t. 104, p. 159–170.
[6] DEŠRIŪTĖ, Justina. Esminiai asmens duomenų apsaugos baudžiamajame procese reformos Europos Sąjungoje aspektai ir jų įtaka nacionaliniam teisiniam reguliavimui. *Teisės problemos*, 2016, nr. 1 (91), p. 25-51.
[7] CIVILKA, Mindaugas; ŠLAPIMAITĖ, Lina. Asmens duomenų samprata elektroninėje erdvėje. *Teisė*, 2015, t. 96, p. 126–148.

1. DUOMENŲ APSAUGOS TEISĖ IR JOS REFORMA ES

1.1. Duomenų apsaugos teisės samprata ir turinys

Lietuvoje asmens duomenų apsaugos teisė buvo pradėta formuoti siekiant užtikrinti prigimtinę asmens teisę į privatų gyvenimą informacijos srityje.[8] Tai atsispindi ir Lietuvos Respublikos Konstitucijoje, kurios 22 straipsnyje, įtvirtinančiame teisę į privatų gyvenimą, galima įžvelgti ir teisės į duomenų apsaugą pagrindus: „Informacija apie privatų asmens gyvenimą gali būti renkama tik motyvuotu teismo sprendimu ir tik pagal įstatymą.“[9]. Todėl teisė į duomenų apsaugą gali būti laikoma ir sudėtine teisės į privatų gyvenimą dalimi.

Asmens duomenų apsauga yra neatsiejama nuo privataus gyvenimo apsaugos. Informacija apie asmenį yra asmens duomenys, kurie yra vienas iš asmens privataus gyvenimo elementų. Todėl asmens duomenų rinkimas ir tvarkymas daro įtaką privačiam asmens gyvenimui. Dėl šių priežasčių, siekiant užtikrinti asmens teisę į privatų gyvenimą, turi būti užtikrinama ir asmens duomenų apsauga. Taip pat yra ir priešingas ryšys – saugant asmens duomenis, kartu yra saugomas ir asmens gyvenimo privatumas.[10]

Dėl šių sąsajų galima išskirti šiuos duomenų apsaugos teisės bruožus:

- asmens duomenų apsaugos teisė yra formuojama teisės į privatų gyvenimą garantijos pagrindu;
- asmens duomenų apsaugos teisės turinys yra tokios apimties, kuri yra būtina asmens informaciniam privatumui apsaugoti.[11]

Nors duomenų apsaugos teisė yra stipriai susijusi su privataus gyvenimo teise, Europos Sąjungos teisinėje sistemoje šios dvi teisės buvo aiškiai išskirtos ir atskirai įtvirtintos Europos Sąjungos pagrindinių teisių chartijoje (atitinkamai 8 ir 7 str.). Pagal Chartijos 8 straipsnį, „[k]iekvienas turi teisę į savo asmens duomenų apsaugą.“[12] Toks atskiras teisės į asmens duomenų apsaugą įtvirtinimas atskleidžia, jog ši teisė yra ne tik teisės į privatų gyvenimą dalis, bet ir pati savaime turėtų būti laikoma individualia ir viena iš pagrindinių žmogaus teisių.

Tuo tarpu Europos Tarybos priimtoje Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencijoje (EŽTK) teisė į duomenų apsaugą nėra įtvirtinta atskirai, tačiau yra viena iš teisių, saugomų pagal 8 straipsnyje įtvirtintą teisę į privatumą. Europos Žmogaus

[8] PETRAITYTĖ, Ilona. Asmens duomenų apsauga ir teisė į privatų gyvenimą. *Teisė*, 2011, t. 80, p. 172.
[9] Lietuvos Respublikos Konstitucija. *Valstybės žinios*, 1992, nr. 33-1014.
[10] PETRAITYTĖ, Ilona. Asmens duomenų apsauga ir teisė į privatų gyvenimą. *Teisė*, 2011, t. 80, p. 165.
[11] Ibid., p. 166.
[12] Europos Sąjungos pagrindinių teisių chartija. *OL* C 326, 2012 10 26, p. 391-407.

Teisių Teismas jau prieš daugelį metų išvystė teisės į privatumą sampratą ir išplėtė ją taip, kad ši apimtų ir asmens duomenų apsaugą. Byloje *Z. Prieš Suomiją* buvo pabrėžta, jog asmens duomenų apsauga turi fundamentalią reikšmę asmeniui įgyvendinant savo teisę į privatų gyvenimą, kuri yra įtvirtinta EŽTK 8 straipsnyje. O siekiant nustatyti šios teisės pažeidimą ir jo mastą, buvo remiamasi Europos Tarybos Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (Konvencija Nr. 108).[13]

Pamatinė asmens duomenų apsaugos teisės sąvoka yra asmens duomenys. Tai duomenų valdytojų ir duomenų tvarkytojų įpareigojimų taikymo pagrindas.[14] Pagal Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymą, tai yra „bet kuri informacija, susijusi su fiziniu asmeniu – duomenų subjektu, kurio tapatybė yra žinoma arba gali būti tiesiogiai ar netiesiogiai nustatyta pasinaudojant tokiais duomenimis kaip asmens kodas, vienas arba keli asmeniui būdingi fizinio, fiziologinio, psichologinio, ekonominio, kultūrinio ar socialinio pobūdžio požymiai.“[15] Ši sąvoka iš esmės sutampa ir su Europos Sąjungos teisės aktuose įtvirtinta asmens duomenų sąvoka (lyginant tiek esamą, tiek ir būsimą teisinį reguliavimą įgyvendinus duomenų apsaugos teisės reformą).

Nagrinėjant asmens duomenų sąvoką galima išskirti keturis svarbius elementus:

- bet kuri informacija;
- susijusi su;
- tapatybė yra nustatyta arba gali būti nustatyta;
- fizinis asmuo (duomenų subjektas).[16]

Tokius pačius asmens duomenų sąvokos elementus išskiria ir ES 29 straipsnio duomenų apsaugos darbo grupė (toliau – 29 str. darbo grupė) nuomonėje 4/2007 dėl asmens duomenų sąvokos[17]. Taip pat pažymima, jog platus sąvokos turinys buvo nustatytas specialiai, siekiant užtikrinti deramą asmens duomenų apsaugos lygį.[18] Be to, svarbu pabrėžti, jog visi keturi asmens duomenų sąvokos elementai yra vienas su kitu susiję ir turi būti vertinami kaip visuma.[19]

---

[13] Europos Žmogaus Teisių Teismas. 1997 m. vasario 25 d. sprendimas byloje *Z. prieš Suomiją*, Nr. 22009/93, ECHR:1997:0225JUD002200993.

[14] Europos Komisija. Visapusiškas požiūris į asmens duomenų apsaugą Europos Sąjungoje. *Komisijos komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialiniu reikalų komitetui ir Regionų komitetui COM(2010) 609 galutinis*, 2010, Briuselis, p. 5.

[15] Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas (su pakeitimais ir papildymais). *Valstybės žinios*, 1996, nr. 63-1479.

[16] Valstybinė duomenų apsaugos inspekcija. *Asmens duomenų teisinės apsaugos įstatymo komentaras*. Vilnius, 2005, p. 24-25.

[17] Article 29 Data Protection Working Party. *Opinion 4/2007 on the concept of personal data*. 01248/07/EN WP 136, p. 1-26.

[18] Ibid., p. 4.

[19] CIVILKA, Mindaugas; ŠLAPIMAITĖ, Lina. Asmens duomenų samprata elektroninėje erdvėje. *Teisė*, 2015, t. 96, p. 132.

Informacijos, kuri gali būti laikoma asmens duomenimis, spektras yra labai platus. Informacija gali būti objektyvi, subjektyvi, taip pat jai priskiriamos nuomonės ar vertinimai. Į informacijos sampratą patenka visa su asmens privačiu ir šeimos gyvenimu susijusi informacija, taip pat informacija apie asmens veiklą, darbo santykius, ekonominį ir socialinį elgesį.[20] Informacijos sampratai nėra svarbus jos fiksavimo būdas. Tai reiškia, jog asmens duomenų sąvoka yra technologiškai neutrali. Asmens duomenys apima garso ar vaizdo įrašus, o taip pat ir biometrinius duomenis.[21]

Nagrinėjant duomenų sąsają yra svarbu pabrėžti, jog duomenų paskirtis neprivalo būti informacijos apie asmenį pateikimas. Svarbiausia yra tai, kad ta informacija yra siejama su konkrečiu asmeniu.[22] Tokia sąsaja su konkrečiu asmeniu gali pasireikšti įvairiomis formomis ir būti paremta įvairiais ryšiais, sąveika ir santykiais.

Asmens tapatybės nustatymo galimybė yra ypač svarbus elementas. Net pačioje asmens duomenų sąvokoje yra pasakyta, jog tapatybė gali būti jau žinoma arba tiesiogiai ar netiesiogiai nustatoma pagal kitos informacijos visumą. Tačiau kiekvienu atveju asmens tapatybės nustatymas priklauso nuo informacijos vertintojo turimų žinių ir priemonių[23]. Laikoma, kad asmens tapatybę galima nustatyti tik tais atvejais, kai nustatymui naudojami savi ištekliai ar papildoma informacija, kurią bet kas gali gauti teisėtu būdu.[24]

Fizinio asmens elementas reiškia tai, jog saugomi tik fizinių (bet ne juridinių) asmenų duomenys. Tokį reguliavimą paaiškina teisės į duomenų apsaugą kilmė. Ši teisė yra kilusi iš teisės į privatų gyvenimą. Privatus gyvenimas yra susijęs būtent su žmonėmis, fiziniais asmenimis, todėl ir duomenų apsauga yra skirta fiziniams asmenims.[25] Šią savoką galima būtų patikslinti pabrėžiant, jog asmens duomenų apsauga taikoma tik gyviems fiziniams asmenims.[26]

Platus asmens duomenų vertinimas atsispindi ir Lietuvos teismų jurisprudencijoje. Pavyzdžiui, Lietuvos vyriausiojo administracinio teismo teisėjų kolegija 2012 metų byloje nusprendė, jog automobilio valstybinis numeris, modelis, pagaminimo metai yra laikytini

---

[20] Article 29 Data Protection Working Party. *Opinion 4/2007 on the concept of personal data*. 01248/07/EN WP 136, p. 6.
[21] CIVILKA, Mindaugas; ŠLAPIMAITĖ, Lina. Asmens duomenų samprata elektroninėje erdvėje. *Teisė*, 2015, t. 96, p. 133.
[22] Valstybinė duomenų apsaugos inspekcija. *Asmens duomenų teisinės apsaugos įstatymo komentaras*. Vilnius, 2005, p. 24.
[23] CIVILKA, Mindaugas; ŠLAPIMAITĖ, Lina. Asmens duomenų samprata elektroninėje erdvėje. *Teisė*, 2015, t. 96, p. 137.
[24] Valstybinė duomenų apsaugos inspekcija. *Asmens duomenų teisinės apsaugos įstatymo komentaras*. Vilnius, 2005, p. 25.
[25] Europos Sąjungos pagrindinių teisių agentūra (FRA); Europos Taryba; Europos Žmogaus Teisių Teismas. *Europos duomenų apsaugos teisės vadovas*. Liuksemburgas: Europos Sąjungos leidinių biuras, 2014, p. 35.
[26] Article 29 Data Protection Working Party. *Opinion 4/2007 on the concept of personal data*. 01248/07/EN WP 136, p. 22.

asmens duomenimis, nes netiesiogiai gali būti siejami su konkrečiu asmeniu – atitinkamo automobilio savininku.[27] Taip pat ir telefono numeris yra asmens duomuo, nes pagal jį galima identifikuoti asmenį, kuris naudojasi tuo telefono numeriu, kadangi telefono abonento numeris yra asmeninio naudojimo dalykas. Tokį išaiškinimą 2014 metų byloje pateikė Vilniaus miesto apylinkės teismas.[28]

Tačiau, nepaisant plataus teisės į duomenų apsaugą turinio, ši teisė nėra absoliuti.[29] Ji turi būti derinama kartu su kitomis teisėmis ir laisvėmis, ypač su saviraiškos laisve. Be to, naudojimasis teise į duomenų apsaugą gali būti apribotas, jeigu apribojimai yra numatyti įstatymuose, nekeičia teisės į duomenų apsaugą esmės ir, remiantis proporcingumo principu, yra būtini arba reikalingi kitų teisėms ir laisvėms apsaugoti.[30]

Pastebima, jog asmens duomenų apsaugos teisė iš pradžių buvo laikoma teisės į privatų gyvenimą įgyvendinimo priemonių sistema, kurios centrinė figūra yra asmuo, galintis inicijuoti asmens duomenų apsaugos priemonių taikymą.[31] Tačiau pastaruoju metu teisė į duomenų apsaugą tampa vis aktualesnė ir įgyja vis daugiau savarankiškumo. Todėl apibendrinant galima teigti, jog duomenų apsaugos teisė yra teisės normų, reguliuojančių bet kurios informacijos, susijusios su fiziniu asmeniu, kurio tapatybė yra žinoma arba gali būti nustatyta pagal tam tikrus duomenis, apsaugą, sistema.

1.2. Duomenų apsaugos teisės šaltiniai

Tarptautinės teisės šaltiniai

Tarptautiniu lygmeniu teisė į duomenų apsaugą dažniausiai yra suprantama kaip sudėtinė teisės į privatų gyvenimą dalis, tačiau atskirai nėra įtvirtinta kaip viena pagrindinių žmogaus teisių.[32] Tuo tarpu teisė į privatų gyvenimą jau daugybę metų yra laikoma universalia žmogaus teise, tarptautinėje teisinėje priemonėje pirmą kartą nustatyta 1948 m.

[27] Lietuvos vyriausiasis administracinis teismas. 2012 m. liepos 26 d. nutartis administracinėje byloje *UADBB „Edrauda“ v. Valstybinė duomenų apsaugos inspekcija*, Nr. A-858-2133-12.
[28] Vilniaus miesto apylinkės teismas. 2014 m. vasario 26 d. nutarimas administracinio teisės pažeidimo byloje Nr. A2.11.-1793-295/2014.
[29] Europos Sąjungos Teisingumo Teismas. 2010 m. lapkričio 9 d. sprendimas sujungtose bylose *Volker und Markus Schecke GbR (C-92/09) ir Hartmut Eifert (C-93/09) prieš Land Hessen*, EU:C:2010:662, 48 punktas.
[30] Europos Sąjungos pagrindinių teisių chartija. *OL* C 326, 2012 10 26, p. 402.
[31] PETRAITYTĖ, Ilona. Asmens duomenų apsauga ir teisė į privatų gyvenimą. *Teisė*, 2011, t. 80, p. 173.
[32] European Data Protection Supervisor. *Data Protection*. [interaktyvus; žiūrėta 2018 m. vasario 6 d.]. Prieiga per internetą: <https://edps.europa.eu/data-protection/data-protection_en>.

Jungtinių Tautų Visuotinės žmogaus teisių deklaracijos (VŽTD)[33] 12 str. dėl teisės į privataus ir šeimos gyvenimo gerbimą.[34] Ši deklaracija buvo priimta kaip privalomos teisinės galios neturintis teisės šaltinis, tačiau tapo paprotine tarptautine teise, kurios principai vėliau buvo įtvirtinti kituose privalomuose žmogaus teisių šaltiniuose.

Pagrindus teisei į duomenų apsaugą galima rasti ir 1950 metais Europos Tarybos priimtoje Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencijoje. Konvencijos 8 str. 1 d. nurodo, jog „[k]iekvienas turi teisę į tai, kad būtų gerbiamas jo asmeninis ir jo šeimos gyvenimas, buto neliečiamybė ir susirašinėjimo slaptumas“.[35] Teisė į asmens duomenų apsaugą yra viena iš teisių, saugomų pagal šį straipsnį.[36] Tai patvirtina ir Europos Žmogaus Teisių Teismo praktika. Pavyzdžiui, 2008 m. gruodžio 4 d. byloje *S. ir Marper prieš Jungtinę Karalystę* teismas nurodė, jog asmens duomenų apsauga yra labai svarbi įgyvendinant asmens teisę į privatų gyvenimą, kuri yra įtvirtinta Europos žmogaus teisių konvencijos 8 str.[37]

Tačiau pirmasis tiesiogiai su duomenų apsauga susijęs teisiškai privalomas tarptautinis dokumentas yra 1981 m. sausio 28 d. Europos Tarybos Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (Konvencija Nr. 108).[38] Šios konvencijos tikslas yra užtikrinti, kad, tvarkant asmens duomenis automatizuotai, visų šalių teritorijose būtų gerbiamos kiekvieno asmens, nepaisant jo tautybės ir gyvenamosios vietos, teisės ir pagrindinės laisvės, o svarbiausia, jo teisė į privatų gyvenimą.[39] Taip pat konvencijoje numatyti duomenų apsaugos principai, šalių abipusės pagalbos ir bendradarbiavimo nuostatos bei galimybės taikyti apribojimus su duomenų apsauga susijusioms teisėms.[40]

---

[33] Visuotinė žmogaus teisų deklaracija. Jungtinės Tautos (JT). 1948. *Valstybės žinios*, 2006-06-17, nr. 68-2497. 12 straipsnis: „Niekas neturi patirti savavališko kišimosi į jo privatumą, šeimos gyvenimą, buitį ar susirašinėjimą arba kėsinimosi į jo garbę ir reputaciją. Kiekvienas turi teisę į įstatymo apsaugą nuo tokio kišimosi arba kėsinimosi.“

[34] Europos Sąjungos pagrindinių teisių agentūra (FRA); Europos Taryba; Europos Žmogaus Teisių Teismas. *Europos duomenų apsaugos teisės vadovas*. Liuksemburgas: Europos Sąjungos leidinių biuras, 2014, p. 14.

[35] 1950 m. lapkričio 4 d. Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencija. *Valstybės žinios*, 1995-05-16, nr. 40-987.

[36] Europos Sąjungos pagrindinių teisių agentūra (FRA); Europos Taryba; Europos Žmogaus Teisių Teismas. *Europos duomenų apsaugos teisės vadovas*. Liuksemburgas: Europos Sąjungos leidinių biuras, 2014, p. 15.

[37] Europos Žmogaus Teisių Teismas. 2008 m. gruodžio 4 d. sprendimas byloje *S. ir Marper prieš Jungtinę Karalystę*, Nr. 30562/04 ir 30566/04, ECLI:CE:ECHR:2008:1204JUD003056204, 103 punktas.

[38] Europos Parlamentas. *Asmens duomenų apsauga*. [interaktyvus; žiūrėta 2018 m. vasario 6 d.]. Prieiga per internetą:<http://www.europarl.europa.eu/atyourservice/lt/displayFtu.html?ftuId=FTU_4.2.8.html>.

[39] 1981 m. sausio 28 d. Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (Konvencija Nr. 108). *Valstybės žinios*, 2001-04-13, nr. 32-1059.

[40] Ibid.

Europos Sąjungos teisės šaltiniai

Europos Sąjungos lygmeniu teisei į duomenų apsaugą didelę reikšmę turėjo 2007 m. pasirašyta Lisabonos sutartis, iš dalies keičianti Europos Sąjungos sutartį ir Europos bendrijos steigimo sutartį.[41] Pirma, teisė į asmens duomenų apsaugą buvo įtvirtinta kaip viena iš pagrindinių ES vertybių. Be to, Lisabonos sutartimi į Sutartį dėl Europos Sąjungos veikimo (SESV)[42] buvo įtraukta 16 str. 1 d., kurioje nustatytas principas, kad kiekvienas asmuo turi teisę į savo asmens duomenų apsaugą. Taip pat Lisabonos sutartimi SESV 16 str. 2 d. numatytas specialus asmens duomenų apsaugos taisyklių priėmimo teisinis pagrindas.[43]

Teisė į duomenų apsaugą taip pat yra įtvirtinta Europos Sąjungos pagrindinių teisių chartijoje. Chartijos 8 str. 1 d., kaip ir SESV 16 str. 1 d., įtvirtinta, kad „[k]iekvienas turi teisę į savo asmens duomenų apsaugą“.[44] Iš pradžių Chartija buvo tik politinio pobūdžio, vėliau tapo teisiškai privalomu dokumentu, o galiausiai Lisabonos sutartimi tapo Europos Sąjungos pirminės teisės dalimi.[45] Toks pokytis dar labiau sustiprina duomenų apsaugos teisinį pagrindą ir patvirtina Europos Komisijos požiūrį, jog „[d]uomenų apsauga yra viena iš pagrindinių teisių Europoje, įtvirtinta Europos Sąjungos pagrindinių teisių chartijos 8 str. 1 d. ir Sutarties dėl Europos Sąjungos veikimo 16 str. 1 d., ir turi būti atitinkamai saugoma“.[46]

Tinkamą teisės į duomenų apsaugą įgyvendinimą užtikrina antrinė Europos Sąjungos teisė. Šiuo metu pagrindinė ES teisinė priemonė duomenų apsaugos srityje vis dar yra 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo (Duomenų apsaugos direktyva),[47] kurią 2018 m. gegužės 25 d. pakeis Bendrasis duomenų apsaugos reglamentas. Ši direktyva buvo priimta siekiant praplėsti ir detalizuoti Konvencijoje Nr. 108 numatytus

[41] Lisabonos sutartis, iš dalies keičianti Europos Sąjungos sutartį ir Europos bendrijos steigimo sutartį. *OL* C 306, 2007 12 13, p. 51.
[42] Sutartis dėl Europos Sąjungos veikimo (suvestinė redakcija). *OL* C 202, 2016 6 7, p. 55.
[43] Europos Komisija. Europos Parlamento ir Tarybos reglamentas dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo (Bendrasis duomenų apsaugos reglamentas). *Pasiūlymas COM(2012) 11 galutinis*, 2012, Briuselis, p. 3.
[44] Europos Sąjungos pagrindinių teisių chartija. *OL* C 326, 2012 10 26.
[45] Europos Sąjungos pagrindinių teisių agentūra (FRA); Europos Taryba; Europos Žmogaus Teisių Teismas. *Europos duomenų apsaugos teisės vadovas*. Liuksemburgas: Europos Sąjungos leidinių biuras, 2014, p. 20.
[46] Europos Komisija. Privatumo apsauga glaudžiai susijusiame pasaulyje: Europos duomenų apsaugos reglamentavimo pagrindai XXI amžiuje. *Komisijos komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui COM(2012) 9galutinis*, 2012, Briuselis, p. 2.
[47] 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo. *OL* 2004 m. specialusis leidimas, 13 skyrius, 15 tomas, p. 355–374.

principus.[48] Vienas iš pagrindinių šios direktyvos tikslų yra apsaugoti pagrindines fizinių asmenų teises ir laisves, ypač privatumo teisę tvarkant asmens duomenis (Duomenų apsaugos direktyvos 1 str.). Šis tikslas atskleidžia, jog teisė į duomenų apsaugą ir teisė į privatų gyvenimą yra glaudžiai susijusios teisės. Tokį požiūrį patvirtina ir Europos Sąjungos Teisingumo Teismas, pažymėdamas, jog Chartijos 7 ir 8 straipsniais pripažinta teisė į privataus gyvenimo gerbimą tvarkant asmens duomenis.[49]

Tačiau Duomenų apsaugos direktyva netaikoma su bendradarbiavimu policijos ir baudžiamosios teisenos sritimi susijusiems klausimams. Šią sritį reguliuoja 2008 m. lapkričio 27 d. Tarybos pamatinis sprendimas 2008/977/TVR dėl asmens duomenų, tvarkomų vykdant policijos ir teisminį bendradarbiavimą baudžiamosiose bylose, apsaugos (Duomenų apsaugos pamatinis sprendimas)[50]. 2018 m. gegužės 25 d. šį pamatinį sprendimą pakeis Europos Parlamento ir Tarybos direktyva (ES) 2016/680 dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo, ir kuriuo panaikinamas Tarybos pamatinis sprendimas 2008/977/TVR.[51]

Tam tikroms sritims, net ir reguliuojamoms Duomenų apsaugos direktyvos, yra taikomi specialūs teisės aktai dėl aiškesnių ir išsamesnių nuostatų poreikio. Todėl ES duomenų apsaugą taip pat reguliuoja šie teisės aktai:

- 2000 m. gruodžio 18 d. Europos Parlamento ir Tarybos Reglamentas (EB) Nr. 45/2001 dėl asmenų apsaugos Bendrijos institucijoms ir įstaigoms tvarkant asmens duomenis ir laisvo tokių duomenų judėjimo (ES institucijų duomenų apsaugos reglamentas).[52]

[48] Europos Sąjungos pagrindinių teisių agentūra (FRA); Europos Taryba; Europos Žmogaus Teisių Teismas. *Europos duomenų apsaugos teisės vadovas*. Liuksemburgas: Europos Sąjungos leidinių biuras, 2014, p. 18.
[49] Europos Sąjungos Teisingumo Teismas. 2011 m. lapkričio 24 d. sprendimas sujungtose bylose *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) ir Federación de Comercio Electrónico y Marketing Directo (FECEMD) prieš Administración del Estado* C-468/10 ir C-469/10, EU:C:2011:777. 42 punktas.
[50] 2008 m. lapkričio 27 d. Tarybos pamatinis sprendimas 2008/977/TVR dėl asmens duomenų, tvarkomų vykdant policijos ir teisminį bendradarbiavimą baudžiamosiose bylose, apsaugos (Duomenų apsaugos pamatinis sprendimas). *OL* L 350, 2008 12 30, p. 60-71.
[51] 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/680 dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo, ir kuriuo panaikinamas Tarybos pamatinis sprendimas 2008/977/TVR. *OL* L 119, 2016 5 4, p. 89-131.
[52] 2000 m. gruodžio 18 d. Europos Parlamento ir Tarybos Reglamentas (EB) Nr. 45/2001 dėl asmenų apsaugos Bendrijos institucijoms ir įstaigoms tvarkant asmens duomenis ir laisvo tokių duomenų judėjimo (ES institucijų duomenų apsaugos reglamentas). *OL* L 8, 2001 1 12, p. 1-22.

- 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių).[53]
- 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.[54]

Lietuvos Respublikos teisės šaltiniai

Lietuvoje asmens duomenų apsaugos teisinio reguliavimo branduolį sudaro Lietuvos Respublikos Konstitucijos 22 str. 1 d. nuostata, pagal kurią žmogaus privatus gyvenimas neliečiamas.[55] Konstitucinis Teismas 2000 m. gegužės 8 d. nutarime pažymėjo, jog asmens teisė į privatų gyvenimą „apima asmeninį, šeimos ir namų gyvenimą, asmens fizinę ir psichinę neliečiamybę, garbę ir reputaciją, asmeninių faktų slaptumą, draudimą skelbti gautą ar surinktą konfidencialią informaciją ir kt.“[56] Pagal tai galima teigti, jog informacija apie asmenį (asmens duomenys) ir šios informacijos apsauga yra sudedamoji teisės į privatų gyvenimą dalis. Užtikrinant asmens teisę į privatų gyvenimą, kartu turi būti užtikrinama ir asmens duomenų apsauga.[57]

Pagrindinis teisės aktas duomenų apsaugos srityje yra Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas (toliau – Duomenų apsaugos įstatymas), kuris įgyvendina Duomenų apsaugos direktyvą. Policijos ir teisminio bendradarbiavimo baudžiamosiose bylose asmens duomenų apsaugą reglamentuoja Lietuvos Respublikos asmens duomenų, tvarkomų vykdant policijos ir teisminį bendradarbiavimą baudžiamosiose bylose, teisinės apsaugos įstatymas.[58] Taip pat, kaip nurodo Lietuvos Respublikos Teisingumo ministerija, teisės aktams, reguliuojantiems asmens duomenų

[53] 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių). *OL* L 201, 2002 7 31, p. 37–47.
[54] 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, p. 1–30.
[55] PETRAITYTĖ, Ilona. Asmens duomenų apsaugos teisinis reguliavimas Lietuvos teisės sistemoje. *Teisė*, 2011, t. 79, p. 135.
[56] Lietuvos Respublikos Konstitucinis Teismas. 2000 m. gegužės 8 d. nutarimas byloje Nr. 12/99-27/99-29/99-1/2000-2/2000.
[57] PETRAITYTĖ, Ilona. Asmens duomenų apsauga ir teisė į privatų gyvenimą. *Teisė*, 2011, t. 80, p. 165.
[58] Lietuvos Respublikos asmens duomenų, tvarkomų vykdant policijos ir teisminį bendradarbiavimą baudžiamosiose bylose, teisinės apsaugos įstatymas. *Valstybės žinios*, 2011-05-03, nr. 52-2511.

apsaugą priskiriamas ir Lietuvos Respublikos elektroninių ryšių įstatymas.[59] Šis įstatymas reguliuoja asmens duomenų tvarkymą teikiant viešųjų elektroninių ryšių paslaugas.[60]

1.3. Duomenų apsaugos teisės reforma ES

Šiuo metu Europos Sąjungos lygmeniu vyksta duomenų apsaugos teisės reforma. Dar 2009 m. Europos Komisija inicijavo dabartinės duomenų apsaugos teisės sistemos peržiūrą, kurios pradžia tapo 2009 m. gegužės mėnesį surengta konferencija, po kurios vyko viešos konsultacijos ir buvo vykdomi tyrimai.[61] 2012 m. Europos Komisija jau pateikė pasiūlymą dėl naujojo asmens duomenų apsaugos ES teisinio reglamentavimo pagrindų, kuriuo siekiama modernizuoti dabartinį reglamentavimą prisiderinant prie vykstančių pokyčių.[62]

Po ilgų derybų su pasiūlymu galiausiai buvo sutikta ir 2016 m. buvo priimti du teisės aktai, kurie sudaro naujojo duomenų apsaugos reglamentavimo pagrindą:

- 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);[63]
- 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/680 dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo, ir kuriuo panaikinamas Tarybos pamatinis sprendimas 2008/977/TVR.[64]

---

[59] Lietuvos Respublikos Teisingumo ministerija. *Teisės aktai, reguliuojantys asmens duomenų apsaugą*. [interaktyvus; žiūrėta 2018 m. vasario 5 d.]. Prieiga per internetą: <http://www.tm.lt/teisineinfo/teisesaktas/52>.

[60] Lietuvos Respublikos elektroninių ryšių įstatymas (su pakeitimais ir papildymais). *Valstybės žinios*, 2004-04-30, nr. 69-2382.

[61] Europos Komisija. Visapusiškas požiūris į asmens duomenų apsaugą Europos Sąjungoje. *Komisijos komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialiniu reikalų komitetui ir Regionų komitetui COM(2010) 609 galutinis*, 2010, Briuselis, p. 3.

[62] Europos Komisija. Europos Parlamento ir Tarybos reglamentas dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo (Bendrasis duomenų apsaugos reglamentas). *Pasiūlymas COM(2012) 11 galutinis*. 2012, Briuselis, p. 2.

[63] 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). *OL* L 119, 2016 5 4, p. 1-88.

[64] 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/680 dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo, ir kuriuo panaikinamas Tarybos pamatinis sprendimas 2008/977/TVR. *OL* L 119, 2016 5 4, p. 89-131.

1.3.1. Poreikio reformai priežastys

1995 m. Europos Parlamento ir Tarybos priimta Duomenų apsaugos direktyva jau daugelį metų yra pagrindinis ES teisės aktas duomenų apsaugos srityje. Šios direktyvos 1 straipsnis įtvirtina du ypač svarbius ES integracijos proceso tikslus:

- apsaugoti pagrindines fizinių asmenų teises ir laisves, ypač privatumo teisę tvarkant asmens duomenis;
- užtikrinti laisvą asmens duomenų judėjimą tarp valstybių narių taip sukuriant ir stiprinant vidaus rinką.[65]

Po Duomenų apsaugos direktyvos priėmimo praėjo daug metų ir nors joje įtvirtinti tikslai ir principai išlieka ne mažiau svarbūs ir aktualūs ir šiomis dienomis, tačiau visuomenėje įvyko daugybė pokyčių, kuriuos ypač lemia suaktyvėjusi globalizacija ir spartus technologijų vystymasis.[66]

Didžiausią grėsmę duomenų apsaugai kelia internetas. Internete kaupiami dideli kiekiai asmens duomenų, kurie dažnai yra saugomi neribotą laiką ir gali būti prieinami iš bet kurios pasaulio vietos. Pavieniai viešai matomi asmens duomenys paprastai neturi neigiamos įtakos asmens privačiam gyvenimui, tačiau duomenų visuma gali padidinti asmens reputacijos ir orumo pažeidžiamumą bei sukelti kitų neigiamų pasekmių.

Kaip itin dažną šių laikų pavyzdį galima paminėti vis labiau populiarėjančius socialinius tinklus, kurių naudotojais aktyviai tampa įvairaus amžiaus žmonės. Socialiniuose tinkluose vartotojai skelbia įvairaus turinio informaciją, kuri apima ne tik pačius pagrindinius asmens duomenis, tokius kaip vardą, pavardę, telefoną, bet ir gyvenamosios vietos adresą, lankytinas vietas, veiklas, kuriomis užsiima, ir elgseną. Atsidūrusi netinkamose rankose ši informacija gali padaryti didelę žalą asmens privatumui ar net saugumui.

Nerimą dėl duomenų subjektų privatumo ir apsaugos kelia taip pat ir debesų kompiuterija. Kai asmeninė informacija yra saugoma serveriuose, kurie yra nuolatos prijungti prie interneto ir prie kurių galima prisijungti iš bet kurio kito prie interneto prijungto įrenginio, tokios informacijos saugumas tampa dar labiau abejotinas. Vis didėjant kibernetinių nusikaltimų grėsmei debesų kompiuterijos paslaugų srityje, asmenys, prieš

[65] 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo. *OL* 2004 m. specialusis leidimas, 13 skyrius, 15 tomas, p. 362.

[66] Europos Komisija. Visapusiškas požiūris į asmens duomenų apsaugą Europos Sąjungoje. *Komisijos komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialiniu reikalų komitetui ir Regionų komitetui COM(2010) 609 galutinis*, 2010, Briuselis, p. 2.

pradėdami naudotis šiomis paslaugomis turėtų pasirinkti patikimą paslaugos teikėją, kuris garantuotų asmens duomenų saugumą ir privatumą.[67]

Dar vienas iššūkis duomenų apsaugai yra asmens duomenų rinkimo būdų sudėtingėjimas ir atsekimo galimybių mažėjimas. Apie asmenis dažniausiai yra sužinoma labai daug vertingos informacijos tiesiog stebint jų veiklą, pavyzdžiui, sekant apsipirkimo internetu tendencijas. Tam tikros technologijos leidžia automatiškai rinkti asmens duomenis, pavyzdžiui, kai asmuo naudojasi elektroninėmis viešojo transporto bilietų kortelėmis. Taip pat daug lengviau nustatomos asmens lankymosi vietos naudojantis įvairiomis išmaniųjų telefonų programėlėmis.[68]

Tyrimai taip pat patvirtina tai, jog tiek duomenų apsaugos institucijos, tiek įmonių asociacijos, tiek ir vartotojų organizacijos mano, kad grėsmė asmens duomenų privatumui ir saugumui nuolat auga.[69] Todėl duomenų apsaugos teisei taip pat tenka prisiderinti prie sparčių pokyčių visuomenėje ir užtikrinti naujų kilusių uždavinių įgyvendinimą.

Kitas ypač svarbus veiksnys, lemiantis poreikį duomenų apsaugos reformai, yra tai, jog dabar taikoma Duomenų apsaugos direktyva neužtikrina vienodo duomenų apsaugos lygio Europos Sąjungoje. Šią direktyvą įgyvendina valstybių narių nacionaliniai įstatymai, kuriuose įtvirtintos taisyklės skiriasi. Todėl Europos Sąjungoje yra 28 skirtingi su duomenų apsauga susiję teisės aktai, lemiantys skirtingą teisinę aplinką. Dėl to skirtingose valstybėse narėse neužtikrinama vienoda asmenų apsauga ir tai sukelia teisinį netikrumą. Tai taip pat stipriai apsunkina tarptautines įmones, kurioms dėl skirtingų duomenų apsaugos įstatymų gali kilti papildoma administracinė našta ir išlaidos.[70]

Dėl visų šių priežasčių Europos Sąjungoje vyksta duomenų apsaugos teisinio reguliavimo reforma – 2018 m. gegužės 25 d. bus pradėtas taikyti Bendrasis duomenų apsaugos reglamentas.

---

[67] Ryšių reguliavimo tarnyba. *RRT teikia rekomendacijas dėl debesų kompiuterijos paslaugų saugumo*. [interaktyvus; žiūrėta 2018 m. sausio 7.]. Prieiga per internetą: <http://www.rrt.lt/lt/vartotojui/tinklu-informacijos-saugumas-vartotojui/debesu-kompiuterija.html>.

[68] Europos Komisija. Visapusiškas požiūris į asmens duomenų apsaugą Europos Sąjungoje. *Komisijos komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialiniu reikalų komitetui ir Regionų komitetui COM(2010) 609 galutinis*, 2010, Briuselis, p. 2.

[69] London Economics. *Study on the economic benefits of privacy-enhancing technologies (PETs): Final Report to The European Commission, DG Justice, Freedom and Security*. 2010, London, p. 16. Prieiga per internetą:
<https://londoneconomics.co.uk/wp-content/uploads/2011/09/17-Study-on-the-economic-benefits-of-privacy-enhancing-technologies-PETs.pdf>.

[70] Europos Komisija. Privatumo apsauga glaudžiai susijusiame pasaulyje: Europos duomenų apsaugos reglamentavimo pagrindai XXI amžiuje. *Komisijos komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui COM(2012) 9 galutinis*, 2012, Briuselis, p. 7.

1.3.2. Reformos tikslai ir priemonės

Siekiant modernizuoti ES asmens duomenų apsaugos sistemą, kitaip tariant, bandant paskatinti visoje ES galiojančių taisyklių nustatymą, kad duomenys galėtų laisvai judėti tarp skirtingų valstybių ir kad būtų užtikrintas teisinis tikrumas bei sumažinta administracinė našta,[71] buvo nustatyti šie pagrindiniai tikslai:

- stiprinti asmenų teises duomenų apsaugos srityje;
- stiprinti ES vidaus rinkos aspektą;
- užtikrinti pasaulinę duomenų apsaugą;
- stiprinti institucines priemones, skirtas veiksmingam duomenų apsaugos taisyklių įgyvendinimui.[72]

Stiprinant asmenų teises duomenų apsaugos srityje, pirmiausiai turi būti užtikrinta tinkama jau esamų teisių apsauga ir tik tada kuriamos naujos teisės atsižvelgiant į naujųjų technologijų vystymąsi ir jų poveikį asmens teisėms duomenų apsaugos srityje. Taip pat turėtų būti didinamas asmens duomenų valdymo ir tvarkymo skaidrumas. Kiekvienas asmuo turėtų žinoti, kas ir kokiais tikslais renka jo duomenis, kaip tie duomenys tvarkomi ir kuriam laikui saugomi, kad galėtų tinkamai savo asmens duomenis kontroliuoti. Šioje srityje išskirtinis dėmesys turėtų būti skiriamas vaikų asmens duomenims.[73]

Galimybės kontroliuoti savo duomenis didinimas pasireiškia tokių teisių visuma kaip teisė susipažinti su savo duomenimis, juos ištaisyti, ištrinti, apriboti ar sustabdyti jų tvarkymą. Taip pat asmens turima kontrolė jo duomenims būtų didinama laikantis duomenų kiekio mažinimo principo. Pagal šį principą duomenų valdytojai galėtų tvarkyti asmens duomenis tik numatytais tikslais.[74] Tai reiškia, jog būtų apsiribojama tik pačių būtiniausių duomenų rinkimu, kaupimu ir tvarkymu, tokiu būdu duomenų subjektui paliekant didesnę savo duomenų kontrolės galimybę.

Veiksmingas duomenų subjekto teisių įgyvendinimas neatsiejamas nuo asmenų informuotumo. Visuomenė turėtų būti informuota visais su duomenų tvarkymu susijusiais klausimais, kad kiekvienas asmuo žinotų, kokias teises turi ir kaip gali jomis pasinaudoti. Todėl turėtų būti skatinamos informuotumo duomenų apsaugos srityje didinimo veiklos. Į

[71] Europos Komisija. Privatumo apsauga glaudžiai susijusiame pasaulyje: Europos duomenų apsaugos reglamentavimo pagrindai XXI amžiuje. *Komisijos komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui COM(2012) 9 galutinis*, 2012, Briuselis, p.2.
[72] Europos Komisija. Visapusiškas požiūris į asmens duomenų apsaugą Europos Sąjungoje. *Komisijos komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialiniu reikalų komitetui ir Regionų komitetui COM(2010) 609 galutinis*, 2010, Briuselis, p. 5-17.
[73] Ibid., p. 5-6.
[74] Ibid., p. 7.

šias veiklas galėtų įsitraukti įvairūs subjektai, tokie kaip patys duomenų valdytojai, duomenų apsaugos institucijos ir net švietimo įstaigos.[75]

Siekiant išvengti situacijų, kai asmens duomenys yra tvarkomi neteisėtai, turėtų būti gaunamas konkretus aiškiai informuoto duomenų subjekto sutikimas, leidžiantis tvarkyti jo duomenis. Šis sutikimas visais atvejais turi būti duodamas savanoriškai, o tam yra būtina, jog duomenų subjektas aiškiai suvoktų, su kokiomis būtent sąlygomis sutinka.[76] Taip pat turėtų būti užtikrinamas aiškus sąlygų pateikimas, kad asmuo galėtų įvertinti situaciją ir savo sutikimą pateikti eksplicitiškai.

Kalbant apie ES vidaus rinkos aspekto stiprinimą, pirmiausiai reikia užtikrinti vienodų sąlygų skirtingose valstybėse narėse taikymą duomenų valdytojams. Tokiu būdu užtikrinamas teisinis tikrumas ir skatinamas laisvas asmens duomenų judėjimas tarp valstybių narių. Bendrų nuostatų, susijusių su duomenų apsauga, nebuvimas sukelia papildomų problemų suinteresuotiems subjektams. Šios problemos pasižymi padidėjusia administracine našta ir papildomų išlaidų buvimu. Ypač tarptautinėms organizacijoms tenka susidurti su skirtingais kiekvienos šalies duomenų apsaugos įstatymais. Be to, tai iškreipia vienodo apsaugos lygio galimybes ir duomenų subjektams. Dėl šių priežasčių ypač svarbu duomenų apsaugos taisykles suderinti visos ES lygmeniu.[77]

ES vidaus rinkos aspektas galėtų būti stiprinamas taip pat ir suteikiant didesnę atsakomybę duomenų valdytojams. Asmens duomenys renkami ir tvarkomi duomenų valdytojų tikslams įgyvendinti, todėl būtent jie pirmiausiai ir turėtų atsakyti už duomenų subjektų teisių įgyvendinimą. Tam turėtų būti užtikrinama veiksminga duomenų valdytojų vidinė politika ir duomenų apsaugai taikomi mechanizmai. Pagrindinės priemonės duomenų valdytojų atsakomybei didinti yra atskaitomybės principo įtvirtinimas ir privalomas duomenų apsaugos pareigūno paskyrimas.[78]

Dėl sparčios globalizacijos nuolat aktyvėja asmens duomenų judėjimas už ES ribų. Todėl vis aktualesni tampa iššūkiai, susiję su pasauline duomenų apsauga. Siekiant tinkamai apsaugoti ES piliečių asmens duomenis, turi būti deramai įvertinta, ar trečioji šalis, kuriai planuojama perduoti asmens duomenis, gali užtikrinti pagal ES standartus pakankamą duomenų apsaugos lygį. Todėl turėtų būti gerinami dabartiniai tarptautinio asmens duomenų perdavimo mechanizmai bei aiškiau išdėstomos ir supaprastinamos su

[75] Europos Komisija. Visapusiškas požiūris į asmens duomenų apsaugą Europos Sąjungoje. *Komisijos komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialiniu reikalų komitetui ir Regionų komitetui COM(2010) 609 galutinis*, 2010, Briuselis, p. 8.
[76] Ibid., p. 8-9.
[77] Ibid., p. 10.
[78] Ibid., p. 11-12.

perdavimu susijusios procedūros.[79] Tik tokiu būdu asmens duomenys bus tinkamai apsaugomi ne tik ES viduje, bet ir už jos ribų.

Institucinių priemonių, skirtų veiksmingam duomenų apsaugos taisyklių įgyvendinimui, stiprinimas pasižymi pirmiausiai nacionalinių duomenų apsaugos institucijų vaidmens didinimu. Būtent šios institucijos prižiūri, kaip užtikrinamos su duomenų apsauga susijusios teisės ir laisvės bei jų įgyvendinimas. Taip pat didesnis vaidmuo galėtų būti skiriamas 29 str. darbo grupei (jos darbą nuo 2018 m. gegužės 25 d. perims Europos duomenų apsaugos valdyba), kuri turėtų tapti pagrindiniu patariamuoju organu ir kurti rekomendacijas visais su naujuoju duomenų apsaugos reguliavimu susijusiais klausimais.[80]

[79] Europos Komisija. Visapusiškas požiūris į asmens duomenų apsaugą Europos Sąjungoje. *Komisijos komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialiniu reikalų komitetui ir Regionų komitetui COM(2010) 609 galutinis*, 2010, Briuselis, p. 15-16.
[80] Ibid., p. 17-18.

2. BENDRASIS DUOMENŲ APSAUGOS REGLAMENTAS IR JUO ĮGYVENDINAMOS NAUJOVĖS

2.1. Reglamento turinys

2018 m. gegužės 25 d. pradedamu taikyti Bendruoju duomenų apsaugos reglamentu (toliau – Reglamentas) siekiama nustatyti šiuolaikiškas ir visoje Europos Sąjungoje galiojančias asmens duomenų apsaugos taisykles. Reglamentas kaip teisės akto rūšis buvo pasirinktas neatsitiktinai. Reglamentas yra taikomas tiesiogiai visose valstybėse narėse[81], todėl jo nereikės perkelti į nacionalinius teisės aktus. Tai užtikrins duomenų apsaugos teisės suderinamumą, sustiprins teisinį tikrumą ir paskatins bendros rinkos vystymąsi.

Reglamentą sudaro 11 skyrių: 1) bendrosios nuostatos; 2) principai; 3) duomenų subjekto teisės; 4) duomenų valdytojas ir duomenų tvarkytojas; 5) asmens duomenų perdavimai į trečiąsias valstybes arba tarptautinėms organizacijoms; 6) nepriklausomos priežiūros institucijos; 7) bendradarbiavimas ir nuoseklumas; 8) teisių gynimo priemonės, atsakomybė ir sankcijos; 9) nuostatos, susijusios su konkrečiais duomenų tvarkymo atvejais; 10) deleguotieji aktai ir įgyvendinimo aktai; 11) baigiamosios nuostatos.[82]

Šiuose skyriuose įtvirtinta nemažai atnaujintų ES duomenų apsaugos taisyklių, kuriomis užtikrinama aukšto lygio asmens duomenų apsauga, ypač sustiprinant fizinių asmenų teises ir taikant griežtesnį taisyklių vykdymo užtikrinimą.[83] Nors Reglamentas grindžiamas galiojančiais teisės aktais, tačiau dėl plataus poveikio ir daugybės naujovių tam tikrus aspektus reikės iš esmės pakoreguoti.[84]

Pirmiausia, išplečiama teritorinė taikymo sritis. Reglamentas bus taikomas ir tuo atveju, kai ES esančių duomenų subjektų asmens duomenis tvarko ES neįsisteigęs duomenų valdytojas arba duomenų tvarkytojas, jeigu duomenų tvarkymo veikla yra susijusi su: a) prekių arba paslaugų siūlymu tokiems duomenų subjektams Sąjungoje; arba b) elgesio, kai jie veikia Sąjungoje, stebėsena (Reglamento 3 str. 2 d.). Taigi, nuo šiol daug daugiau organizacijų, net ir neįsisteigusių ES, privalės laikytis Reglamento taisyklių.

---

[81] Sutartis dėl Europos Sąjungos veikimo (suvestinė redakcija). *OL* C 202, 2016 6 7, 288 str.

[82] 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). *OL* L 119, 2016 5 4, p. 1-88.

[83] Europos Komisija. Privatumo apsauga glaudžiai susijusiame pasaulyje: Europos duomenų apsaugos reglamentavimo pagrindai XXI amžiuje. *Komisijos komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui COM(2012) 9 galutinis*, 2012, Briuselis, p.4.

[84] Europos Komisija. Didesnė apsauga, naujos galimybės. Komisijos gairės dėl tiesioginio Bendrojo duomenų apsaugos reglamento taikymo nuo 2018 m. gegužės 25 d. *Komisijos komunikatas Europos Parlamentui ir Tarybai COM(2018) 43 galutinis*, 2018, Briuselis, p. 2.

Šalia jau dabar egzistuojančių su asmens duomenų tvarkymu susijusių teisėtumo, sąžiningumo, tikslo apribojimo, duomenų kiekio mažinimo, tikslumo, saugojimo trukmės apribojimo, vientisumo ir konfidencialumo principų pridedami skaidrumo ir atskaitomybės principai. Nuo šiol duomenų valdytojas bus atsakingas ne tik už visų šių duomenų apsaugos principų laikymąsi, bet ir turės sugebėti įrodyti, kad jų laikomasi (Reglamento 5 str. 2 d.).

Taip pat sugriežtėjo sutikimo, reikalingo tam, kad asmens duomenys būtų tvarkomi tam tikru tikslu, sąlygos. Sutikimu negali būti laikoma tyla, iš anksto pažymėti langeliai arba neveikimas. Sutikimas turi būti konkretus, pagrįstas informacija, duodamas laisva valia, išreiškiamas aiškiai ir vienareikšmiškai (Reglamento preambulės 32 p.). Duomenų valdytojas turi galėti įrodyti, kad duomenų subjektas davė sutikimą, kad būtų tvarkomi jo asmens duomenys (Reglamento 7 str. 1 d.). Be to, kai informacinės visuomenės paslaugos siūlomos vaikui iki 16 metų, sutikimas turi būti duotas vaiko tėvų. Tiesa, valstybės narės gali numatyti jaunesnio amžiaus ribą, bet ne mažiau nei 13 metų (Reglamento 8 str. 1 d.). Dėl visų šių reikalavimų organizacijoms bus sunkiau gauti sutikimą.

Reglamentu yra sustiprinamos duomenų subjektų teisės. Kai kurios senosios teisės yra išplečiamos ir detaliau reglamentuojamos. Taip pat suteikiama visiškai nauja teisė – teisė į duomenų perkeliamumą, pagal kurią duomenų subjektas turi teisę gauti su juo susijusius asmens duomenis, kuriuos jis pateikė duomenų valdytojui susistemintu, įprastai naudojamu ir kompiuterio skaitomu formatu, ir turi teisę persiųsti tuos duomenis kitam duomenų valdytojui (Reglamento 20 str. 1 d.).

Naujasis reguliavimas leidžia išskirti dar vieną principą – pritaikytosios ir standartizuotosios duomenų apsaugos. Duomenų valdytojas, tiek nustatydamas duomenų tvarkymo priemones, tiek paties duomenų tvarkymo metu, turi įgyvendinti tinkamas technines ir organizacines priemones, kuriomis užtikrinamas veiksmingas duomenų apsaugos teisės įgyvendinimas (Reglamento 25 str. 1 d.). Šis principas reiškia, jog atitikimas duomenų apsaugos taisyklėms turi būti svarstomas dar iki pradedant taikyti naujus duomenų tvarkymo būdus.

Reglamentas detaliai reglamentuoja taisykles, susijusias su asmens duomenų perdavimu į trečiąsias valstybes arba tarptautinėms organizacijoms. Toks perdavimas bus įmanomas tik tuo atveju, jeigu valstybė arba tarptautinė organizacija, kuriai ketinama perduoti asmens duomenis, užtikrina tinkamo lygio asmens duomenų apsaugą (Reglamento 45 str. 1 d.). Tai turėtų paveikti duomenų apsaugos teisės plėtrą už ES ribų ir paspartinti globalią duomenų apsaugos teisės europeizaciją, kadangi kitos valstybės ir jų organizacijos,

norėdamos naudotis ES esančių asmenų duomenimis, turės suvienodinti duomenų apsaugos reguliavimą su ES standartais.[85]

Taip pat įtvirtinamas vieno langelio principas, pagal kurį vadovaujanti priežiūros institucija yra vienintelė institucija, su kuria duomenų valdytojas arba duomenų tvarkytojas palaiko ryšius, kai jie vykdo tarpvalstybinį duomenų tvarkymą (Reglamento 56 str. 6 d.). Be to, Reglamentu įsteigiama Europos duomenų apsaugos valdyba, kuri perims 29 str. darbo grupės pareigas ir užtikrins nuoseklų Reglamento taikymą (Reglamento 68 str. 1 d.).

Dar viena didelė naujovė – numatomos didžiulės administracinės baudos už Reglamento reikalavimų pažeidimus. Duomenų valdytojai, siekdami išvengti iki 20 000 000 EUR (įmonės atveju – iki 4 % jos ankstesnių finansinių metų bendros metinės pasaulinės apyvartos) siekiančios administracinės baudos, bus skatinami atidžiai laikytis jiems skirtų įsipareigojimų (Reglamento 83 str. 5 d.).

Reglamentas įtvirtina išties daug naujų pareigų duomenų valdytojams: pranešimas apie asmens duomenų saugumo pažeidimą, poveikio duomenų apsaugai vertinimas, išankstinės konsultacijos su priežiūros institucija, duomenų apsaugos pareigūno skyrimas. Visos šios pareigos kartu su duomenų subjekto teisėmis dėl jų didelės svarbos duomenų apsaugos teisei išsamiai nagrinėjamos tolesnėse šio darbo dalyse.

2.2. Duomenų subjekto teisių naujovės

Pagal dabartinį reguliavimą Duomenų apsaugos direktyva suteikia šias Duomenų apsaugos įstatymo 23 str. 1 d. įtvirtintas duomenų subjekto teises:

1) žinoti (būti informuotas) apie savo asmens duomenų tvarkymą;
2) susipažinti su savo asmens duomenimis ir kaip jie yra tvarkomi;
3) reikalauti ištaisyti, sunaikinti (ištrinti) savo asmens duomenis arba sustabdyti (blokuoti), išskyrus saugojimą, savo asmens duomenų tvarkymo veiksmus, kai duomenys tvarkomi nesilaikant įstatymų nuostatų;
4) nesutikti, kad būtų tvarkomi jo asmens duomenys.[86]

[85] ZALESKIS, Julius. ES Bendrasis duomenų apsaugos reglamentas: reikšmė duomenų apsaugos teisei. *Teisė*, 2017, t. 103, p. 48-49.
[86] Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas (su pakeitimais ir papildymais). *Valstybės žinios*, 1996, nr. 63-1479.

Reglamentas šias duomenų subjekto teises dar labiau sustiprina ir išplečia jų turinį. Be to, kaip teigia Valstybinė duomenų apsaugos inspekcija, Reglamentas duomenų subjektui suteikia tris naujas teises:

1) teisę reikalauti ištrinti duomenis (teisė būti pamirštam);
2) teisę apriboti duomenų tvarkymą;
3) teisę į duomenų perkeliamumą.[87]

Tačiau iš šių trijų teisių vos viena yra visiškai nauja duomenų subjekto teisė – tai teisė į duomenų perkeliamumą. Kitos dvi teisės – teisė būti pamirštam ir teisė apriboti duomenų tvarkymą – yra tik išplėstos ir detaliau reglamentuotos, tačiau jų pagrindai įtvirtinti ir dabar galiojančioje Duomenų apsaugos direktyvoje (12 str.). Todėl šias teises galima būtų vadinti iš dalies naujomis duomenų subjekto teisėmis.

Pirmiausia, Reglamentas įpareigoja duomenų valdytojus visą su duomenų tvarkymu susijusią informaciją duomenų subjektui pateikti glausta, skaidria, suprantama ir lengvai prieinama forma, aiškia ir paprasta kalba, ypač jei informacija yra konkrečiai skirta vaikui (Reglamento 12 str. 1 d.). Dabartiniai ES valstybių narių nacionaliniai įstatymai turi panašius reikalavimus, tačiau įsigaliojus Reglamentui ši duomenų valdytojo pareiga bus įtvirtinta eksplicitiškai.

Antra, Reglamentas duomenų valdytojui nustato konkretų terminą imtis veiksmų, susijusių su duomenų subjekto teisių įgyvendinimu. Pagal naująjį reguliavimą duomenų valdytojas privalės nepagrįstai nedelsdamas, bet ne vėliau kaip per vieną mėnesį nuo prašymo gavimo, pateikti duomenų subjektui informaciją apie veiksmus, kurių buvo imtasi gavus prašymą dėl duomenų subjekto teisių įgyvendinimo (Reglamento 12 str. 3 d.). Toks reikalavimas padidina duomenų valdytojo pareigų vykdymo efektyvumą.

Teisė žinoti, būti informuotam apie asmens duomenų tvarkymą iš esmės nesikeičia. Ir dabartinis reguliavimas reikalauja duomenų subjektui pateikti bent minimalią informaciją, susijusią su jo duomenų tvarkymo tikslais. Duomenų subjektui taip pat turi būti atskleidžiama duomenų valdytojo tapatybė bei kontaktiniai duomenys. Vienintelis pokytis yra tai, jog Reglamentas reikalauja duomenų valdytojo pateikti informaciją ne tik duomenų tvarkymo sąžiningumui, bet ir skaidrumui užtikrinti (Reglamento 13 str. 2 d.).

[87] Valstybinė duomenų apsaugos inspekcija. *Jūsų teisės asmens duomenų apsaugos srityje*. (viešoji konsultacija), 2017 m. liepos 11 d. [interaktyvus; žiūrėta 2018 m. sausio 14 d.]. Prieiga per internetą: <https://www.ada.lt/go.php/JUSU-TEISES770>.

Teisės susipažinti su savo asmens duomenimis turinys pagal naująjį reguliavimą yra išplečiamas. Reglamentas (15 str. 1 d.) įtvirtina naujas kategorijas informacijos, kurios gali reikalauti duomenų subjektai:

- numatomas asmens duomenų saugojimo laikotarpis, kai jį numatyti yra įmanoma, arba kriterijai, taikomi tam laikotarpiui nustatyti, jeigu saugojimo laikotarpio numatyti nėra įmanoma;
- teisė prašyti duomenų valdytojo ištaisyti asmens duomenis arba juos ištrinti ar apriboti su duomenų subjektu susijusių asmens duomenų tvarkymą arba nesutikti su tokiu tvarkymu;
- teisė pateikti skundą priežiūros institucijai;
- visa turima informacija apie asmens duomenų rinkimo šaltinius, kai šie duomenys renkami ne iš duomenų subjekto.[88]

Šie reikalavimai galimai sukels didesnę administracinę naštą duomenų valdytojams, tačiau didesnis duomenų subjektų informuotumas užtikrina efektyvesnį jų teisių užtikrinimą. Be to, duomenų valdytojai įpareigojami daugeliu atvejų suteikti informaciją duomenų subjektams nemokamai, išskyrus išimtis, jeigu duomenų subjektas šia galimybe piktnaudžiautų (pavyzdžiui, pakartotiniai prašymai ar nepagrįsti prašymai).

Teisė reikalauti ištaisyti duomenis išlieka nepakitusi, tuo tarpu teisė nesutikti su asmens duomenų tvarkymu keičiasi iš esmės. Reglamentas perkelia įrodinėjimo naštą duomenų valdytojui. Nuo šiol ne duomenų subjektas turės įrodyti, kad duomenų tvarkymui prieštaraujama pagrįstai, o duomenų valdytojas, norėdamas toliau tvarkyti asmens duomenis, privalės įrodyti, kad duomenys tvarkomi dėl įtikinamų teisėtų priežasčių, kurios yra viršesnės už duomenų subjekto interesus, teises ir laisves, arba siekiant pareikšti, vykdyti ar apginti teisinius reikalavimus (Reglamento 21 str. 1 d.).

Likusios trys teisės – teisė reikalauti ištrinti duomenis (teisė būti pamirštam), teisė apriboti duomenų tvarkymą ir teisė į duomenų perkeliamumą – bus analizuojamos atskirai dėl savo naujumo ir itin didelės svarbos duomenų subjektui bei duomenų teisės sistemai apskritai.

[88] 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). *OL* L 119, 2016 5 4, p. 43.

2.2.1. Teisė reikalauti ištrinti duomenis (teisė būti pamirštam)

Teisė reikalauti ištrinti duomenis, kuri dar yra vadinama teise būti pamirštam, nėra visiškai nauja duomenų subjekto teisė. Jos pagrindai atsirado būtent Europos Sąjungoje ir buvo įtvirtinti dar 1995 m. Duomenų apsaugos direktyvoje.[89] Taigi, nors Reglamentas išplečia ir detalizuoja teisę būti pamirštam, asmenys ir pagal dabartinį teisinį reguliavimą gali pasinaudoti šia teise, kuri yra suteikiama Duomenų apsaugos direktyvos 12 ir 14 straipsniuose[90].

Pagal Duomenų apsaugos direktyvos 12 str. valstybės narės garantuoja kiekvienam duomenų subjektui teisę reikalauti, kad duomenų valdytojas ištrintų duomenis, kurie yra tvarkomi nesilaikant teisės akto nuostatų, ypač, kai tie duomenys yra neišsamūs arba netikslūs. Tuo tarpu Duomenų apsaugos direktyvos 14 str. nurodo, jog duomenų subjektas gali prieštarauti duomenų apie jį tvarkymui, jeigu turi tam su jo konkrečia padėtimi susijusį teisėtą pagrindą, ir tuo atveju, kai prieštaravimas yra pagrįstas, tie duomenys nebegali būti toliau tvarkomi.

Lietuvos Respublikos teisės sistemoje duomenų subjektas gali reikalauti sunaikinti savo asmens duomenis pagal Duomenų apsaugos įstatymo 23 str. 1 d. 3 p. bei 26 str.[91]. Taip pat teisės būti pamirštam principas įkūnijamas ir Lietuvos Respublikos civilinio kodekso 2.22 str., 2.23 str. nuostatose[92], garantuojančiose individo teisę į atvaizdo, privataus gyvenimo ir jo slaptumo apsaugą[93].

Teisės būti pamirštam turinio plėtra

Teisė būti pamirštam yra neatsiejama nuo interneto ir skaitmeninių technologijų plėtros.[94] Skaitmeninių technologijų dėka internete nuolat daugėja asmeninės informacijos. Tai sudaro ne tik žiniasklaidos talpinama informacija, tačiau ir pačių duomenų subjektų įkeliami asmens duomenys. Visa ši informacija tuo pačiu metu gali būti kaupiama skirtingose vietose ir jos mastas gali būti didžiulis. Kartais net ir vienos asmeninės detalės

[89] NEVILLE, Andrew. Is it a Human Right to be Forgotten? Conceptualizing the World View. *Santa Clara Journal of International Law*, 2017, Vol. 15, No. 2, p. 160.
[90] DE TERWANGNE, Cecile. *Internet Privacy and the Right to Be Forgotten/Right to Oblivion*. 2012, No. 13, p. 115.
[91] Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas (su pakeitimais ir papildymais). *Valstybės žinios*, 1996, nr. 63-1479.
[92] Lietuvos Respublikos civilinis kodeksas. *Valstybės žinios*, 2000, nr. 74-2262.
[93] CIVILKA, Mindaugas. *Teisė būti pamirštam: mitologija ir tikrovė*. 2016. [interaktyvus; žiūrėta 2018 m. vasario 4 d.]. Prieiga per internetą: <https://www.linkedin.com/pulse/teis%C4%97-b%C5%ABti-pamir%C5%A1tam-mitologija-ir-tikrov%C4%97-mindaugas-civilka>.
[94] CASTELLANO, Pere Simon. The right to be forgotten under European Law: a Constitutional debate. *Lex Electronica*, 2012, vol. 16.1, p. 24.

viešas egzistavimas internete gali prieštarauti teisei į privatų gyvenimą, pažeisti teisę į orumą ar sugriauti reputaciją[95]. Šios problemos sprendimas yra svarbus ypač tada, kai daugybę metų internete viešinama informacija yra praradusi aktualumą, tikslumą ir reikšmingumą.

Teisė būti pamirštam didesnio dėmesio sulaukė 2014 metais, Europos Sąjungos Teisingumo Teismui priėmus sprendimą byloje C-131/12 (*Google Spain SL ir Google Inc. prieš Agencia Española de Protección de Datos (AEPD) ir Mario Costeja González*[96]), kurioje buvo pripažinta duomenų subjektų teisė reikalauti paieškos variklio eksploatuotojo, kuris yra laikytinas duomenų valdytoju, kad būtų pašalintos su duomenų subjektu susijusios nuorodos. Ši byla iki šiol yra laikoma viena svarbiausių bylų Europos Sąjungos Teisingumo Teismo praktikoje, susijusių ne tik su teise reikalauti ištrinti duomenis, bet ir duomenų apsaugos srityje apskritai[97]. Sprendimu išplečiamos esamos duomenų subjektų galimybės remiantis galiojančia Duomenų apsaugos direktyva naudotis savo teise reikalauti ištrinti duomenis[98].

Pagrindinėje byloje Ispanijos pilietis M. Costeja González kreipėsi į Ispanijos Duomenų apsaugos agentūrą su prašymu įpareigoti dienraštį *La Vanguardia* arba panaikinti puslapius, kuriuose minimas M. Costeja González asmenvardis, apie areštuoto nekilnojamojo turto pardavimo aukcioną, vykdomą išieškant socialinės apsaugos srities skolą, arba pakeisti taip, kad juose nebeliktų jo asmens duomenų. Jis taip pat prašė įpareigoti *Google Spain* arba *Google Inc*. pašalinti arba paslėpti jo asmens duomenis, kad šie nebūtų pateikiami paieškos rezultatų sąraše ir nuorodose į *La Vanguardia*. Prašymai buvo grindžiami tuo, jog visa skola, dėl kurios jam taikytas areštas, jau buvo sumokėta prieš daug metų ir nebėra poreikio toliau jį minėti.[99]

Ispanijos Duomenų apsaugos agentūra atmetė skundo dalį, susijusią su *La Vanguardia*, nes atitinkama informacija šiame laikraštyje buvo paskelbta teisėtai, siekiant kiek įmanoma didesnio rengiamo aukciono žinomumo, tačiau skundo dalis, susijusi su *Google* buvo

---

[95] VAN HOBOKEN, Joris. *The Proposed Right to be Forgotten Seen from the Perspective of Our Right to Remember, Freedom of Expression Safeguards in a Converging Information Environment (Prepared for the European Commission)*. Amsterdam, 2013, p. 4.

[96] Europos Sąjungos Teisingumo Teismas. 2014 m. gegužės 13 d. sprendimas byloje *Google Spain SL ir Google Inc. Prieš Agencia Española de Protección de Datos (AEPD) ir Mario Costeja González* C-131/12, EU:C:2014:317.

[97] European Anti-Fraud Office. *OLAF Data Protection Officer: Summaries of EU Court Decisions Relating to Data Protection 2000-2015*. Belgium, 2016, p. 44.

[98] Europos Sąjungos Taryba. Pirmininkaujančios valstybės narės pranešimas Nuolatinių atstovų komitetui / Tarybai. *Teisė būti pamirštam ir Teisingumo Teismo sprendimas dėl „Google" – Politiniai debatai*. Briuselis, 2014, Nr. 13619/14.

[99] Europos Sąjungos Teisingumo Teismas. 2014 m. gegužės 13 d. sprendimas byloje *Google Spain SL ir Google Inc. Prieš Agencia Española de Protección de Datos (AEPD) ir Mario Costeja González* C-131/12, EU:C:2014:317. 14-15 punktai.

patenkinta. Buvo nuspręsta, jog paieškos variklių eksploatuotojai yra duomenų valdytojai ir privalo sunaikinti duomenis bei uždrausti prieigą prie tam tikrų duomenų, kai jų sklaida gali kelti pavojų pagrindinei teisei į asmens duomenų apsaugą ir apskritai asmens orumui.[100]

Europos Sąjungos Teisingumo Teismas iš pradžių pasisakė, kad paieškos variklio veikimo operacijos, kurias sudaro internete trečiųjų asmenų paskelbtos ar jau esančios informacijos suradimas ir galiausiai padarymas prieinamos interneto naudotojams tam tikra pasirinkta tvarka, laikytinos asmens duomenų tvarkymu. Be to, paieškos variklio eksploatuotojas laikytinas tokių duomenų „valdytoju“, kadangi jo veikla padidina duomenų matomumą, todėl jis, kaip asmuo, kuris nustato šios veiklos tikslus ir būdus, turi užtikrinti, kad jo veikla atitiktų duomenų apsaugos įstatymų reikalavimus ir kad duomenų subjekto teisės į privataus gyvenimo gerbimą apsauga būtų įgyvendinta.[101]

Buvo pabrėžta, jog asmens duomenų tvarkymas, kurį vykdo paieškos variklių eksploatuotojas, gali daryti didelį neigiamą poveikį pagrindinėms teisėms į privatų gyvenimą ir asmens duomenų apsaugą tais atvejais, kai paieška per šį paieškos variklį atliekama panaudojant fizinio asmens asmenvardį, nes dėl tokio tvarkymo kiekvienas internautas kartu su paieškos rezultatų sąrašu gali gauti struktūruotą asmens apžvalgą ir taip sudaryti daugiau ar mažiau išsamų duomenų subjekto profilį.[102] Dar didesnį neigiamą poveikį daro tai, jog interneto svetainių turinys pasiekiamas neriboto interneto vartotojų skaičiaus ir iš bet kurios pasaulio vietos[103].

Svarstant duomenų subjekto prašymą ištrinti duomenis, reikia nustatyti teisingą internautų teisėto intereso gauti informaciją ir Europos Sąjungos pagrindinių teisių chartijos 7 ir 8 straipsniuose įtvirtintų duomenų subjekto teisių pusiausvyrą. Nors paprastai duomenų subjekto teisės yra viršesnės, tačiau kiekvienu atveju situaciją reikia vertinti atsižvelgiant į šiuos veiksnius:

- informacijos pobūdis;
- informacijos ypatingumas duomenų subjekto privačiam gyvenimui;
- visuomenės interesas gauti prieigą prie informacijos;

[100] Europos Sąjungos Teisingumo Teismas. 2014 m. gegužės 13 d. sprendimas byloje *Google Spain SL ir Google Inc. Prieš Agencia Española de Protección de Datos (AEPD) ir Mario Costeja González* C-131/12, EU:C:2014:317. 16-17 punktai.
[101] Ibid., 41 p.
[102] Ibid., 80 p.
[103] Europos Sąjungos Teisingumo Teismas. 2011 m. spalio 25 d. sprendimas sujungtose bylose *eDate Advertising GmbH prieš X ir Olivier Martinez, Robert Martinez prieš MGN Limited* C-509/09 ir C-161/10, EU:C:2011:685. 45 p.

- duomenų subjekto padėtis viešajame gyvenime.[104]

Galiausiai buvo pasakyta, jog pagal Duomenų apsaugos direktyvą paieškos variklio eksploatuotojas gali turėti pareigą pašalinti nuorodas į trečiųjų asmenų paskelbtus tinklalapius net ir tais atvejais, kai informacija su asmens duomenimis nėra ištrinama iš šių tinklalapių bei kai duomenys šiuose tinklalapiuose paskelbti teisėtai[105]. Net iš pradžių teisėtas tikslių duomenų tvarkymas, praėjus tam tikram laikui, gali tapti neatitinkantis Duomenų apsaugos direktyvos, jei duomenys nebereikalingi tais tikslais, dėl kurių buvo surinkti arba tvarkomi ar informacija yra neadekvati, nereikšminga ar nebereikšminga arba perteklinė[106]. Tuomet gali būti reikalaujama tokio pobūdžio duomenis ištrinti.

Taigi, nors Europos Sąjungos Teisingumo Teismas išaiškino Duomenų apsaugos direktyvos suteikiamas galimybes prašyti ištrinti asmens duomenis, šie išaiškinimai buvo pateikti atsižvelgiant tik į internetinės paieškos variklio eksploatuotojo pareigas. Galima teigti, jog pagal šį sprendimą būtų tik apsunkinama asmens duomenų prieiga per paieškos sistemas, tačiau teisė būti pamirštam nėra absoliučiai įgyvendinama. Tačiau šio sprendimo dėka viena populiariausių internetinės paieškos sistemų – *Google* – sukūrė formą,[107] skirtą paieškoje indeksuoto turinio pašalinimo užklausai pateikti, kuria jau naudojasi daugybė duomenų subjektų, įgyvendindami savo teisę reikalauti ištrinti asmens duomenis.

Reguliavimo pokyčiai

Reglamentas išplečia teisės būti pamirštam turinį, lyginant su iki dabar galiojančia Duomenų apsaugos direktyva. Pirmiausia, Reglamentas eksplicitiškai įtvirtina teisę būti pamirštam (teisę reikalauti ištrinti duomenis). Antra, nurodomi konkretūs pagrindai, kuriais vadovaudamasis duomenų subjektas turi teisę reikalauti, kad duomenų valdytojas nepagrįstai nedelsdamas ištrintų su juo susijusius asmens duomenis, o duomenų valdytojas yra įpareigotas nepagrįstai nedelsdamas ištrinti asmens duomenis:

1) asmens duomenys nebėra reikalingi tiems tikslams, kuriems duomenys buvo renkami ar kitaip tvarkomi, pasiekti;
2) asmens duomenų subjektas atšaukia sutikimą, kuriuo grindžiamas duomenų tvarkymas, ir nėra jokio kito teisinio pagrindo tiems duomenims tvarkyti;

[104] Europos Sąjungos Teisingumo Teismas. 2014 m. gegužės 13 d. sprendimas byloje Google Spain SL ir Google Inc. Prieš Agencia Española de Protección de Datos (AEPD) ir Mario Costeja González C-131/12, EU:C:2014:317. 81 p.
[105] Ibid., 88 p.
[106] Ibid., 93-94 p.
[107] Google. *Paieškoje indeksuoto turinio pašalinimo užklausa, pateikta atsižvelgiant į Europos duomenų apsaugos įstatymus*. [interaktyvus; žiūrėta 2018 m. vasario 5 d.]. Prieiga per internetą: <https://www.google.com/webmasters/tools/legal-removal-request?complaint_type=rtbf&visit_id=1-636557183438938250-1427818002&hl=lt&rd=1>.

3) asmens duomenų subjektas nesutinka su duomenų tvarkymu ir nėra viršesnių teisėtų priežasčių tuos duomenis tvarkyti;
4) asmens duomenys buvo tvarkomi neteisėtai;
5) asmens duomenys turi būti ištrinti laikantis teisinės prievolės, nustatytos Europos Sąjungos arba valstybės narės teisėje, kuri yra taikoma duomenų valdytojui;
6) asmens duomenys buvo surinkti informacinės visuomenės paslaugų siūlymo kontekste[108].[109]

Naujuoju reguliavimu išplečiamas teisės būti pamirštam turinys lemia tai, jog organizacijos susidurs su daugiau ir įvairesnių prašymų ištrinti duomenis. Tam, kad būtų pasiruošusios įgyvendinti duomenų subjekto teisę būti pamirštam, organizacijos turi užtikrinti, jog procesai ir techniniai sprendimai, reikalingi asmens duomenų ištrynimui būtų tinkamai pritaikyti šiam tikslui pasiekti per numatytą laikotarpį[110]. Taip pat organizacija (duomenų valdytojas) privalo užtikrinti, kad, iškilus pareigai ištrinti asmens duomenis, apie tai turi būti informuoti ir kiti tuos duomenis tvarkantys duomenų valdytojai. Kad ši pareiga būtų tinkamai įgyvendinta, duomenų valdytojas turi pasirūpinti, jog duomenų kaupimo sistema įtrauktų informaciją ir apie tai, su kuriais trečiaisiais asmenimis šia informacija yra dalinamasi.

Tai reiškia, jog kai asmens duomenys yra paskelbti viešai, bet duomenų valdytojas turi pareigą šiuos duomenis ištrinti, jis, atsižvelgdamas į turimas technologijas ir įgyvendinimo sąnaudas, imasi pagrįstų veiksmų, įskaitant technines priemones, kad informuotų duomenis tvarkančius duomenų valdytojus apie duomenų subjekto prašymą tokiems duomenų valdytojams ištrinti visas nuorodas į tuos asmens duomenis arba jų kopijas ar dublikatus (Reglamento 17 str. 2 d.). Tačiau duomenų valdytojas atleidžiamas nuo pareigos informuoti trečiuosius asmenis, jeigu toks informavimas yra neįmanomas arba reikalaujantis neproporcionaliai didelių pastangų[111].

[108] Bendrojo duomenų apsaugos reglamento 8 straipsnio (Sąlygos, taikomos vaiko, kuriam siūlomos informacinės visuomenės paslaugos, sutikimui) 1 d.: Kai taikomas 6 straipsnio 1 dalies a punktas, kai tai susiję su informacinės visuomenės paslaugų tiesioginiu siūlymu vaikui, vaiko asmens duomenų tvarkymas yra teisėtas tik tuo atveju, jei vaikas yra bent 16 metų amžiaus. Kai vaikas yra jaunesnis nei 16 metų, toks tvarkymas yra teisėtas tik tuo atveju, jeigu tą sutikimą davė arba tvarkyti duomenis leido vaiko tėvų pareigų turėtojas, ir tokiu mastu, kokiu duotas toks sutikimas ar leidimas.
[109] 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). *OL* L 119, 2016 5 4, p. 43-44.
[110] TIKKINEN-PIRI, Christina; ROHUNEN, Anna; MARKKULA, Jouni. EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law and Security Review*, 2018, t. 34, p. 150.
[111] DOWNING, Robbie. Overview of EU General Data Protection Regulation. *Thomson Reuters*, 2017, p. 22.

Taigi, Reglamentas sustiprina teisę į duomenų ištrynimą nustatydamas organizacijoms, ypač veikiančioms internete, kurios asmens duomenis paskelbia viešai, pareigą informuoti kitus duomenis tvarkančius duomenų valdytojus, kad šie taip pat ištrintų nuorodas į šiuos duomenis, jų kopijas ar dublikatus. Šis procesas nėra paprastas ir daugiausiai sunkumų galimai sukelsiantis socialinių tinklų ir įvairių naujienų tinklalapių valdytojams.

Teisei reikalauti ištrinti duomenis yra keliami papildomi saugumo reikalavimai, kai tai yra susiję su vaikų duomenimis. Reglamentas sustiprina vaikų asmens duomenų apsaugą ypač internetinėje erdvėje.[112] Organizacijos, apdorojančios vaikų asmens duomenis, privalo ypač didelį dėmesį skirti situacijoms, kai vaikas duoda sutikimą savo duomenų tvarkymui, tačiau vėliau reikalauja savo duomenis ištrinti. Šiuo atveju nėra svarbu, kokio amžiaus asmuo pateikia šį prašymą. Svarbiausias yra sutikimo duomenų tvarkymui davimo momentas.

Pagal Reglamento preambulės 65 punktą, duomenų subjekto teisė reikalauti, kad jo asmens duomenys būtų ištrinti, yra ypač svarbi tais atvejais, kai duomenų subjektas sutikimą duomenų tvarkymui išreiškė būdamas vaikas ir nevisiškai suvokdamas su duomenų tvarkymu susijusius pavojus, o vėliau nori, kad tokie – ypač internete saugomi – asmens duomenys būtų pašalinti. Duomenų subjektas turėtų galėti naudotis ta teise, nepaisant to, kad jis nebėra vaikas (Reglamento preambulės 65 p.).

Šis reguliavimas yra ypač aktualus, kai tai susiję su vaikų elgesiu socialiniuose tinkluose. Pavyzdžiui, asmuo, būdamas vaikas, neįvertina galimo savo veiksmų poveikio privatumui ir į *Facebook* socialinį tinklą patalpina asmens duomenis, kurių po daugelio metų jis nebenorėtų skelbti viešai, todėl jis turi galimybę pasinaudoti naujuoju Reglamente įtvirtintu reguliavimu įgyvendinti savo teisei būti pamirštam.

Nors Reglamentas žymiai išplėtė duomenų subjekto teisės būti pamirštam turinį, ši teisė nėra absoliuti. Duomenų ištrynimas turi būti suderintas su kitomis teisėmis ir laisvėmis, ypač su informacijos laisve ir viešuoju interesu. Reglamentas nustato penkias sąlygas, pagal kurias gali būti atsisakoma tenkinti reikalavimą ištrinti asmens duomenis, jeigu duomenų tvarkymas yra būtinas:

1) siekiant naudotis teise į saviraiškos ir informacijos laisvę;
2) siekiant laikytis duomenų valdytojui skirtos teisinės prievolės, nustatytos Europos Sąjungos ar valstybės narės teisėje, pagal kurią yra reikalaujama tvarkyti duomenis, arba siekiant atlikti užduotį, vykdomą viešojo intereso labui, arba vykdant duomenų valdytojui pavestas viešosios valdžios funkcijas;

[112] MACENAITE, Milda. From universal towards child-specific protection of the right to privacy online: Dilemmas in the EU General Data Protection Regulation. *New Media and Society*, 2017, Vol. 19(5), 766.

3) dėl viešojo intereso priežasčių visuomenės sveikatos srityje;
4) archyvavimo tikslais viešojo intereso labui, mokslinių ar istorinių tyrimų tikslais arba statistiniais tikslais, jeigu dėl teisės reikalauti ištrinti duomenis gali tapti neįmanoma arba ji gali labai sukliudyti pasiekti to tvarkymo tikslus;
5) siekiant pareikšti, vykdyti arba apginti teisinius reikalavimus.[113]

Pavyzdžiui, paieškos sistemos valdytojas informuoja naujienų tinklalapius, jog duomenų subjekto reikalavimu yra ištrinami paieškos rezultatai, nurodantys į su juo susijusią informaciją tuose naujienų tinklalapiuose. Tačiau tai dar nereiškia, jog naujienų tinklalapiai taip pat turi ištrinti visą su duomenų subjektu susijusią informaciją. Jeigu naujienų tinklalapio turinys, konkrečiau, tam tikras straipsnis, yra apsaugotas saviraiškos laisvės išimtimi, numatytoje Reglamente.

Prieš tai aptartas sąrašas išimčių, ribojančių teisę reikalauti ištrinti duomenis, nėra baigtinis. Kiekviena valstybė narė gali nustatyti apribojimus, kuriais būtų suvaržoma teisė būti pamirštam, jeigu toks ribojimas būtinas ir proporcingas demokratinėje visuomenėje siekiant užtikrinti visuomenės saugumą, įskaitant žmonių gyvybių apsaugą, nusikalstamų veikų prevenciją, tyrimą ir patraukimą į baudžiamąją atsakomybę už jas ar baudžiamųjų sankcijų vykdymą (Reglamento preambulės 73 p.).

Galimi įgyvendinimo iššūkiai ir problemos

Vienas iš didžiausių iššūkių, susijusių su teise reikalauti ištrinti duomenis, gali būti tai, jog patys duomenų valdytojai turės svarstyti duomenų subjekto reikalavimą ir įvertinti, ar duomenų ištrynimas nepažeistų kitų konkuruojančių teisių, pavyzdžiui, saviraiškos ir informacijos teisės. Kitaip tariant, duomenų valdytojai turės prisiimti teisėjo vaidmenį ir jiems atiteks dar didesnė atsakomybė.

Naujasis reguliavimas, susijęs su teise reikalauti ištrinti duomenis, taip pat nėra pakankamai aiškus. Reglamente netrūksta abstrakčių sąvokų, tokių kaip *pagrįsti veiksmai, nepagrįstai nedelsdamas*, *atsižvelgiant į turimas technologijas ir įgyvendinimo sąnaudas* (Reglamento 17 str.). Didžiausias trūkumas yra tai, jog tai yra vertinamieji kriterijai, kuriems nėra pateikta išaiškinimų nei pačiame Reglamente, nei kituose teisės šaltiniuose.

[113] 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). *OL* L 119, 2016 5 4, p. 44.

Rekomendacijų, susijusių su teise būti pamirštam, nepateikia net ir 29 str. darbo grupė[114]. Todėl pareiga vertinti visus su šia teise susijusius kriterijus tenka duomenų valdytojui.

Be to, pagal greitai įsigaliosiantį naująjį reguliavimą daugybė organizacijų, ypač veikiančių skaitmeninėje erdvėje, susidurs su galimai didžiuliu kiekiu reikalavimų ištrinti asmens duomenis. Tokių reikalavimų svarstymas ir įgyvendinimas, priklausomai nuo masto, reikalaus specialių procesų sukūrimo bei gali pareikalauti nemažai lėšų iš pačių organizacijų. Nors naudojimasis teise būti pamirštam duomenų subjektui yra nemokamas, tačiau gali būti, jog organizacijos savo išlaidas, susijusias su reikalavimų ištrinti duomenis svarstymu, gali paskirstyti kitiems subjektams rinkoje. Tokiu atveju, nors ir netiesiogiai, duomenų subjektai taip pat gali patirti kainų augimą arba prekių ar teikiamų paslaugų kokybės mažėjimą.

Teisė būti pamirštam duomenų subjektui vis dėlto gali turėti ir priešingą poveikį. Tam tikrais atvejais gali egzistuoti techninė galimybė identifikuoti asmenį, pateikusį prašymą ištrinti duomenis. Tuomet kyla grėsmė, jog vietoj to, kad informacija būtų pamiršta, ji bus dar labiau eskaluojama ir viešinama.[115] Tai vadinama *Streisand* efektu, kai bandoma ką nors nuslėpti, tačiau tai išprovokuoja dar daugiau dėmesio[116]. Dėl šio galimo neigiamo teisės būti pamirštam efekto, duomenų valdytojai privalo užtikrinti, jog duomenų subjektų prašymai ištrinti duomenis bus svarstomi ir įgyvendinami laikantis konfidencialumo reikalavimų.

Taip pat svarbu pabrėžti, jog tam tikrais atvejais yra neįmanoma ištrinti visos asmeninės informacijos. Tai ypač būdinga internetui ir socialiniams tinklams. Todėl net ir įsigaliosiantis naujasis teisinis reguliavimas negarantuos galimybės duomenų subjektui būti visiškai pamirštam. Dažnu atveju tai bus tik paieškos, naudojantis paieškos varikliu, tokiu kaip *Google*, rezultato pašalinimas, tačiau pirminis šaltinis su asmens duomenimis gali išlikti. Todėl tokiu būdu nebus visiškai ištrinami asmens duomenys, bet tik ženkliai apribojama prieiga prie tų duomenų.

Tikėtina, jog daugiausiai prašymų ištrinti asmens duomenis bus pateikta socialinių tinklų valdytojams, kadangi būtent socialiniai tinklai tampa pagrindine komunikacijos priemone tarp įvairių amžiaus grupių duomenų subjektų. Tuo labiau, jog būtent

[114] Europos Komisija. *29 straipsnio darbo grupė* (internetinio puslapio skiltis) [interaktyvus; žiūrėta 2018 m. vasario 17 d.]. Prieiga per internetą: <http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083>.

[115] CIVILKA, Mindaugas. *Teisė būti pamirštam: mitologija ir tikrovė*. 2016. <https://www.linkedin.com/pulse/teis%C4%97-b%C5%ABti-pamir%C5%A1tam-mitologija-ir-tikrov%C4%97-mindaugas-civilka>.

[116] The Economist. *What is the Streisand effect?* 2013. [interaktyvus; žiūrėta 2018 m. vasario 18 d.]. Prieiga per internetą: <https://www.economist.com/blogs/economist-explains/2013/04/economist-explains-what-streisand-effect>.

socialiniuose tinkluose atskleidžiami didžiuliai kiekiai asmens duomenų. Tai patvirtina ir tai, jog šiuo metu daugiausiai prašymų ištrinti nuorodas *Google* paieškos sistemoje pateikiama būtent dėl informacijos socialiniuose tinkluose, ypač *Facebook* ir *Twitter*[117]. Todėl būtent socialiniai tinklai turi būti itin gerai pasiruošę įgyvendinti duomenų subjekto teisę reikalauti ištrinti asmens duomenis.

Apibendrinant galima teigti, jog Reglamentas išplėtė ir detalizavo teisės reikalauti ištrinti duomenis turinį. Pagal naująjį reguliavimą tai viena iš svarbiausių duomenų subjekto teisių, kurios įgyvendinimas užtikrinamas įpareigojant duomenų valdytojus laikytis jiems nurodytų pareigų ir sudaryti sąlygas duomenų subjektams naudotis savo teise, nors ji ir nėra absoliuti bei turi nemažai išimčių ir apribojimų.

Įgyvendinant šią teisę daug atsakomybės tenka duomenų valdytojams, kurie turi įvertinti daugybę aspektų, tarp jų ir turimas technologijas bei sąnaudas, prieš imdamiesi įgyvendinti duomenų subjekto teisę reikalauti ištrinti duomenis. Su šia teise taip pat yra itin glaudžiai susiję asmens duomenų tvarkymo principai, ypač tikslumo, tikslo apribojimo ir duomenų kiekio mažinimo principai. Todėl kiekvienoje situacijoje duomenų valdytojas privalo individualiai vertinti kiekvieno duomenų subjekto reikalavimą ištrinti asmens duomenis, atsižvelgdamas ir į tai, ar reikalavimo patenkinimas neprieštarautų kitiems teisiniams pagrindams.

2.2.2. Teisė apriboti duomenų tvarkymą

Teisė apriboti duomenų tvarkymą reiškia, jog šios duomenų subjekto teisės galiojimo laikotarpiu duomenų valdytojas gali tik saugoti asmens duomenis, tačiau negali jų tvarkyti. Tais atvejais, kai duomenų subjektas neatitinka visų reikalavimų, sudarančių galimybę pasinaudoti teise reikalauti ištrinti asmens duomenis, arba dėl tam tikrų priežasčių nenori, kad jo duomenys būti visiškai ištrinti, teisė apriboti tų duomenų tvarkymą gali tapti alternatyva.[118] Tačiau bet kuriuo atveju ši teisė automatiškai nereiškia, jog asmens duomenys turi būti ar bus ištrinti. Teise siekiama tik apriboti duomenų tvarkymą, o ne juos ištrinti.

[117] Google. *Skaidrumo ataskaita: Paieškos rezultatų pašalinimas dėl Europos privatumo įstatymo pažeidimų*. [interaktyvus; žiūrėta 2018 m. vasario 18 d.]. Prieiga per internetą: <https://transparencyreport.google.com/eu-privacy/overview>.

[118] TIKKINEN-PIRI, Christina; ROHUNEN, Anna; MARKKULA, Jouni. EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law and Security Review*, 2018, t. 34, p. 140.

Pagal dabartinį duomenų apsaugos reguliavimą teisė apriboti duomenų tvarkymą nėra įtvirtinta eksplicitiškai. Tačiau šios teisės pagrindus galima įžvelgti Duomenų apsaugos direktyvos 12 str. b) dalyje, pagal kurią duomenų subjektai gali duomenų valdytojo reikalauti, kad šis blokuotų asmens duomenis, jeigu jie tvarkomi nesilaikant direktyvoje įtvirtintų reikalavimų, ypač tais atvejais, kai duomenys yra neišsamūs ar netikslūs. Duomenų apsaugos direktyvą įgyvendinančio Duomenų apsaugos įstatymo 23 str. minimas asmens duomenų tvarkymo veiksmų, išskyrus saugojimą, sustabdymas, kai duomenų tvarkymas prieštarauja įstatymo nuostatoms.[119]

Išanalizavus Duomenų apsaugos direktyvos ir Duomenų apsaugos įstatymo nuostatas, galima daryti išvadą, jog Reglamente įtvirtinta teisė apriboti duomenų tvarkymą atitinka dabar suteikiamą teisę blokuoti duomenis ar sustabdyti duomenų tvarkymo veiksmus. Tačiau pagal dabartinį reguliavimą apie tokias galimybes tik užsimenama, tuo tarpu Reglamentas teisę apriboti duomenų tvarkymą įtvirtina eksplicitiškai ir išsamiai ją detalizuoja.

Pagal Reglamento 18 str. 1 d. duomenų subjektas gali reikalauti duomenų valdytojo, kad jo asmens duomenų tvarkymas būtų apribotas esant vienam iš šių atvejų:

- duomenų subjektas užginčija duomenų tikslumą (šiuo atveju duomenų tvarkymas apribojimas laikotarpiui, per kurį duomenų valdytojas turi galimybę patikrinti tų duomenų tikslumą);
- asmens duomenų tvarkymas yra neteisėtas, tačiau duomenų subjektas nesutinka su duomenų ištrynimu ir vietoj to siekia apriboti tų duomenų naudojimą;
- asmens duomenų nebereikia pradiniam duomenų tvarkymo tikslui pasiekti, tačiau jų negalima ištrinti dėl teisinių pagrindų (kai duomenų subjektui reikia tų duomenų kaip įrodymų siekiant pareikšti, vykdyti arba apginti teisinius reikalavimus);
- duomenų subjektas nesutinka su jo asmens duomenų tvarkymu (šiuo atveju duomenų tvarkymas apribojamas laikotarpiui, per kurį duomenų valdytojas turi galimybę patikrinti, ar jo teisėtos priežastys yra viršesnės už duomenų subjekto priežastis).

Kai asmens duomenys yra apribojami pagal vieną iš šių atvejų, tie duomenys gali būti tik saugomi, nebent duomenų subjektas duoda aiškų sutikimą jiems tvarkyti. Taip pat Reglamentas (18 str. 2 d.) numato dar tris atvejus, pagal kuriuos duomenų valdytojas gali tvarkyti apribotus asmens duomenis:

[119] Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas (su pakeitimais ir papildymais). *Valstybės žinios*, 1996, nr. 63-1479.

- siekiant pareikšti, vykdyti arba apginti teisinius reikalavimus;
- siekiant apsaugoti kito fizinio ar juridinio asmens teises;
- dėl svarbaus Europos Sąjungos arba valstybės narės viešojo intereso priežasčių.[120]

Tačiau yra svarbu pabrėžti, jog prieš panaikindamas duomenų tvarkymo apribojimą, duomenų valdytojas privalo apie tai informuoti duomenų subjektą (Reglamento 18 str. 3 d.).

Tuo metu, kai asmens duomenų tvarkymas yra apribotas, tie duomenys turi būti saugomi atskiroje sistemoje, nesupainiojant šių duomenų su neapriboto tvarkymo duomenimis, arba turi būti blokuojami kokiu nors kitu techniniu būdu.[121] Reglamento preambulės 67 punktas nurodo šiuos galimus asmens duomenų tvarkymo ribojimo būdus:

- laikinas atrinktų apribotų asmens duomenų perkėlimas į kitą tvarkymo sistemą;
- atrinktų apribotų asmens duomenų prieinamumo naudotojams blokavimas ar išėmimas iš interneto svetainės.

Iš to galima pastebėti, jog tokių veiksmų tikslas yra panaikinti galimybes apribotus duomenis tvarkyti ar kaip nors juos pakeisti. Bet kuriuo atveju asmens duomenų tvarkymo apribojimas privalo būti aiškiai nurodytas. Pavyzdžiui, asmeniui keičiant banką galima reikalauti, kad senasis bankas uždarytų asmens sąskaitas ir ištrintų visus su juo susijusius duomenis. Tačiau šiam bankui gali būti taikomas įstatymas, pagal kurį bankas turi pareigą saugoti klientų duomenis 10 metų laikotarpiui. Tai reiškia, jog bankas vykdo teisinį reikalavimą ir neturi teisės asmens duomenų ištrinti.[122] Tokiu atveju duomenų subjektas gali prašyti apriboti savo asmens duomenų tvarkymą ir pasinaudoti alternatyvia teise duomenų ištrynimui.

Taigi, teisė apriboti duomenų tvarkymą yra svarbi dėl to, jog šios teisės dėka duomenų subjektas gali būti užtikrintas, kad jo asmens duomenys nebus tvarkomi tol, kol sprendžiami svarbūs su duomenų subjekto teisėmis susiję klausimai, pavyzdžiui, svarstomas prašymas dėl nesutikimo tvarkyti duomenis, ar egzistuoja tam tikri teisiniai pagrindai, neleidžiantys duomenų ištrinti.

---

[120] 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). *OL* L 119, 2016 5 4, p. 44.

[121] Baker & McKenzie. *EU General Data Protection Regulation in 13 Game Changers*. 2016, p. 13.

[122] Europos Komisija. *Kada turėčiau pasinaudoti savo teise apriboti savo asmens duomenų tvarkymą?* [interaktyvus; žiūrėta 2018 m. kovo 2 d.]. Prieiga per internetą: <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/my-rights/when-should-i-exercise-my-right-restriction-processing-my-personal-data_lt>.

2.2.3. Teisė į duomenų perkeliamumą

Teisė į duomenų perkeliamumą yra visiškai nauja duomenų subjektui suteikiama teisė, pagal kurią galima gauti duomenų valdytojui pateiktus asmens duomenis ir juos persiųsti kitam duomenų valdytojui.[123] Taip pat ši teisė laikoma viena svarbiausių Reglamento naujovių ne tik dėl to, kad suteikia duomenų subjektams didelę savo asmens duomenų kontrolę, bet ir todėl, kad ji susijusi su kitomis teisės sritimis – konkurencijos teise, intelektinės nuosavybės teise ir vartotojų apsauga.[124]

Pirmuoju duomenų perkeliamumo pavyzdžiu galėtų būti laikomas telefono numerio perkėlimas, suteikiamas vartotojui keičiant mobiliojo ryšio operatorių. Tačiau sparčiai vystantis internetui atsirado poreikis iš vieno paslaugų teikėjo perkelti kitam teikėjui daug platesnio turinio informaciją. Lengvas asmens duomenų judėjimas duomenų subjekto noru yra pagrindinis teisės į duomenų perkeliamumą tikslas, kuriuo siekiama sustiprinti duomenų subjekto galimybes laisvai ir nevaržomai disponuoti savo duomenimis.[125] Kiti ne mažiau svarbūs tikslai yra:

- suteikti duomenų subjektui daugiau galių kontroliuoti savo asmens duomenis;
- skatinti laisvą asmens duomenų srautą Europos Sąjungoje;[126]
- užkirsti kelią duomenų susaistymui;
- skatinti efektyvią konkurenciją tarp duomenų valdytojų;
- sukurti pasitikėjimą skaitmeninėje erdvėje.[127]

Teisės į duomenų perkeliamumą teikiami privalumai

Pats pagrindinis teisės į duomenų perkeliamumą privalumas yra tai, jog duomenų subjektai galės lengvai perkelti savo asmens duomenis iš vieno duomenų valdytojo kitam. Tokia galimybė užtikrina nevaržomą pasirinkimo teisę asmenims rinktis labiausiai jų lūkesčius ir interesus atitinkantį duomenų valdytoją. Be to, tokiu būdu duomenų subjektams suteikiama didesnė galimybė patiems kontroliuoti savo asmens duomenis, o tai savaime sukuria

[123] 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). *OL* L 119, 2016 5 4, p. 45.
[124] DE HART, Paul *et al*. The right to data portability in the GDPR: Towards user-centric interoperability of digital services. *Computer Law and Security Review*, 2017, p. 2.
[125] ZANFIR, Gabriela. The right to Data portability in the context of the EU data protection reform. *International Data Privacy Law*, 2012, Vol. 2, No. 3, p. 149.
[126] ES 29 str. duomenų apsaugos darbo grupė. 2016 m. gruodžio 13 d. *Teisės į duomenų perkeliamumą gairės* (su paskutiniais pakeitimais 2017 m. balandžio 5 d.). Nr. 16/LT WP 242 rev. 01, p. 3.
[127] VAN DER AUWERMEULEN, Barbara. How to attribute the right to data portability in Europe: A comparative analysis of legislations. *Computer Law and Security Review*, 2017, t. 33, p. 68.

vartotojams draugišką aplinką ir lemia didesnį pasitikėjimą duomenų valdytojais. Šis argumentas yra ypač akcentuojamas Europos Komisijos, siekiant pagrįsti teisės į duomenų perkeliamumą efektyvumą.[128]

Kitas aspektas, susijęs su teisės į duomenų perkeliamumą privalumais, yra vartotojų teisių apsauga. Galimybė perkelti asmens duomenis užkerta kelią duomenų susaistymo efektui (angl. *lock-in effect*), kuris yra viena iš prielaidų teisės į duomenų perkeliamumą sukūrimui.[129] Šis efektas susidaro kai ilgą laikotarpį vieno paslaugų teikėjo paslaugomis besinaudojantis vartotojas yra sukaupęs nemažai duomenų, kurie jam yra ypač svarbūs naudojantis tam tikra paslauga, ir todėl nėra linkęs keisti paslaugų teikėjo. Nesuteikiant duomenų subjektui teisės perkelti su juo susijusią informaciją būtų pažeidžiamos vartotojų teisės ir iškraipoma konkurencija tarp paslaugų teikėjų.

Duomenų susaistymas yra dažnas reiškinys skaitmeniniame pasaulyje. Daugelis organizacijų, siūlančių tam tikras paslaugas, renka, tvarko ir apdoroja duomenis išimtinai savo organizacijos veiklai vykdyti ir tikslams pasiekti, taip siekdamos įgyti konkurencinį pranašumą prieš kitas organizacijas, kurios šių duomenų neturi[130]. Todėl nauja duomenų subjektui suteikiama teisė į duomenų perkeliamumą šiek tiek keičia nusistovėjusias konkurencijos taisykles. Jeigu teisė į duomenų perkeliamumą nebūtų užtikrinama, duomenų subjektas galimai nesiryžtų keisti duomenų valdytojo dėl didelių pastangų poreikio, net jeigu naujas duomenų valdytojas siūlytų patrauklesnes paslaugas.[131]

Taigi, nuo šiol duomenų perkėlimas iš vieno valdytojo kitam gali suteikti daug privalumų ir naujoms, inovatyvioms organizacijoms. Pavyzdžiui, jeigu rinkoje ilgą laiką egzistuoja ir didelę rinkos dalį užima viena verslo įmonė, kuri naudojasi dideliais savo klientų duomenų kiekiais, naujoms įmonėms patekti į šią rinką ir pritraukti vartotojus iš pirmosios įmonės yra labai sunku. Net jeigu naujoji įmonė vartotojams siūlo geresnes prekių ar paslaugų sąlygas, vartotojai gali nenorėti pereiti prie naujos įmonės dėl šio perėjimo sudėtingumo. Todėl galimybė perkelti asmens duomenis kitai verslo įmonei turės didelę reikšmę.[132]

Be to, naujoji teisė, su sąlyga, kad bus užtikrinamas jos įgyvendinimo paprastumas, gali paspartinti asmens duomenų judėjimą. Tai paslaugų teikėjams sudarys galimybę surinkti aktualios su duomenų judėjimu susijusios informacijos, kuri nebuvo prieinama iki

[128] VAN DER AUWERMEULEN, Barbara. How to attribute the right to data portability in Europe: A comparative analysis of legislations. *Computer Law and Security Review*, 2017, t. 33, p. 59.
[129] Ibid., p. 58.
[130] ENGELS, Barbara. Data portability among online platforms. *Internet Policy Review: Journal on Internet Regulation*, 2016, t. 5(2), p. 2.
[131] Ibid., p. 6-7.
[132] Ibid., p. 6.

šiol, ir ši informacija galės būti naudojama į tikslines vartotojų grupes nukreiptai reklamai kurti[133]. Padidėjusi konkurencija paskatintų verslo įmones gerinti prekių ar paslaugų kokybę arba mažinti kainas, tokiu būdu siekiant neprarasti esamų vartotojų, svarstančių pereiti prie kitų įmonių. Taigi, tai skatina paslaugų vystymąsi, tobulėjimą ir inovacijų kūrimą. Taip pat paslaugų teikėjai, užtikrinantys duomenų perkėlimo prieinamumą, paprastumą ir skaidrumą, pelnys vartotojų pasitikėjimą ir padės juos išlaikyti bei pritraukti naujų. Visi šie aspektai dar labiau pagerina duomenų subjektų padėtį.

Teisės į duomenų perkeliamumą įgyvendinimo pagrindai

Teisė į duomenų perkeliamumą įtvirtinama Reglamento 20 straipsnyje, pagal kurį tai yra duomenų subjekto teisė gauti su juo susijusius asmens duomenis, kuriuos jis prieš tai pateikė duomenų valdytojui, susistemintu, įprastai naudojamu ir kompiuterio skaitomu formatu, ir teisė persiųsti tuos duomenis kitam duomenų valdytojui, o duomenų valdytojas, kuriam tie asmens duomenys buvo pateikti, turi nesudaryti tam kliūčių.[134]

Išanalizavus šį straipsnį galima daryti išvadą, kad teisė į duomenų perkeliamumą yra sudaryta iš trijų skirtingų teisių:

1) teisė gauti su duomenų subjektu susijusius asmens duomenis, kuriuos jis pateikė duomenų valdytojui (be jokių duomenų valdytojo sudaromų kliūčių);
2) teisė persiųsti tuos gautus duomenis kitam duomenų valdytojui (be jokių duomenų valdytojo sudaromų kliūčių);
3) teisė, kad vienas duomenų valdytojas asmens duomenis tiesiogiai persiųstų kitam, kai tai techniškai įmanoma.[135]

Taip pat svarbu pabrėžti, jog pagal teisės į duomenų perkeliamumą turinį nėra būtina, kad asmens duomenys būtų perduoti kitam duomenų valdytojui. Duomenų subjektas gali prašyti perkelti jam duomenis savo asmeniniam naudojimui.[136] Tai suteiks galimybę pakartotinai disponuoti savo duomenimis bet kokiems teisėtiems tikslams įgyvendinti.

Reglamento 20 str. 3 d. įtvirtinta, jog naudojimasis teise į duomenų perkeliamumą nedaro poveikio teisei būti pamirštam. 29 str. darbo grupės gairėse nurodoma, jog net ir tuo atveju, kai asmens duomenys yra perkeliami kitam duomenų valdytojui, duomenų

[133] VAN DER AUWERMEULEN, Barbara. How to attribute the right to data portability in Europe: A comparative analysis of legislations. *Computer Law and Security Review*, 2017, t. 33, p. 60.
[134] 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). *OL* L 119, 2016 5 4, p. 45.
[135] DE HART, Paul *et al*. The right to data portability in the GDPR: Towards user-centric interoperability of digital services. *Computer Law and Security Review*, 2017, p. 5.
[136] ES 29 str. duomenų apsaugos darbo grupė. 2016 m. gruodžio 13 d. *Teisės į duomenų perkeliamumą gairės* (su paskutiniais pakeitimais 2017 m. balandžio 5 d.). Nr. 16/LT WP 242 rev. 01, p. 5.

subjektas vis tiek gali naudotis pirmojo duomenų valdytojo teikiamomis paslaugomis. Vien tai, jog duomenys buvo perkelti, neįpareigoja pirmojo duomenų valdytojo tuos duomenys ištrinti iš savo saugomų duomenų sistemos ir nesutrumpina anksčiau nustatyto laikotarpio, skirto duomenims saugoti.[137]

Tačiau duomenų subjektai turės teisę perkelti savo asmens duomenis tik tuomet, jeigu jie atitiks šiuos reikalavimus:

- duomenų tvarkymas yra grindžiamas sutikimu arba sutartimi;
- duomenys yra tvarkomi automatizuotomis priemonėmis.

Kitais atvejais, kai asmens duomenų tvarkymas yra būtinas atliekant užduotį, kuri yra vykdoma viešojo intereso labui arba vykdant viešosios valdžios funkcijas, pavestas duomenų valdytojui, teisė į duomenų perkeliamumą nėra taikoma. Tokių atvejų pavyzdžiu galėtų būti finansų įstaigų veikla – kai asmens duomenys yra tvarkomi siekiant užkirsti kelią finansiniams nusikaltimams ar juos aptikti.[138]

Aiškinant teisės į duomenų perkeliamumą turinį svarbiausia yra nustatyti dviejų sąvokų ribas:

- su duomenų subjektu susiję asmens duomenys;
- duomenų subjekto pateikti duomenų valdytojui duomenys.

Abi šios sąvokos turėtų būti aiškinamos plečiamai. Kalbant apie *susijusius su duomenų subjektu duomenis*, reikėtų tokiems duomenims priskirti ir tą informaciją, kurioje aptinkama kitų žmonių asmens duomenų, pavyzdžiui, telefono pokalbių ar susirašinėjimo išklotinės.[139] Šiuo atveju nėra įmanoma atskirti vieno asmens subjekto duomenų nuo kito, nepažeidžiant duomenų turinio, todėl su vienu duomenų subjektu susiję duomenys gali apimti ir kito subjekto duomenis.

Duomenų valdytojui *pateikti duomenys* taip pat gali būti vertinami dviem būdais – siaurinamai ir plečiamai. Tačiau atsižvelgiant į teisės į duomenų perkeliamumą tikslus, rekomenduojama *pateiktų duomenų* sampratą aiškinti plečiamai.[140] Tai reiškia, jog pateikti duomenys apima ne tik tą informaciją, kurią duomenų subjektas eksplicitiškai pateikė duomenų valdytojui (pavyzdžiui, užpildydamas registracijos anketą), bet ir tą informaciją, kurią duomenų valdytojas pats surinko apie duomenų subjektą jį stebėdamas (pavyzdžiui,

[137] ES 29 str. duomenų apsaugos darbo grupė. 2016 m. gruodžio 13 d. *Teisės į duomenų perkeliamumą gairės* (su paskutiniais pakeitimais 2017 m. balandžio 5 d.). Nr. 16/LT WP 242 rev. 01, p. 8.
[138] Ibid., 10.
[139] Ibid.
[140] DE HART, Paul *et al*. The right to data portability in the GDPR: Towards user-centric interoperability of digital services. *Computer Law and Security Review*, 2017, p. 11.

stebint naršymo istoriją).[141] Tačiau pateikti duomenys neapima tu duomenų, kurie yra sukuriami duomenų valdytojo analizuojant tiesiogiai jam pateiktus ar jo pastebėtus duomenis.[142]

Siekiant įgyvendinti teisę į duomenų perkeliamumą turi būti užtikrinta dar viena sąlyga – ši teisė negali daryti neigiamo poveikio kitų teisėms ir laisvėms (Reglamento 20 str. 4 d.). Savaime suprantama, jog dažnu atveju, perkeliant asmens duomenis kitam duomenų valdytojui, tuose duomenyse galima aptikti ir su kitais asmenimis susijusios informacijos. Siekiant apsaugoti trečiųjų šalių duomenis, naujam duomenų valdytojui draudžiama naudoti tuos duomenis savo tikslams siekti. Pavyzdžiui, naujas duomenų valdytojas neturi teisės siūlyti savo paslaugų tretiesiems duomenų subjektams ar stebėti ir analizuoti jų veiklą, kitaip toks elgesys būtų neteisėtas.[143]

Svarbu paminėti, jog kiekvienu atveju, svarstant prašymo dėl teisės į duomenų perkeliamumą tenkinimą, situacija turi būti vertinama individualiai. Šios teisės turinį sudaro net keletas abstrakčių sąvokų, reikalaujančių kompetentingo aiškinimo. Todėl yra neabejotina, jog pradėjus taikyti Reglamentą daugiausiai iššūkių sukelsiančios situacijos pasieks teismus ir jų formuojama praktika lems teisės į duomenų perkeliamumą turinio aiškinimą.

Teisės į duomenų perkeliamumą problemos ir iššūkiai

Vienas iš didžiausių iššūkių, susijusių su teise į duomenų perkeliamumą yra pakankamo privatumo išsaugojimas[144]. Yra didelė tikimybė, kad duomenų valdytojai pateiks nepakankamą kiekį informacijos, susijusios su duomenų perkėlimo įgyvendinimu. Tokiu atveju duomenų subjektai negalės būti užtikrinti, kad su jų asmens duomenimis susijusi informacija perkeliama saugiai ir laikantis įstatymų reikalavimų. Net ir išsamios informacijos pateikimo atveju duomenų subjektams greičiausiai nebus suteikta galimybė kontroliuoti jų asmens duomenų perdavimo, todėl taip pat nebus galimybės įsitikinti duomenų perkėlimo skaidrumu.[145] Tai apsunkins asmens duomenų kontrolę ir galimai sudarys prielaidas piktnaudžiavimui duomenų perkėlimu. Todėl duomenų valdytojai turėtų

[141] ES 29 str. duomenų apsaugos darbo grupė. 2016 m. gruodžio 13 d. *Teisės į duomenų perkeliamumą gairės* (su paskutiniais pakeitimais 2017 m. balandžio 5 d.). Nr. 16/LT WP 242 rev. 01., p. 7.
[142] Ibid., p. 11.
[143] Ibid., p. 13.
[144] YOO, Christopher. When Antitrust Met Facebook. *Penn Law: Legal Scholarship Repository – Faculty Scholarship*, 2012, t. 422, p. 1155.
[145] WEISS, Stefan. Privacy Threat Model for Data Portability in Social Network Applications. *Americas Conference on Information Systems (AMCIS) 2008 Proceedings*, 2008, t. 84, p. 1.

užtikrinti skaidrų duomenų perkėlimo procesą ir garantuoti duomenų subjektams kuo daugiau jų teises apsaugančių saugiklių.

Dar vienas pavojus yra tai, jog duomenų perkėlimu gali piktnaudžiauti tie duomenų valdytojai, kuriems yra perkeliami asmens duomenys[146]. Naujieji duomenų valdytojai gali gauti didesnį kiekį asmens duomenų nei yra būtina jų teikiamoms paslaugoms teikti ir naudotis papildoma tokių duomenų suteikiama verte. Tokiu būdu ne tik elgiamasi nesąžiningai su vartotojais – duomenų subjektais, bet ir iškraipoma konkurencija su kitais paslaugų teikėjais. Dėl šios priežasties turėtų būti sukuriamos išsamios taisyklės, reguliuojančios reikiamą duomenų perdavimo kiekį. Tik taip bus užtikrinama duomenų subjekto teisių apsauga ir duomenų perdavimo reikalingumas.

Kita problema, susijusi su teise į duomenų perkeliamumą, yra galima duomenų subjekto tapatybės vagystė[147]. Pasirūpinti saugumu internete pirmiausiai yra paties duomenų subjekto atsakomybė. Kiekvienas asmuo turi įvertinti savo asmens duomenų saugumo riziką ypač internetinėje erdvėje ir pasirūpinti visomis įmanomomis priemonėmis, kad su juo susijusi informacija būtų saugi, pavyzdžiui, naudoti stiprius ir nenuspėjamus slaptažodžius ir niekam jų neatskleisti.

Tačiau duomenų valdytojas taip pat turi imtis visų galimų saugumo užtikrinimo priemonių, garantuodamas teisės į duomenų perkeliamumą įgyvendinimą. Dar prieš svarstydamas asmens prašymą į duomenų perkeliamumą, duomenų valdytojas privalo duomenų subjektą identifikuoti. Šiam tikslui turėtų būti sukurta procedūra, patvirtinanti autentiškumą, kurios pagalba duomenų valdytojas galėtų nustatyti tapatybę asmens, prašančio perkelti duomenis.[148]

Tokios procedūros daugeliu atvejų jau yra taikomos. Jų pavyzdžiu galėtų būti vartotojo vardas ir slaptažodis, kuriuos asmuo naudoja prisijungdamas prie savo duomenų elektroninio pašto ar socialinių tinklų paskyrose. Tas pats vartotojo vardas bei slaptažodis galėtų būti naudojami ir prašant perkelti duomenis. Šiuo atveju tokie duomenys būtų duomenų subjekto tapatybę ir autentiškumą patvirtinantis įrodymas.[149] Tačiau, esant pagrįstoms abejonėms dėl duomenų subjekto tapatybės, jis gali būti prašomas pateikti papildomos informacijos jo tapatybei patvirtinti (Reglamento 12 str. 6 d.).

[146] VAN DER AUWERMEULEN, Barbara. How to attribute the right to data portability in Europe: A comparative analysis of legislations. *Computer Law and Security Review*, 2017, t. 33, p. 60.
[147] Ibid.
[148] ES 29 str. duomenų apsaugos darbo grupė. 2016 m. gruodžio 13 d. *Teisės į duomenų perkeliamumą gairės* (su paskutiniais pakeitimais 2017 m. balandžio 5 d.). Nr. 16/LT WP 242 rev. 01, p. 15.
[149] Ibid.

Taigi, duomenų valdytojas, imdamasis duomenų perkeliamumo įgyvendinimo, turėtų įvertinti galimus tokio perkėlimo pavojus ir užtikrinti, kad yra imamasi visų įmanomų priemonių siekiant pavojaus išvengti.[150] Turėtų būti nustatoma ne tik asmens, prašančio perkelti duomenis, tapatybė, bet ir užtikrinama, kad duomenys perkeliami reikiamam subjektui, ypač tuo atveju, kai duomenis prašoma persiųsti tiesiai kitam duomenų valdytojui. Taip pat turėtų būti garantuojamas paties duomenų persiuntimo proceso saugumas, kuris galėtų būti užtikrinamas įvairiais technologiniais būdais, saugančiais duomenis nuo įsibrovimų ir vagysčių.

Tačiau duomenų subjekto galimybes įgyvendinti savo teisę į greitą ir lengvą duomenų perkeliamumą gali apriboti duomenų valdytojų turimos techninės priemonės. Duomenų valdytojai nėra įpareigojami naudoti suderinamas sistemas duomenų perkeliamumui, tik yra pageidaujama, jog formatas, kuriuo duomenų valdytojas teikia duomenis, būtų sąveikus (Reglamento preambulės 68 p.). Kitaip tariant, sąveikumas yra skatinamas, tačiau jo įgyvendinimas priklauso tik nuo duomenų valdytojų naudojamų techninių priemonių.

Dar vienas didelis su duomenų perkeliamumu susijęs iššūkis yra siekis apsaugoti intelektinę nuosavybę.[151] Tam tikrais atvejais gali būti sudėtinga nustatyti, kurie būtent duomenys yra laikomi asmens duomenimis. Tai atskleidžia socialinio tinklo *Facebook* pavyzdys. Didelė dalis šiame socialiniame tinkle esančio turinio priklauso daugiau nei vienam duomenų subjektui. Pavyzdžiui, vartotojo profilyje yra nuotraukų, kuriose yra užfiksuotas jis pats, tačiau pati nuotrauka yra padaryta ir įkelta kito asmens. Ar duomenų subjektui, norinčiam perkelti visas tokias nuotraukas, reikia gauti visų tose nuotraukose esančių žmonių sutikimą? Ar nepaprašius sutikimo nebus pažeistos kitų asmenų autorių teisės? Be to, tam tikrą turinį, pavyzdžiui, video įrašus, sukurtus iš vartotojų nuotraukų, sukuria pats *Facebook* socialinis tinklas. Ar tokiu atveju būtų teisinga tokį duomenų valdytojo sukurtą galutinį turinį perkelti kitam duomenų valdytojui? Tai tik keletas su intelektinės nuosavybės problemomis susijusių klausimų, keliančių dvejones dėl teisės į duomenų perkeliamumą įgyvendinimo tikslingumo.

Apibendrinant galima daryti išvadą, jog teisė į duomenų perkeliamumą asmenims suteikia daug privalumų. Ši teisė dar labiau sustiprina duomenų subjekto galimybes pačiam kontroliuoti savo asmens duomenis, užkerta kelią jų susaistymui ir sudaro prielaidas

[150] KINGSTON, John. Using artificial intelligence to support compliance with the general data protection regulation. *Artificial Intelligence and Law*, 2017, Vol. 25, No. 4, p. 437.
[151] VAN DER AUWERMEULEN, Barbara. How to attribute the right to data portability in Europe: A comparative analysis of legislations. *Computer Law and Security Review*, 2017, t. 33, p. 60.

lengviau keisti duomenų valdytojus. Taip pat ši teisė naudinga ir naujoms besisteigiančioms organizacijoms, kurios dėl lengvesnio duomenų perkėlimo turi daugiau galimybių patekti į rinką ir pritraukti vartotojų. Tai didina konkurenciją jau egzistuojančioms organizacijoms, kurios yra priverstos prisiderinti prie pokyčių. Tokių pokyčių pasekmės dažniausiai apima gerėjančią paslaugų kokybę, mažėjančias paslaugų kainas ir inovacijų kūrimą.

Tačiau teisė į duomenų perkeliamumą turi ir neigiamų aspektų. Kyla grėsmė, jog bus perduodama daugiau duomenų nei yra būtina naujam duomenų valdytojui turėti. Taip pat gali būti kėsinamasi pasisavinti duomenų subjekto tapatybę prašant perkelti duomenis. Tam tikrais atvejais gali kilti iššūkių siekiant suderinti teisę į duomenų perkeliamumą su intelektinės nuosavybės apsauga. Dėl šių priežasčių duomenų valdytojai privalo imtis visų galimų priemonių, siekiant užtikrinti efektyvų teisės į duomenų perkeliamumą įgyvendinimą.

2.3. Pranešimas apie asmens duomenų saugumo pažeidimą

Reglamentas nustato naują pareigą duomenų valdytojams – įvykus asmens duomenų saugumo pažeidimui duomenų valdytojas privalo nepagrįstai nedelsdamas ir, jei įmanoma, per 72 valandas nuo tada, kai jis sužino apie asmens duomenų saugumo pažeidimą, apie tai pranešti priežiūros institucijai, nebent asmens duomenų saugumo pažeidimas neturėtų kelti pavojaus fizinių asmenų teisėms ir laisvėms (Reglamento 33 str. 1 d.). Kai dėl asmens duomenų saugumo pažeidimo gali kilti didelis pavojus duomenų fizinių asmenų teisėms ir laisvėms, duomenų valdytojas nepagrįstai nedelsdamas privalo apie pažeidimą pranešti taip pat ir duomenų subjektui, kurio duomenų saugumas buvo pažeistas (Reglamento 34 str. 1 d.).[152]

Tam, kad duomenų valdytojas galėtų nuspręsti, ar turi pareigą apie pažeidimą pranešti priežiūros institucijai ar duomenų subjektui, pirmiausiai turi būti atskiriamas asmens duomenų saugumo pažeidimas, nuo bet kokio kito saugumo pažeidimo. Kaip teigia 29 str. darbo grupė, ne kiekvienas saugumo pažeidimas yra susijęs su asmens duomenimis[153]. Konkretus asmens duomenų saugumo pažeidimo apibrėžimas yra pateiktas Reglamento 4

[152] 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). *OL* L 119, 2016 5 4, p. 52-53.
[153] Article 29 Data Protection Working Party. *2017 October 3 Guidelines on Personal data breach notification under Regulation 2016/679*. 17/EN WP250, p. 6.

str. 12 d., pagal kurią tai yra saugumo pažeidimas, dėl kurio netyčia arba neteisėtai sunaikinami, prarandami, pakeičiami, be leidimo atskleidžiami persiųsti, saugomi arba kitaip tvarkomi asmens duomenys arba prie jų be leidimo gaunama prieiga.

Nustačius, jog įvyko asmens duomenų apsaugos pažeidimas, tai dar nereiškia, jog apie šį pažeidimą duomenų valdytojas turi pranešti priežiūros institucijai ar duomenų subjektui. Pareiga pranešti priklauso nuo to, ar kyla pavojus fizinių asmenų teisėms ir laisvėms bei koks to pavojaus mastas. Esant pavojui, duomenų valdytojas privalo apie pažeidimą pranešti priežiūros institucijai, o esant dideliam pavojui – taip pat ir pačiam duomenų subjektui. Bet kuriuo atveju pranešimo apie asmens duomenų saugumo pažeidimą tikslas yra sumažinti galimą žalą duomenų subjektams. Tačiau, kai pranešimas yra skirtas duomenų subjektui, tokiu atveju yra taip pat siekiama pateikti informaciją dėl priemonių, kurių galėtų imtis pats duomenų subjektas neigiamoms pažeidimo pasekmėms sumažinti.

Pranešimo apie asmens duomenų saugumo pažeidimą turinį turi sudaryti bent ši informacija:

- aprašytas asmens duomenų saugumo pažeidimo pobūdis;
- nurodyta duomenų apsaugos pareigūno arba kito kontaktinio asmens, galinčio suteikti daugiau informacijos, vardas bei pavardė ir kontaktiniai duomenys;
- aprašytos tikėtinos asmens duomenų saugumo pažeidimo pasekmės;
- aprašytos priemonės, kurių ėmėsi arba pasiūlė imtis duomenų valdytojas, kad būtų pašalintas asmens duomenų saugumo pažeidimas, įskaitant, kai tinkama, priemones galimoms neigiamoms jo pasekmėms sumažinti. (Reglamento 33 str. 3 d. ir 34 str. 2 d.)

Tiesa, kai pranešimas yra skirtas duomenų subjektui, pažeidimo pobūdžio aprašymui yra keliamas aiškios ir paprastos kalbos reikalavimas (Reglamento 34 str. 2 d.). Tuo tarpu pranešime skirtame priežiūros institucijai yra keliami aukštesni pažeidimo pobūdžio aprašymo reikalavimai – taip pat turėtų būti nurodoma paveiktų duomenų subjektų kategorijos ir apytikris skaičius, asmens duomenų įrašų kategorijos ir jų apytikris skaičius (Reglamento 33 str. 3 d.).

Vis dėlto didžiausias iššūkis duomenų valdytojui yra nustatyti pavojaus fizinių asmenų teisėms ir laisvėms mastą. Kiekvienu atveju situacija turi būti vertinama individualiai. Tačiau 29 str. darbo grupė rekomenduoja naudoti šiuos vertinimo kriterijus: pažeidimo tipas; asmens duomenų pobūdis, jautrumas ir apimtis; asmenų identifikavimo sudėtingumas; pasekmių asmenims mastas; ypatingos asmens savybės; paveiktų asmenų

skaičius; duomenų valdytojo ypatybės.[154] Visi šie kriterijai turėtų būti vertinami sistemiškai.

Laiku nesiimant tinkamų priemonių dėl asmens duomenų saugumo pažeidimo, asmenys gali patirti net kūno sužalojimą, materialinę ar nematerialinę žalą. Didelės žalos pavyzdžiais yra asmens duomenų kontrolės praradimas, teisių apribojimo patyrimas, diskriminacija, asmens tapatybės vagystė ar suklastojimas, sukelti finansiniai nuostoliai, pakenkimas reputacijai, prarastas asmens duomenų, kurie saugomi profesine paslaptimi, konfidencialumas arba padaryta kita ekonominė ar socialinė žala (Reglamento preambulės 85 p.). Pavyzdžiui, ligoninei praradus duomenis apie pacientus, šių sveikatai ar net gyvybei gali kilti rimtas pavojus ypač tais atvejais, kai duomenų praradimas lemia operacijų atšaukimą.[155]

Tikėtina, jog žala gali kilti ir tais atvejais, kai pažeidimas apima asmens duomenis, kurie atskleidžia rasinę ar etninę kilmę, politines pažiūras, religiją, filosofinius įsitikinimus ar narystę profesinėje sąjungoje, apima genetinius duomenis, duomenis apie sveikatą ar duomenis apie lytinį gyvenimą, informaciją apie baudžiamuosius nuosprendžius ar nusikaltimus.[156] Todėl, siekiant išvengti neigiamų asmens duomenų saugumo pažeidimo pasekmių ar bent jau sumažinti jų mastą, duomenų valdytojas turi nedelsdamas imtis jam numatytų atitinkamų pareigų įgyvendinimo.

2.4. Poveikio duomenų apsaugai vertinimas

Reglamentas numato dar vieną pareigą duomenų valdytojams. Prieš pradėdamas duomenų tvarkymo operacijas, duomenų valdytojas turės įvertinti, ar dėl tokio duomenų tvarkymo gali kilti didelis pavojus fizinių asmenų teisėms bei laisvėms. Jei toks pavojus yra įmanomas, tuomet duomenų valdytojas privalės atlikti duomenų tvarkymo operacijų poveikio asmens duomenų apsaugai vertinimą (Reglamento 35 str. 1 d.).[157]

Jeigu atlikus vertinimą nustatoma, kad tvarkant duomenis kiltų didelis pavojus, jei nebūtų imamasi priemonių pavojui sumažinti, tuomet duomenų valdytojas turi dar vieną naują pareigą – prieš pradėdamas tvarkyti duomenis privalo konsultuotis su priežiūros

[154] Article 29 Data Protection Working Party. *2017 October 3 Guidelines on Personal data breach notification under Regulation 2016/679*. 17/EN WP250, p. 20-22.
[155] Ibid., p. 7.
[156] Ibid., p. 20.
[157] 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). *OL* L 119, 2016 5 4, p. 53.

institucija (Reglamento 36 str. 1 d.). Šios pareigos keičia pagal dabartinį teisinį reguliavimą egzistuojančią pareigą iš anksto pranešti duomenų apsaugos priežiūros institucijai apie duomenų tvarkymą (Duomenų apsaugos direktyvos 18 str.).[158]

Svarbu pabrėžti, jog nėra būtina atlikti kiekvienos duomenų tvarkymo operacijos poveikio duomenų apsaugai vertinimą. Šis vertinimas yra būtinas tik tais atvejais, kai fizinių asmenų teisėms bei laisvėms gali kilti didelis pavojus. Kiekvienu atveju turėtų būti atsižvelgiama į duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus. Be to, vertinimas gali būti atliekamas nebūtinai tik vienai konkrečiai duomenų tvarkymo operacijai. Jeigu yra daugiau panašių duomenų tvarkymo operacijų, joms gali būti atliekamas vienas poveikio duomenų apsaugai vertinimas (Reglamento 35 str. 1 d.). Tam tikrais atvejais tai yra protingiau ir ekonomiškiau, pavyzdžiui, kai keli duomenų valdytojai planuoja taikyti bendrą duomenų tvarkymo programą (Reglamento preambulės 92 p.).

Didžiausias iššūkis duomenų valdytojams gali kilti vertinant, ar konkreti duomenų tvarkymo operacija galimai sukels didelį pavojų fiziniams asmenims. Didelio pavojaus samprata nėra apibrėžta Reglamente, tačiau 35 str. 3 d. pateikti 3 atvejai, kuriems esant yra būtina atlikti poveikio duomenų apsaugai vertinimą:

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

Šis sąrašas nėra baigtinis, todėl priežiūros institucija turėtų sudaryti duomenų tvarkymo operacijų, kurioms būtinas poveikio duomenų apsaugai vertinimas, sąrašą (Reglamento 35 str. 4 d.). Taip pat 29 str. darbo grupė pateikia kriterijus, pagal kuriuos turėtų būti nustatomas vertinimo būtinumas:

1) duomenų subjekto vertinimas arba balų skyrimas;
2) automatizuotas sprendimų, sukeliančių teisinį arba panašų rimtą poveikį, priėmimas;
3) sisteminga stebėsena;

[158] 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo. *OL* 2004 m. specialusis leidimas, 13 skyrius, 15 tomas, p. 367.

4) neskelbtini duomenys arba labai asmeniški duomenys (pavyzdžiui, nusikalstamos veikos, pacientų medicininė informacija);
5) didelio masto duomenų tvarkymas;
6) duomenų rinkinių siejimas ir derinimas;
7) su pažeidžiamais duomenų subjektais susiję duomenys (pavyzdžiui, vaikų, darbuotojų, vyresnio amžiaus asmenų, pacientų duomenys);
8) naujoviškas naudojimas arba naujų technologinių ar organizacinių sprendimo būdų taikymas (pavyzdžiui, pirštų atspaudų naudojimo ir veido atpažinimo derinimas);
9) atvejis, kai dėl paties duomenų tvarkymo duomenų subjektams užkertamas kelias naudotis savo teisėmis, paslaugomis arba sudaryti sutartis (pavyzdžiui, kai bankas tikrina savo klientą kredito informacinėje duomenų bazėje, kad nuspręstų, ar suteikti jam paskolą).[159]

Įprastai, kuo daugiau kriterijų duomenų tvarkymo operacija atitinka, tuo labiau tikėtina, kad dėl jos kils didelis pavojus duomenų subjektų teisėms ir laisvėms, todėl bus būtina atlikti poveikio duomenų apsaugai vertinimą. Jeigu vis dėlto nėra aišku, ar vertinimą atlikti būtina, 29 str. darbo grupė tai padaryti rekomenduoja.[160]

Poveikio duomenų apsaugai vertinimu duomenų valdytojai turi galimybę nustatyti galimai kilsiančius pavojus duomenų subjektų teisėms ir tuos pavojus valdyti. Todėl vertinime privalo būti bent šie aspektai (Reglamento 35 str. 7 d.):

- sistemingas numatytų duomenų tvarkymo operacijų aprašymas ir duomenų tvarkymo tikslai;
- duomenų tvarkymo operacijų reikalingumo ir proporcingumo vertinimas;
- duomenų subjektų teisėms ir laisvėms kylančių pavojų vertinimas;
- pavojams pašalinti numatytos priemonės.

Kitaip tariant, aplinkybių nustatymas, rizikos įvertinimas ir jos valdymas (pavojaus mažinimas) užtikrina asmens duomenų apsaugą. Kartu tai yra atskaitomybės priemonė, nes padeda duomenų valdytojams įrodyti, kad yra laikomasi duomenų apsaugos teisės aktų reikalavimų ir imamasi tinkamų priemonių tiems reikalavimams vykdyti.[161] Visa tai turėtų didinti duomenų subjektų pasitikėjimą duomenų valdytojais ir jų atliekamomis duomenų tvarkymo operacijoms.

[159] ES 29 str. duomenų apsaugos darbo grupė. *2017 m. balandžio 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. 17/LT WP 248, 1-oji peržiūrėta versija, p. 10-12.
[160] Ibid., p. 9.
[161] Ibid., p. 4.

2.5. Duomenų apsaugos pareigūnas

Duomenų apsaugos pareigūnas – tai dar vienas naujas Reglamente įtvirtinamas institutas. Tai asmuo, kurio pareigos apima duomenų valdytojo ar duomenų tvarkytojo atitikties Reglamentui priežiūrą ir užtikrinimą bei tarpininkavimą tarp suinteresuotųjų subjektų – organizacijos padalinių, duomenų subjektų ir priežiūros institucijų. Tačiau pati duomenų apsaugos pareigūno sąvoka nėra visiškai nauja. Jos atitikmenys randami tiek Duomenų apsaugos direktyvoje, tiek ir kai kurių ES valstybių narių nacionaliniuose įstatymuose.

2.5.1. Dabartinis duomenų apsaugos pareigūno reglamentavimas

Duomenų apsaugos direktyvoje duomenų apsaugos pareigūnas minimas net kelis kartus – 18 ir 20 straipsniuose. Pagal šios direktyvos 18 str. duomenų valdytojas arba jo atstovas, jei toks yra, privalo pranešti priežiūros institucijai prieš atlikdamas bet kurią visiškai ar iš dalies automatinę tvarkymo operaciją arba operacijų grupę, numatytą vienam tikslui ar keletui susijusių tikslų. Tačiau duomenų valdytojas pagal valstybės narės įstatymus gali būti atleistas nuo šio reikalavimo ar šis reikalavimas supaprastintas jeigu duomenų valdytojas, laikydamasis jam taikomų nacionalinių įstatymų, paskiria pareigūną asmens duomenų apsaugai, kuris privalo užtikrinti, kad duomenų valdytojas laikytųsi pagal šią direktyvą priimtų nacionalinių nuostatų, ir pildyti duomenų valdytojo atliktų tvarkymo operacijų registrą tokiu būdu užtikrinant, kad duomenų subjektų teisės ir laisvės negalėtų būti neigiamai paveiktos dėl tvarkymo operacijų (Duomenų apsaugos direktyvos 18 str.).

Dar viena duomenų apsaugos pareigūno funkcija įtvirtinta Duomenų apsaugos direktyvos 20 str., reglamentuojančiame išankstinę tvarkymo operacijų patikrą. Pagal šį straipsnį priežiūros institucija, gavusi pranešimą iš duomenų valdytojo, arba duomenų apsaugos pareigūnas, kuris, kilus abejonėms, privalo tartis su priežiūros institucija, atlieka išankstines patikras tvarkymo operacijoms, kurios valstybės narės reglamentuojamos kaip galinčios kelti konkretų pavojų duomenų subjekto teisėms ir laisvėms (Duomenų apsaugos direktyvos 20 str.).

Taigi, pagal dabartinį teisinį duomenų apsaugos reguliavimą ES lygmeniu duomenų apsaugos pareigūno paskyrimas nėra būtinas, todėl daugumos ES valstybių narių duomenų apsaugos įstatymuose nėra nustatyta pareiga jį paskirti. Išimtys tokiam reguliavimui yra tik Vokietija ir Kroatija, kurių įstatymuose įtrauktos nuostatos, reikalaujančios tiek privačiųjų, tiek ir viešųjų organizacijų (su išimtimi tik labai mažoms organizacijoms) paskirti

privalomą duomenų apsaugos pareigūną[162]. Dar nedidelė dalis valstybių nustato privalomai skiriamą duomenų apsaugos pareigūną tik tam tikruose sektoriuose. Pavyzdžiui, Suomijoje duomenų apsaugos pareigūną privalo paskirti socialinės apsaugos ir sveikatos priežiūros paslaugų teikėjai, o Vengrijoje – finansų įstaigos, komunalinių paslaugų įmonės ir telekomunikacijų bendrovės. Kitos valstybės, tokios kaip Nyderlandai, Liuksemburgas, Lenkija ir Švedija reglamentuoja savanorišką duomenų apsaugos pareigūno skyrimą,[163] kurio dėka organizacijos gali būti atleistos nuo tam tikrų reikalavimų atlikimo, pavyzdžiui, nuo pranešimo priežiūros institucijai prieš atliekant automatinę tvarkymo operaciją kaip ir nurodyta Duomenų apsaugos direktyvos 18 str.

Duomenų apsaugos pareigūno skyrimas nėra privalomas ir Lietuvos teisinėje sistemoje, tačiau Duomenų apsaugos įstatymo 32 str. numatyta duomenų valdytojo teisė paskirti už duomenų apsaugą atsakingą asmenį ar padalinį, kurio funkcijos atitinka pagal Reglamentą privalomai skiriamo asmens duomenų pareigūno būsimas funkcijas. Tai labiausiai atsispindi pagal tame pačiame Duomenų apsaugos įstatymo straipsnyje nustatytą už duomenų apsaugą atsakingo asmens ar padalinio funkciją prižiūrėti, kad asmens duomenys būtų tvarkomi laikantis įstatymų (Duomenų apsaugos įstatymo 32 str. 2 d.).

Duomenų apsaugos direktyvoje numatyta galimybė atleisti duomenų valdytoją nuo pareigos pranešti priežiūros institucijai prieš atliekant automatinę tvarkymo operaciją, jeigu paskiriamas asmens duomenų apsaugos pareigūnas (Duomenų apsaugos direktyvos 18 str.), nėra įtvirtinta Duomenų apsaugos įstatyme. Tačiau pagal Duomenų valdytojų pranešimo apie duomenų tvarkymą taisyklių, patvirtintų Lietuvos Respublikos Vyriausybės, 8 punktą, apie asmens duomenų tvarkymą Valstybinei duomenų apsaugos inspekcijai gali būti pranešama supaprastinta pranešimo tvarka, jeigu duomenų valdytojas yra paskyręs už duomenų apsaugą atsakingą asmenį ar padalinį.[164] Ši sąlyga skatina duomenų valdytojus paskirti duomenų apsaugos pareigūnus, tokiu būdu palengvinant duomenų valdytojų pareigas.

[162] Baker & McKenzie. *EU Data Protection Officer - Must Have, Nice to Have or Safe to Ignore?* 2016.
[163] Ibid.
[164] Duomenų valdytojų pranešimo apie duomenų tvarkymą taisyklės, patvirtintos Lietuvos Respublikos Vyriausybės 2002 m. vasario 20 d. nutarimu Nr. 262 (su pakeitimais ir papildymais). *Valstybės žinios*, 2002, nr. 20-768; TAR, 2015-09-11, nr. 13748.

2.5.2. Duomenų apsaugos pareigūno skyrimo pagrindai

Pagal Reglamentą duomenų apsaugos pareigūno skyrimas taps privalomas, tačiau ne visoms įmonėms, institucijoms ar įstaigoms, o tik toms, kurios nurodytos Reglamento 37 str. 1 d., pagal kurią duomenų valdytojas ir duomenų tvarkytojas privalo paskirti duomenų apsaugos pareigūną, kai:

- duomenis tvarko valdžios institucija arba įstaiga, išskyrus teismus, kai jie vykdo savo teismines funkcijas;
- duomenų valdytojo arba duomenų tvarkytojo pagrindinė veikla yra duomenų tvarkymo operacijos, dėl kurių pobūdžio, aprėpties ir (arba) tikslų būtina reguliariai ir sistemingai dideliu mastu stebėti duomenų subjektus; arba
- duomenų valdytojo arba duomenų tvarkytojo pagrindinė veikla yra specialių kategorijų duomenų[165] tvarkymas dideliu mastu pagal 9 str. ir 10 str. nurodytų asmens duomenų apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas tvarkymas dideliu mastu.[166]

Pagal šias nuostatas matoma, jog asmens duomenų pareigūnas privalomas toms įmonėms, institucijoms ar įstaigoms, kurių veikla galimai kelia didesnį pavojų asmens duomenims. Tačiau asmens duomenų pareigūno skyrimas galimas ir kitais, prieš tai nenurodytais atvejais (Reglamento 37 str. 4 d.). Savanoriška praktika skatinama ir 29 str. darbo grupės *Duomenų apsaugos pareigūnų gairėse*[167], kuriose pateikta rekomendacija paskirti asmens duomenų pareigūną net ir toms organizacijoms, kurioms šio pareigūno skyrimas nėra privalomas pagal Reglamentą ar nacionalinius teisės aktus.

Net jeigu paskirti asmens duomenų pareigūną nėra privaloma pagal Reglamentą, kartais toks paskyrimas gali suteikti organizacijai daug privalumų. Pavyzdžiui, bent laikinas asmens duomenų apsaugos pareigūno turėjimas galėtų būti labiausiai praktiškas ir mažiausiai išlaidų reikalaujantis sprendimas siekiant sukurti pasitikėjimą užtikrinančios organizacijos įvaizdį. Tai ypač aktualu verslo organizacijoms, kurios, turėdamos specialistą

[165] Pagal Duomenų apsaugos reglamento 9 straipsnį specialių kategorijų duomenys apima asmens duomenis, atskleidžiančius rasinę ar etninę kilmę, politines pažiūras, religinius ar filosofinius įsitikinimus ar narystę profesinėse sąjungose, taip pat genetinių duomenų ir biometrinių duomenų tvarkymą siekiant konkrečiai nustatyti fizinio asmens tapatybę, sveikatos duomenis arba duomenis apie fizinio asmens lytinį gyvenimą ar lytinę orientaciją.

[166] 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). *OL* L 119, 2016 5 4, p. 55.

[167] ES 29 str. duomenų apsaugos darbo grupė. *2016 m. gruodžio 13 d. Duomenų apsaugos pareigūnų gairės (su paskutiniais pakeitimais 2017 m. balandžio 5 d.).* Nr. 16/LT WP 243 rev.01, p. 5-7.

duomenų apsaugos srityje, galėtų daugiau dėmesio skirti kitoms sritims. Taip pat asmens duomenų pareigūno turėjimas palengvina bendradarbiavimą su priežiūros institucijoms.

Vis dėlto aiškinantis, kurioms organizacijoms asmens duomenų pareigūno paskyrimas yra privalomas, gali kilti sunkumų dėl pakankamai abstrakčių Reglamento 37 str. 1 d. vartojamų sąvokų, kurios nėra išaiškintos Reglamente. Tiesa, nagrinėjant *pagrindinės veiklos* sąvoką, ją šiek tiek paaiškina Reglamento preambulės 97 p., kuriame teigiama, jog privačiajame sektoriuje duomenų valdytojo pagrindinė veikla yra susijusi su jo svarbiausia veikla ir nesusijusi su asmens duomenų tvarkymu kaip papildoma veikla. 29 str. darbo grupės gairėse pateikiami pagrindinę veiklą aiškinantys pavyzdžiai. Vienas iš jų yra susijęs su ligoninėmis – nors jų pagrindinė veikla yra sveikatos priežiūros paslaugų teikimas, tačiau pacientų duomenų, susijusių su sveikata, tvarkymas yra būtinas sveikatos priežiūros paslaugų teikimui ligoninėse, todėl šis duomenų tvarkymas yra viena iš pagrindinių ligoninės veiklos sričių[168]. Tai reiškia, jog duomenų apsaugos pareigūno paskyrimas ligoninėms yra privalomas.

Sekanti Reglamento 37 str. 1 d. abstrakčiai pateikta sąvoka yra *didelis mastas*. Gairės šios sąvokos aiškinimui yra pateiktos Reglamento preambulės 91 p., pagal kurį didelio masto duomenų tvarkymo operacijos yra tos, kuriomis siekiama regioniniu, nacionaliniu ar viršnacionaliniu lygmeniu tvarkyti didelį kiekį asmens duomenų, kurios galėtų daryti poveikį daugeliui duomenų subjektų ir kurios gali kelti didelį pavojų, pavyzdžiui, dėl jų jautraus pobūdžio, kai atsižvelgiant į pasiektą technologinių žinių lygį nauja technologija yra naudojama dideliu mastu, taip pat taikoma kitoms duomenų tvarkymo operacijoms, kurios kelia didelį pavojų duomenų subjektų teisėms ir laisvėms, visų pirma, kai duomenų subjektams dėl šių operacijų yra sunkiau naudotis savo teisėmis.

29 str. darbo grupės gairėse pateikiamos rekomendacijos, turinčios padėti nustatyti, ar duomenų tvarkymas vykdomas dideliu mastu, atsižvelgiant į šiuos veiksnius:

- susijusių duomenų subjektų skaičių – konkretų skaičių arba atitinkamo gyventojų skaičiaus procentinę dalį;
- įvairių tvarkomų duomenų vienetų kiekį ir (arba) intervalą;
- duomenų tvarkymo veiklos trukmę arba pastovumą;
- geografinę duomenų tvarkymo veiklos aprėptį.[169]

Pagal šias rekomendacijas duomenų tvarkymo dideliu mastu pavyzdžiu galėtų būti jau prieš tai aptartas pacientų duomenų tvarkymas ligoninėse, tačiau kai paciento duomenis

[168] ES 29 str. duomenų apsaugos darbo grupė. *2016 m. gruodžio 13 d. Duomenų apsaugos pareigūnų gairės (su paskutiniais pakeitimais 2017 m. balandžio 5 d.), Nr. 16/LT WP 243 rev.01,* p. 8.
[169] Ibid., p. 9.

tvarko pavienis gydytojas – tai jau nėra laikoma duomenų tvarkymu dideliu mastu. Taip pat didelio masto duomenų tvarkymu laikoma asmens kelionių naudojantis viešojo transporto sistema duomenų tvarkymas (pvz., sekimas naudojant kelionės korteles), klientų duomenų tvarkymas draudimo bendrovės arba banko įprastinės veiklos metu, asmens duomenų tvarkymas paieškos sistemoje vartotojų elgesiu grindžiamos reklamos tikslais bei duomenų (turinio, srauto, vietos duomenų) tvarkymas, kai tai daro telefono ryšio arba interneto paslaugų teikėjai.[170]

Dar viena svarbi sąvoka vertinant, ar yra pareiga paskirti duomenų apsaugos pareigūną, yra *reguliarus ir sistemingas stebėjimas*. Ši sąvoka nėra apibrėžta nei Reglamento straipsniuose, nei paaiškinta jo preambulėje. Tačiau 29 str. darbo grupė pateikia paaiškinimus savo gairėse dėl duomenų apsaugos pareigūnų. Pagal šias gaires sąvoka *reguliarus* gali būti apibrėžiamas kaip:

- vykstantis arba pasitaikantis tam tikrais intervalais konkrečiu laikotarpiu;
- pasikartojantis arba kartojamas konkrečiu metu;
- vykstantis nuolat arba periodiškai.

Tuo tarpu sąvoka *sistemingas* reiškia, jog stebėjimas yra:

- vykstantis pagal tam tikrą sistemą;
- iš anksto suplanuotas, suorganizuotas arba metodiškas;
- vykdomas kaip bendro duomenų rinkimo plano dalis;
- vykdomas kaip strategijos dalis.[171]

Reguliaraus ir sistemingo stebėjimo pavyzdžiais gali būti telekomunikacijų paslaugų teikimas, vietos sekimas (pavyzdžiui, mobiliosiomis programėlėmis), pakartotinis kreipimasis e. paštu, lojalumo programos, vartotojų elgesiu grindžiama reklama, apsauginė vaizdo stebėjimo sistema, sujungtieji įrenginiai (daiktų internetas), pavyzdžiui, išmanieji skaitikliai, išmanieji automobiliai, namų automatizavimas ir kt.[172]

[170] ES 29 str. duomenų apsaugos darbo grupė. *2016 m. gruodžio 13 d. Duomenų apsaugos pareigūnų gairės (su paskutiniais pakeitimais 2017 m. balandžio 5 d.), Nr. 16/LT WP 243 rev.01,* p. 9-10.
[171] Ibid., p. 10.
[172] Ibid., p. 10-11.

2.5.3. Duomenų apsaugos pareigūno veiklos principai

Duomenų apsaugos pareigūnui, kaip ypač svarbiai naujosios ES duomenų apsaugos teisės sistemos daliai, keliami dideli reikalavimai. Analizuojant Reglamentą, galima išskirti penkis pagrindinius duomenų apsaugos pareigūno veiklos principus:

1. ekspertinės kompetencijos;
2. nepriklausomumo;
3. interesų konflikto vengimo;
4. prieinamumo;
5. veiklos formos laisvės.[173]

Ekspertinės kompetencijos principas įtvirtintas Reglamento 37 str. 5 d., pagal kurią duomenų apsaugos pareigūnas paskiriamas remiantis profesinėmis savybėmis, visų pirma duomenų apsaugos teisės ir praktikos ekspertinėmis žiniomis, taip pat gebėjimu atlikti jam įstatymu nurodytas užduotis. Pagal Reglamento preambulės 97 p., būtinas duomenų apsaugos pareigūno ekspertinių žinių lygis turėtų būti nustatomas visų pirma atsižvelgiant į atliekamas duomenų tvarkymo operacijas ir duomenų valdytojo arba duomenų tvarkytojo tvarkomų asmens duomenų reikiamą apsaugą.

29 str. darbo grupės gairės šiek tiek plačiau paaiškina ekspertinės kompetencijos principo turinį. Ekspertinių žinių lygis turi atitikti duomenų sudėtingumą, kiekį ir organizacinius procesus. Kuo sudėtingesnė duomenų tvarkymo veikla ir kuo daugiau yra tvarkytinų neskelbtinų duomenų, tuo aukštesnio lygio ekspertinių žinių galima reikalauti iš duomenų apsaugos pareigūno. Profesinės duomenų apsaugos pareigūno savybės suponuoja tai, jog yra privaloma išmanyti nacionalinės ir ES duomenų apsaugos teisės aktus, turėti praktinės patirties šioje srityje bei labai išsamiai suprasti Reglamentą[174]. Be to, rekomenduotina, jog priežiūros institucijos organizuotų duomenų apsaugos pareigūnų mokymą ir jų žinios būtų reguliariai atnaujinamos.[175]

Ekspertinės kompetencijos principo turiniui taip pat galima būtų priskirti ir duomenų apsaugos pareigūno asmenines savybes bei turimas žinias. Asmeninės savybės apima profesinį sąžiningumą, aukštą profesinę etiką, tuo tarpu turimos žinios turėtų būti suprantamos ne tik kaip žinios teisės srityje, bet rekomenduotina išmanyti ir duomenų

[173] ZALESKIS, Julius. Duomenų apsaugos pareigūno veiklos pagrindai pagal ES Bendrąjį duomenų apsaugos reglamentą. *Teisė*, 2017, t. 104, p. 166–168.
[174] LACHAUD, Eric. Should the DPO be certified? *International Data Privacy Law*, 2014, Vol. 4, No. 3, p. 109.
[175] ES 29 str. duomenų apsaugos darbo grupė. *2016 m. gruodžio 13 d. Duomenų apsaugos pareigūnų gairės (su paskutiniais pakeitimais 2017 m. balandžio 5 d.), Nr. 16/LT WP 243 rev.01,* p. 13.

valdytojo verslo sektorių bei organizacijos veiklos pobūdį, vykdomas duomenų tvarkymo operacijas, informacines sistemas, duomenų saugumo ir duomenų apsaugos poreikius bei kitus ypatumus[176].

Nei Reglamente, nei 29 str. darbo grupės gairėse nėra nieko užsimenama apie duomenų apsaugos pareigūnų kalbos įgūdžių reikalavimus. Tačiau iš praktinės pusės galima būtų rekomenduoti, kad organizacijos, ypač didesnės apimties ir turinčios ryšių su užsienio organizacijomis, paskirtų angliškai šnekančius duomenų apsaugos pareigūnus, kadangi anglų kalba šiuo metu yra labiausiai vartojama Europoje kaip tarpvalstybinė kalba.

Nepriklausomumo principas yra išvedamas iš Reglamento 38 str. 3 d., pagal kurią duomenų valdytojas ir duomenų tvarkytojas privalo užtikrinti, kad duomenų apsaugos pareigūnas negautų jokių nurodymų dėl savo užduočių atlikimo. Kitaip tariant, reikalaujama, kad duomenų apsaugos pareigūnas dirbtų nepriklausomai, neatsižvelgiant į tai, ar jis yra duomenų valdytojo darbuotojas (Reglamento preambulės 97 p.), ir kad nebūtų baudžiamas ar atleidžiamas iš pareigų dėl jam nustatytų užduočių atlikimo (Reglamento 38 str. 3 d.).

Nepriklausomumo principas yra neatsiejamas nuo duomenų valdytojo ir duomenų tvarkytojo pareigos suteikti duomenų apsaugos pareigūnui būtinus išteklius, skirtus užduočių atlikimui (Reglamento 38 str. 2 d.). Ištekliai apima ne tik finansinius išteklius, infrastruktūrą, bet ir vadovybės paramą, galimybę naudotis kitomis tarnybomis (pavyzdžiui, žmogiškųjų išteklių, teisės, IT ir kt.), nuolatinį mokymą, galimybę sudaryti duomenų apsaugos pareigūno grupę, jeigu to reikia atsižvelgiant į organizacijos dydį ir veiklos sudėtingumą[177].

Interesų konflikto vengimo principas atsispindi Reglamento 38 str. 6 d., kurioje įtvirtinama duomenų apsaugos pareigūno galimybė vykdyti kitas užduotis ir pareigas su sąlyga, jog duomenų valdytojas arba duomenų tvarkytojas užtikrina, kad dėl bet kokių tokių užduočių ir pareigų nekiltų interesų konfliktas. Šis principas pirmiausiai reiškia, kad duomenų apsaugos pareigūnas negali organizacijoje eiti pareigų, pagal kurias jis turėtų nustatyti asmens duomenų tvarkymo tikslus ir priemones[178]. Interesų konfliktas dažniausiai kiltų, jeigu duomenų apsaugos pareigūno pareigas atliktų asmenys, užimantys organizacijos vadovybės pareigas. Tačiau konfliktas gali kilti net ir tuo atveju, kai duomenų apsaugos pareigūno pareigas atlieka išorinis specialistas, pavyzdžiui, jeigu jis atstovautų duomenų valdytojui teisme, bylose susijusiose su duomenų apsaugos klausimais.

[176] ES 29 str. duomenų apsaugos darbo grupė. *2016 m. gruodžio 13 d. Duomenų apsaugos pareigūnų gairės (su paskutiniais pakeitimais 2017 m. balandžio 5 d.), Nr. 16/LT WP 243 rev.01,* p. 14.
[177] Ibid., p. 16-17.
[178] Ibid., p. 18.

Prieinamumo principas yra glaudžiai susijęs su duomenų valdytojo arba duomenų tvarkytojo pareiga paskelbti duomenų apsaugos pareigūno kontaktinius duomenis ir pranešti juos priežiūros institucijai (Reglamento 37 str. 7 d.). Šio principo esmė yra tai, kad kiekvienas suinteresuotas asmuo galėtų lengvai ir tiesiogiai susisiekti su duomenų apsaugos pareigūnu, neprivalėdamas į jį kreiptis per kitą organizacijos padalinį[179]. Į pateikiamus kontaktinius duomenų apsaugos pareigūno duomenis turėtų būti įtraukta bent vardas ir pavardė, telefono numeris, elektroninio pašto adresas ir buveinės adresas. Visiems suinteresuotiems asmenims turi būti sudaryta galimybė kreiptis į duomenų apsaugos pareigūną bent jau ryšių priemonių pagalba, jeigu fizinis kreipimasis yra praktiškai neįmanomas arba sunkiai įgyvendinamas.

Lengvas susisiekimas su duomenų apsaugos pareigūnu yra ypač aktualus, kai kelioms organizacijoms yra paskiriamas vienas bendras duomenų apsaugos pareigūnas (Reglamento 37 str. 2 d.). Duomenų apsaugos pareigūnas yra kontaktinis asmuo tiek duomenų subjektams (Reglamento 38 str. 4 d.: Duomenų subjektai gali kreiptis į duomenų apsaugos pareigūną visais klausimais, susijusiais su jų asmeninių duomenų tvarkymu ir naudojimusi savo teisėmis pagal šį reglamentą), tiek ir priežiūros institucijoms (Reglamento 39 str. 1 d. e) p.: atlieka kontaktinio asmens funkcijas priežiūros institucijai kreipiantis su duomenų tvarkymu susijusiais klausimais, įskaitant 36 str. nurodytas išankstines konsultacijas, ir prireikus konsultuoja visais kitais klausimais), todėl jis turi būti lengvai pasiekiamas iš bet kurios buveinės.

Esant įmonių grupei gali būti netgi naudingiau paskirti vieną bendrą duomenų apsaugos pareigūną. Tačiau darant sprendimą, turėtų būti išanalizuoti ir įvertinti daugybė veiksnių, tokių kaip įmonių struktūra, procesai, veikimo principai ir kita. Sprendimas paskirti vieną centrinį duomenų apsaugos pareigūną yra ypač efektyvus, jeigu įmonės yra glaudžiai susijusios savo veikla. Šiuo atveju toks sprendimas įmonių grupei gali palengvinti strategijų, taisyklių ir ateities verslo planų kūrimą visos įmonių grupės mastu.

Veiklos formos laisvės principas reiškia tai, jog duomenų apsaugos pareigūnas gali būti duomenų valdytojo arba duomenų tvarkytojo personalo narys arba atlikti užduotis pagal paslaugų teikimo sutartį (Reglamento 37 str. 6 d.). Kitaip tariant, reikia pasirinkti tarp vidinio ir išorinio duomenų apsaugos pareigūno. Didesnėse organizacijose paprastai yra nuolatines pareigas turintis teisininkas ar net visas teisės skyrius, todėl tokiu atveju gali būti efektyviau duomenų apsaugos pareigūno pareigas paskirti jau esančiam organizacijos

[179] ES 29 str. duomenų apsaugos darbo grupė. *2016 m. gruodžio 13 d. Duomenų apsaugos pareigūnų gairės (su paskutiniais pakeitimais 2017 m. balandžio 5 d.), Nr. 16/LT WP 243 rev.01,* p. 14.

darbuotojui. Tuo labiau, jog organizacijos teisininkas puikiai išmano organizacijos ypatumus.

Sprendžiant, ar paskirti vidinį, ar išorinį duomenų apsaugos pareigūną, reikėtų išanalizuoti visus galimus veiksnius. Vidinis duomenų apsaugos pareigūnas dažniausiai puikiai išmano organizacijos veiklą ir turi daugiau žinių toje konkrečioje srityje, tačiau iš išorės pasamdytas ekspertas yra patyręs duomenų apsaugos srityje ir gali turėti reikalingos patirties dirbant su skirtingomis organizacijomis. Be to, duomenų apsaugos pareigūno funkcijų suteikimas jau esančiam organizacijos darbuotojui galėtų sumažinti finansines išlaidas ir taip pat organizacijos vidiniai reikalai nebūtų atskleidžiami trečiajam asmeniui. Vis dėlto, toks dvigubų pareigų atlikimas organizacijoje turėtų būti deramai suderintas, kad asmens duomenų pareigūno pareigų įgyvendinimui būtų suteikta pakankamai laiko.

Sisteminė analizė atskleidžia, jog Reglamentas įtvirtina nemažai su duomenų apsaugos pareigūnu susijusių reikalavimų. Nors tai sukels didesnę naštą duomenų valdytojams ir duomenų tvarkytojams, duomenų apsaugos pareigūnas padės užtikrinti, jog duomenų apsaugos taisyklės yra įgyvendinamos tinkamai. Jis taip pat bus svarbus stebint, kaip laikomasi Reglamento, ir konsultuojant visais kitais su asmens duomenų apsauga susijusiais klausimais. Sprendžiant visus su duomenų apsaugos pareigūnu susijusius klausimus, ypač vertinant, ar duomenų apsaugos pareigūnas yra būtinas, rekomenduojama vadovautis 29 str. darbo grupės gairėmis, išsamiai išaiškinančiomis Reglamento nuostatų taikymo ypatumus.

3. BENDROJO DUOMENŲ APSAUGOS REGLAMENTO VIETA TEISĖS ŠALTINIŲ SISTEMOJE

3.1. Valstybėms narėms suteikiama diskrecijos teisė

Reglamentas yra taikomas tiesiogiai ir juo siekiama užtikrinti teisinį tikrumą, suvienodinant duomenų apsaugos reguliavimą visose ES valstybėse narėse. Tačiau tam tikrose srityse valstybėms narėms leidžiama nustatyti nacionalines nuostatas, kuriomis konkrečiau apibrėžiamas Reglamente nustatytų taisyklių taikymas (Reglamento preambulės 10 p.). Kitaip tariant, Reglamente nurodytais atvejais valstybės narės turi diskrecijos teisę nustatyti savo nacionalines taisykles duomenų apsaugos srityje, papildančias Reglamento nuostatas.

Reglamente randama apie 50 nuostatų, leidžiančių valstybėms narėms šiose nuostatose numatytose srityse priimti nacionalines taisykles. Tai suteikia teisinį lankstumą, sudarantį galimybę valstybėms narėms priderinti duomenų apsaugos teisę prie visuomenės savitumo ir jau galiojančio teisinio reguliavimo. Todėl tam tikri skirtumai tarp valstybių narių duomenų apsaugos teisinio reguliavimo išliks net ir pradėjus taikyti Reglamentą.

Viena iš svarbiausių sričių, suteikiančių valstybėms narėms lankstumą, yra galimybė apriboti duomenų subjekto teises siekiant užtikrinti: a) nacionalinį saugumą; b) gynybą; c) visuomenės saugumą; d) nusikalstamų veikų prevenciją, tyrimą, nustatymą ar patraukimą už jas baudžiamojon atsakomybėn arba baudžiamųjų sankcijų vykdymą; e) kitus Sąjungos ar valstybės narės svarbius tikslus, susijusius su bendrais viešaisiais interesais; f) teismų nepriklausomumo ir teismo proceso apsaugą; g) reglamentuojamųjų profesijų etikos pažeidimų prevenciją, tyrimą, nustatymą ir patraukimą baudžiamojon atsakomybėn už juos; h) stebėsenos, tikrinimo ar reguliavimo funkciją, kuri yra susijusi su viešosios valdžios funkcijų vykdymu; i) duomenų subjekto apsaugą arba kitų asmenų teisių ir laisvių apsaugą; j) civilinių ieškinių vykdymo užtikrinimą (Reglamento 23 str. 1 d.).

Tačiau bet kuriuo iš šių pagrindų skiriamas apribojimas yra galimas tik tuo atveju, kai jis yra būtinas ir proporcingas demokratinėje visuomenėje bei yra gerbiama pagrindinių teisių ir laisvių esmė. Be to, valstybė narė, numatydama apribojimą, savo nacionaliniuose teisės aktuose taip pat privalo įtvirtinti išsamias su apribojimu susijusias nuostatas, nurodančias tokius aspektus kaip apribojamos teisės, apribojimo tikslas, apribojimo apimtis, apsaugos priemonės, užkertančios kelią apribojimo piktnaudžiavimui (Reglamento 23 str. 2 d.).

Kitos svarbios nuostatos, leidžiančios valstybėms narėms šiek tiek nukrypti nuo vadovavimosi vien tik Reglamentu, yra įtvirtintos Reglamento devintajame skyriuje –

nuostatos, susijusios su konkrečiais duomenų tvarkymo atvejais. Valstybės narės, siekdamos numatyti konkretesnes taisykles ar tiksliau apibrėžti tam tikras sąlygas, gali priimti specialias nuostatas, susijusias su duomenų tvarkymu ir saviraiškos ir informacijos laisve (85 str.), duomenų tvarkymu ir visuomenės teise susipažinti su oficialiais dokumentais (86 str.), nacionalinio asmens identifikavimo numerio tvarkymu (87 str.), duomenų tvarkymu su darbo santykiais susijusiame kontekste (88 str.), apsaugos priemonėmis ir nukrypti leidžiančiomis nuostatomis, susijusiomis su duomenų tvarkymu archyvavimo tikslais viešojo intereso labui, mokslinių ar istorinių tyrimų tikslais arba statistiniais tikslais (89 str.), prievolėmis saugoti paslaptį (90 str.) bei galiojančiomis bažnyčių ir religinių asociacijų duomenų apsaugos taisyklėmis (91 str.).

Diskrecija valstybėms narėms iš dalies suteikiama ir nustatant vaiko amžių, nuo kurio jo duomenų tvarkymui, siūlant informacinės visuomenės paslaugas, nebereikia tėvų sutikimo. Reglamentas nustato 16 metų ribą, tačiau suteikia galimybę valstybėms narėms numatyti jaunesnio amžiaus ribą su sąlyga, kad toks jaunesnis amžius reiškia ne mažiau nei 13 metų (Reglamento 8 str. 1 d.). Šia galimybe pasinaudojo Austrija, Airija ir Jungtinė Karalystė, kurios jau priėmė savo nacionalinių duomenų apsaugos įstatymų pakeitimus. Austrija numatė 14 metų, o Airija ir Jungtinė Karalystė – 16 metų amžiaus ribą. Yra didelė tikimybė, jog ir kitos valstybės narės laikysis nuomonės, kad ir jaunesni nei 16 metų vaikai gali patys priimti tinkamus sprendimus dėl sutikimo tvarkyti jų duomenis davimo.[180]

Dar viena sąlyga, suteikianti valstybėms narėms diskrecijos teisę, yra susijusi su duomenų apsaugos pareigūno skyrimu. Nacionalinėje teisėje gali būti įtvirtinami reikalavimai paskirti duomenų apsaugos pareigūną papildomais, Reglamente nenurodytais atvejais (Reglamento 37 str. 4 d.). Greičiausiai tokie papildomi reikalavimai bus įtvirtinti tų valstybių nacionaliniuose įstatymuose, kuriose dar iki Reglamento priėmimo duomenų apsaugos pareigūnas buvo privalomas. Viena iš tokių valstybių yra Vokietija, kuri pirmoji priėmė duomenų apsaugos įstatymo pakeitimus ir nustatė reikalavimą paskirti duomenų apsaugos pareigūną visiems duomenų valdytojams ar duomenų tvarkytojams, kurie yra įdarbinę bent 10 darbuotojų.[181]

Taip pat valstybės narės savo teisėje gali įtvirtinti detalizuotą duomenų valdytojo sąvoką, išskiriant konkrečius duomenų valdytojo skyrimo kriterijus (Reglamento 4 str. 7 p.). Be to, leidžiama nustatyti konkretesnes sąlygas, reikalingas teisėtam duomenų tvarkymui, kiek tai susiję su duomenų valdytojui taikoma teisine prievole, pavestomis

[180] Information Commissioner's Office. *ICO submission to the inquiry of the House of Lords Select Committee on Communications into Children and the Internet*. 2016, p. 13.
[181] Germany's Act to Adapt Data Protection Law to Regulation (EU) 2016/679 and to Implement Directive (EU) 2016/680. 2017, Section 38.

viešosios valdžios funkcijomis ar viešuoju interesu (6 str. 2 d.). Suteikiama teisė nustatyti specialių kategorijų asmens duomenų tvarkymo taisykles (9 str.), asmens duomenų apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas tvarkymo taisykles (10 str.), taisykles dėl automatizuoto atskirų sprendimų priėmimo, įskaitant profiliavimą (22 str.). Valstybės narės gali numatyti papildomus priežiūros institucijos įgaliojimus (28 str. 6 d.) bei privalo nustatyti priežiūros institucijos įsteigimo taisykles (54 str.).

Apibendrinant galima teigti, jog net ir pradėjus taikyti Reglamentą, valstybių nacionaliniai duomenų apsaugos įstatymai išliks svarbi duomenų apsaugos teisės šaltinių sistemos dalis. Pagal visas aptartas nuostatas, suteikiančias valstybėms narėms diskrecijos teisę papildyti, patikslinti, detalizuoti Reglamento nustatomą teisinį reguliavimą ar minimaliai nuo jo nukrypti, matoma, jog ES duomenų apsaugos teisė nebus visiškai suvienodinta. Kiekvienai organizacijai, norinčiai veikti kitoje valstybėje ir tvarkyti joje esančių asmenų duomenis, vis tiek teks susipažinti ir su tos valstybės duomenų apsaugos teisiniu reguliavimu. Šiuo metu yra sudėtinga numatyti duomenų apsaugos skirtumus tarp valstybių, nes jie priklausys nuo to, kokius nacionalinių duomenų apsaugos įstatymų pakeitimus priims kiekviena iš ES valstybių narių.

3.2. Reglamentas ir LR duomenų apsaugos įstatymo pakeitimo projektas

Lietuva, kaip ir visos kitos ES valstybės narės, ruošiasi su Reglamentu susijusiems pokyčiams. 2018 m. gegužės 25 d. pradėjus taikyti Reglamentą, tą pačią dieną įsigalios Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo Nr. I-1374 nauja redakcija (toliau – Duomenų apsaugos įstatymo pakeitimo projektas)[182] ir šis įstatymas bus taikomas kartu su Reglamentu ir jo įgyvendinamaisiais teisės aktais. Nepaisant to, jog Reglamentas bus taikomas tiesiogiai visose ES valstybėse narėse, Lietuvos Respublikos duomenų apsaugos įstatymas vis tiek išliks labai svarbi Lietuvos duomenų apsaugos teisės sistemos dalis.

Kaip jau buvo aptarta prieš tai, Reglamentas tam tikrose srityse palieka diskrecijos teisę valstybėms narėms papildyti ar detalizuoti Reglamente įtvirtintas nuostatas. Todėl naujasis Duomenų apsaugos įstatymas nustatys kai kurių asmens duomenų tvarkymo atvejų ypatumus, Valstybinės duomenų apsaugos inspekcijos veiklos teisinius pagrindus ir įgaliojimus, kitų valstybės institucijų, formuojančių valstybės politiką asmens duomenų

[182] Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo Nr. I-1374 pakeitimo įstatymo projektas. 2018-02-15, nr. 17-7645(2).

apsaugos srityje ir atliekančių Reglamento ir šio įstatymo taikymo stebėseną, įgaliojimus, taip pat pažeidimų nagrinėjimo ir administracinių baudų skyrimo tvarką.

Pirmiausiai yra pasinaudojama Reglamento 87 str. valstybėms narėms numatyta galimybe tiksliau apibrėžti konkrečias sąlygas, kuriomis tvarkomas nacionalinis asmens identifikavimo numeris. Dabar galiojančio Duomenų apsaugos įstatymo 7 str. 2 d. yra nurodyta, jog naudoti asmens kodą, kai tvarkomi asmens duomenys, galima tik gavus duomenų subjekto sutikimą.[183] Nors to paties straipsnio 3 d. numato dar kelis atvejus, pagal kuriuos asmens kodą galima naudoti be duomenų subjekto sutikimo, pagal tokią įstatymo formuluotę galima pastebėti, jog įstatymo leidėjas šiuos atvejus laiko išimtiniais, o pagrindinė taisyklė yra tai, jog asmens kodo tvarkymui būtinas asmens sutikimas.

Tuo tarpu Duomenų apsaugos įstatymo pakeitimo projekto 3 str. 1 d. nustatoma, jog asmens kodas gali būti tvarkomas, jei yra nors viena iš Reglamento 6 str. 1 d. nurodytų asmens duomenų tvarkymo teisėtumo sąlygų. Šių sąlygų yra net šešios, tarp kurių viena yra ir duomenų subjekto duotas sutikimas. Tai reiškia, jog, įsigaliojus Duomenų apsaugos įstatymo naujajai redakcijai, padaugės teisinių pagrindų, pagal kuriuos bus galima tvarkyti asmens kodą. Be to, visi šie pagrindai bus laikomi lygiaverčiais, neišskiriant duomenų subjekto duoto sutikimo kaip svarbiausio pagrindo.

Vis dėlto Duomenų apsaugos įstatymo pakeitimo projekte nustatomos papildomos taisyklės lyginant su Reglamento nuostatomis. Nurodoma, jog yra draudžiama asmens kodą skelbti viešai bei draudžiama tvarkyti asmens kodą tiesioginės rinkodaros tikslais (Duomenų apsaugos įstatymo pakeitimo projekto 3 str. 2 ir 3 d.). Be to, šie draudimai galioja net ir gavus duomenų subjekto sutikimą. Tiesa, analogiški draudimai Lietuvoje galioja ir pagal dabartinį Duomenų apsaugos įstatymą, todėl, net ir pradėjus taikyti Reglamentą, Lietuva išlaikys dalį nacionalinių ypatumų, susijusių su asmens kodo tvarkymu.

Reglamentas taip pat leidžia ES valstybių narių teisėje ar kolektyvinėse sutartyse numatyti konkretesnes taisykles tvarkant darbuotojų asmens duomenis su darbo santykiais susijusiame kontekste (Reglamento 88 str. 1 d.). Dabartiniame Duomenų apsaugos įstatyme nėra atskirai reglamentuotas darbuotojų asmens duomenų tvarkymas. Vienintelis numatytas ypatumas dėl darbuotojų asmens duomenų yra susijęs su vaizdo stebėjimu darbo vietoje – vaizdo stebėjimas darbo vietoje gali būti vykdomas, kai dėl darbo specifikos būtina užtikrinti asmenų, turto ar visuomenės saugumą, tačiau darbuotojai apie tokį

[183] Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas (su pakeitimais ir papildymais). *Valstybės žinios*, 1996, nr. 63-1479.

stebėjimą turi būti pasirašytinai informuojami (Duomenų apsaugos įstatymo 17 str. ir 20 str. 3 d.).

Tuo tarpu Duomenų apsaugos įstatymo pakeitimo projektas numato atskirą straipsnį, skirtą asmens duomenų tvarkymo su darbo santykiais susijusiame kontekste ypatumams detalizuoti. Tiesa, naujoje įstatymo redakcijoje bus laikomasi panašios taisyklės dėl vaizdo stebėjimo darbo vietoje, kuri yra įtvirtinta ir dabar. Tačiau nuo šiol darbuotojo stebėsena apims ne tik vaizdo, bet ir garso duomenis, o taip pat ir darbuotojų elgesio, vietos ar judėjimo stebėsenai bus taikomas toks pats reikalavimas apie stebėseną informuoti stebimą darbuotoją (Duomenų apsaugos įstatymo pakeitimo projekto 5 str. 3 d.).

Taip pat, įsigaliojus Duomenų apsaugos įstatymo pakeitimams, duomenų valdytojas galės rinkti tik tuos kandidato, pretenduojančio eiti pareigas arba dirbti darbus, asmens duomenis, kurie yra susiję su kvalifikacija, profesiniais gebėjimais ir dalykinėmis savybėmis. Tačiau, jeigu šie duomenys bus renkami iš buvusio darbdavio, kandidatas prieš tai privalo būti informuotas apie rinkimą, o iš esamo darbdavio duomenis galima bus rinkti tik esant kandidato sutikimui (Duomenų apsaugos įstatymo pakeitimo projekto 5 str. 2 d.). Iki šiol teisė rinkti asmens duomenis iš buvusio ar esamo darbdavio nebuvo reglamentuota, todėl tokia nuostata papildo ir konkretizuoja esamą reguliavimą.

Be to, bus draudžiama tvarkyti kandidato ir darbuotojo asmens duomenis apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas, išskyrus atvejus, kai šie duomenys būtini patikrinti, ar asmuo atitinka įstatymuose nustatytus reikalavimus pareigoms eiti arba darbams dirbti (Duomenų apsaugos įstatymo pakeitimo projekto 5 str. 1 d.). Šis draudimas sugriežtina dabartinį reguliavimą ir tam tikrais atvejais tai gali neigiamai paveikti darbdavius, kurie patiki darbuotojui didelės vertės turto priežiūrą, negalėdami patikrinti darbuotojų teistumo.

Lietuva pasinaudoja diskrecijos teise taip pat ir nustatydama vaiko, kuriam siūlomos informacinės visuomenės paslaugos, amžių, reikalingą duoti sutikimą duomenų tvarkymui. Reglamentas nustato 16 metų amžiaus ribą, tačiau valstybėms narėms leidžiama sumažinti šią ribą iki 13 metų (Reglamento 8 str. 1 d.). Taigi, Duomenų apsaugos įstatymo pakeitimo projekto 6 str. numato 14 metų amžiaus ribą.

Naujasis Duomenų apsaugos įstatymas bus svarbus duomenų apsaugos teisės šaltinis dar ir dėl to, jog įtvirtina teisinį pagrindą priežiūros institucijoms Lietuvoje – Valstybinei duomenų apsaugos inspekcijai ir Žurnalistų etikos inspektoriui (Duomenų apsaugos įstatymo pakeitimo projekto 10 str.). Taip pat reglamentuojamas Valstybinės duomenų apsaugos inspekcijos teisinis statusas, veiklos principai, užduotys, įgaliojimai, teisės bei funkcijos, kurios yra išplėstos lyginant su Reglamentu pavestomis funkcijomis.

Vis dėlto naujoji Duomenų apsaugos įstatymo redakcija labiausiai papildys Reglamentu nustatomą teisinį reguliavimą būtent priežiūros institucijų atliekamo pažeidimų nagrinėjimo srityje. Duomenų apsaugos įstatymo pakeitimo projektas nurodo, jog Valstybinės duomenų apsaugos inspekcija savo iniciatyva gali pradėti tyrimą ar tikrinimą bet kokiu klausimu, susijusiu su galimu Reglamento, šio įstatymo ir kitų įstatymų, reglamentuojančių asmens duomenų ir (ar) privatumo apsaugą, pažeidimu (Duomenų apsaugos įstatymo pakeitimo projekto 23 str. 1 d.). Taip pat detalizuojama su skundų nagrinėjimu susijusi tvarka, konkrečiai reglamentuojant skunde privalomą nurodyti informaciją, skundo pateikimo tvarką, atsisakymo nagrinėti skundą pagrindus ir kitus svarbius aspektus.

Valstybinė duomenų apsaugos inspekcija, išnagrinėjusi skundą ir pripažinusi jį pagrįstu, gali imtis ne tik Reglamento 58 str. 2 d. nurodytų taisomųjų veiksmų, tokių kaip duomenų valdytojo ar duomenų tvarkytojo įspėjimas, papeikimo pareiškimas, nurodymas patenkinti duomenų subjekto prašymą, duomenų tvarkymo apribojimo nustatymas ar administracinės baudos skyrimas, tačiau turi ir papildomą Duomenų apsaugos įstatymo pakeitimo projekte įtvirtintą įgaliojimą surašyti administracinio nusižengimo protokolą asmens duomenų ir (ar) privatumo apsaugos pažeidimą padariusiam asmeniui (Duomenų apsaugos įstatymo pakeitimo projekto 34 str. 2 d. 2 p.). Taigi, Lietuvos duomenų apsaugos teisė išplečia Reglamente nustatytus priežiūros institucijos įgaliojimus.

Taip pat Duomenų apsaugos įstatymo pakeitimo projekte detalizuojamas dar vienas labai svarbus aspektas – administracinių baudų skyrimas. Numatoma, jog administracines baudas už Reglamento ir Duomenų apsaugos įstatymo pažeidimus pagal kompetenciją skiria Valstybinės duomenų apsaugos inspekcijos direktorius arba žurnalistų etikos inspektorius ar jų įgaliotas asmuo (Duomenų apsaugos įstatymo pakeitimo projekto 35 str.). Be to, reglamentuojama, kokio dydžio administracinė bauda gali būti skiriama valdžios institucijomis ir įstaigoms, bei nustatoma detali administracinių baudų skyrimo procedūros tvarka.

Išnagrinėjus Duomenų apsaugos įstatymo pakeitimo projektą galima teigti, jog tam tikrose srityse Lietuva pasinaudojo Reglamento suteikiama galimybe šiek tiek nukrypti nuo jo taisyklių ar jas detalizuoti, įtvirtinant nacionalinio duomenų apsaugos teisinio reguliavimo ypatumus. Dėl šių esančių skirtumų, lyginant su Reglamentu, organizacijos privalės susipažinti ir su Duomenų apsaugos įstatymu, kuris papildys Reglamentą ir išliks svarbus duomenų apsaugos teisės šaltinis Lietuvos lygmeniu.

3.3. Reglamentas ir LR darbo kodeksas

Nepaisant to, jog Reglamentu siekiama suvienodinti duomenų apsaugos teisę visose ES valstybėse narėse, tam tikri skirtumai yra neišvengiami. Tai lemia egzistuojančios ribos tarp Europos Sąjungos ir valstybių narių turimos kompetencijos konkrečiose srityse. Darbuotojų asmens duomenų apsauga su darbo santykiais susijusiame kontekste yra viena iš šių sričių, kuriose Reglamentas suteikia galimybę nacionaliniams ypatumams nustatyti. Šie ypatumai Lietuvoje pasireikš ne tik naujoje Duomenų apsaugos įstatymo redakcijoje, bet ir išliks įtvirtinti Lietuvos Respublikos darbo kodekse.

Kaip jau buvo aptarta, valstybės narės gali teisėje ar kolektyvinėse sutartyse numatyti konkretesnes taisykles, kuriomis siekiama užtikrinti teisių ir laisvių apsaugą tvarkant darbuotojų asmens duomenis su darbo santykiais susijusiame kontekste. Asmens duomenų apsaugai šioje srityje turėtų būti skiriamas ypač didelis dėmesys dėl darbuotojų ir darbdavių santykių pobūdžio – darbuotojai yra finansiškai priklausomi nuo darbdavio. Dėl šalių padėties disbalanso darbuotojas retai gali duoti visiškai savanorišką sutikimą tvarkyti jo duomenis, bijodamas apsunkinti santykius su darbdaviu ar net prarasti darbą (Reglamento preambulės 43 p.). Todėl konkrečios taisyklės, ribojančios darbdavių galimybes tvarkyti darbuotojų duomenis, turėtų būti detalizuojamos įstatymuose.

Lietuvos teisinėje sistemoje pagrindinės asmens duomenų apsaugos taisyklės su darbo santykiais susijusiame kontekste yra įtvirtintos Darbo kodekso 27 straipsnyje. Šio straipsnio pirmoje dalyje nustatytas pamatinis reikalavimas darbdaviui gerbti darbuotojo teisę į privatų gyvenimą, užtikrinti darbuotojo asmens duomenų apsaugą.[184] Taip pat įtvirtintas draudimas tvarkyti su darbo reikmėmis nesusijusius (perteklinius) darbuotojo asmens duomenis. Šiuo reikalavimu įgyvendinamas duomenų kiekio mažinimo principas, pagal kurį turi būti tvarkomi tik tie asmens duomenys, kurie yra būtini siekiant tikslų (Reglamento 5 str. 1 d. c) p.).

Darbo kodeksas įtvirtina dar vieną svarbią darbdavio pareigą – supažindinti darbuotojus su informacinių ir komunikacinių technologijų naudojimo bei darbuotojų stebėsenos ir kontrolės darbo vietoje tvarka. Nors nėra įtvirtinta, kaip konkrečiai darbuotojai turėtų būti supažindinami su šia tvarka, tačiau tai gali įgyvendinti specialios darbo sutarties nuostatos ar atskiras dokumentas, detaliai reguliuojantis darbuotojų teises naudotis darbdavio suteiktomis informacinėmis ir komunikacinėmis technologijomis,

[184] Lietuvos Respublikos darbo kodeksas (su pakeitimais ir papildymais). *TAR*, 2016-09-19, nr. 23709.

įgyvendinamas darbuotojų stebėsenos ir kontrolės priemones bei tokiu būdu surinktos informacijos naudojimo tikslus, terminus ir kitus susijusius aspektus.

Naujuoju Darbo kodeksu taip pat buvo nustatyta nauja darbdavio pareiga priimti atskirą vidinį darbovietės dokumentą – darbuotojų asmens duomenų saugojimo politiką ir jos įgyvendinimo priemones. Tiesa, ši pareiga yra taikoma ne visiems darbdaviams, o tik tiems, kurių vidutinis darbuotojų skaičius yra daugiau kaip penkiasdešimt. Darbuotojų asmens duomenų saugojimo politika turėtų apimti nuostatas, susijusias su renkamais darbuotojų asmens duomenimis, jų tvarkymo būdais, darbuotojų teisėmis duomenų apsaugos srityje bei duomenų saugumo užtikrinimo priemonėmis. Šio dokumento priėmimas aiškiau apibrėžia darbuotojų asmens duomenų tvarkymą ir sumažina tikimybę kilti ginčams tarp darbdavio ir darbuotojo dėl pažeistų asmens duomenų apsaugos teisių.

Tačiau, ruošiantis pradėti taikyti Reglamentą, buvo paruoštas Darbo kodekso 27 straipsnio pakeitimo įstatymo projektas, įsigaliosiantis 2018 m. gegužės 25 d.[185] Šis projektas sumažina su darbuotojo asmens duomenų ir jo teisės į privatų gyvenimą apsauga susijusio straipsnio apimtį. Jame išliks vos trys dabartinėje Darbo kodekso 27 straipsnio redakcijoje esančios normos – pamatinė darbdavio pareiga gerbti darbuotojo teises į privatų gyvenimą ir į asmens duomenų apsaugą; draudimas pažeisti darbuotojo asmeninio susižinojimo slaptumą darbdaviui įgyvendinant nuosavybės ar valdymo teises į darbo vietoje naudojamas informacines ir komunikacines technologijas; sąlyga, jog darbuotojo teisės į privatų gyvenimą įgyvendinimo ypatumus gali nustatyti įstatymai ir kitos darbo teisės normos.

Pastebima, jog dabartinė Darbo kodekso norma dėl vaizdo stebėjimo ir garso įrašymo darbo vietoje yra perkeliama į Duomenų apsaugos įstatymo pakeitimo projektą, o kitos normos taip pat gali būti netiesiogiai išvedamos iš Reglamento ar Duomenų apsaugos įstatymo pakeitimo projekto. Tačiau pagal Darbo kodekso pakeitimo projektą nebeliks prieš tai aptartų darbdavio pareigų – supažindinti darbuotojus su informacinių ir komunikacinių technologijų naudojimo bei darbuotojų stebėsenos ir kontrolės darbo vietoje tvarka; priimti darbuotojų asmens duomenų saugojimo politiką ir jos įgyvendinimo priemones. Todėl negali būti vienareikšmiškai teigiama, jog konkrečių darbuotojų asmens duomenis saugančių normų pašalinimas ir kitų patobulintų normų neįtvirtinimas Darbo kodekse nesukels neigiamų pasekmių darbuotojų asmens duomenų apsaugai.

Nepaisant minimalaus darbuotojo asmens duomenų ir jo teisės į privatų gyvenimą apsaugos reguliavimo, numatyto Darbo kodekso 27 straipsnio pakeitimo įstatymo projekte,

[185] Lietuvos Respublikos darbo kodekso 27 straipsnio pakeitimo įstatymo projektas. 2018-02-15, nr. 18-1820.

darbdaviai, rinkdami ir tvarkydami darbuotojų ir kandidatų į darbuotojus asmens duomenis, privalo laikytis fundamentalių duomenų apsaugos principų ir taisyklių. Taip pat reikėtų vadovautis 29 str. darbo grupės *Nuomone 2/2017 dėl duomenų tvarkymo darbe*, kurioje apibūdinami naujų technologijų keliami pavojai ir atliekamas įvairių scenarijų, vykstančių atliekant skirtingas duomenų tvarkymo operacijas, proporcingumo vertinimas.[186]

Kaip nurodo 29 str. darbo grupė, didžiausią grėsmę darbuotojo privatumui kelia jo elektroninių ryšių stebėjimas darbo vietoje. Tobulėjančios technologijos darbdaviams suteikia vis daugiau galimybių stebėti darbuotojų elektroninį susirašinėjimą, kuris gali būti ir asmeninio pobūdžio. Todėl prieš pradėdami stebėti darbuotojų elektroninius ryšius ir jų turinį, darbdaviai privalo įvertinti savo veiksmų proporcingumą ir nustatyti, ar įmanomos kitos priemonės, leidžiančios sumažinti duomenų tvarkymo mastą ir poveikį. Taip pat darbdaviai turi priimti politikos priemones, nurodančias, kaip leidžiama naudoti organizacijos elektroninius ryšius ir kaip tvarkomi darbuotojų asmens duomenys.[187]

Europos Žmogaus Teisių Teismas 2017 m. byloje *Barbulescu prieš Rumuniją* nustatė šešis veiksnius, pagal kuriuos turėtų būti vertinamas darbuotojų elektroninio susirašinėjimo stebėjimo teisėtumas: 1) darbuotojo informavimas apie jo susirašinėjimo stebėjimo galimybę ir įspėjimas prieš pradedant stebėjimą; 2) stebėjimo laipsnis ir privatumo apribojimo mastas; 3) darbdavio siekiamo tikslo teisėtumas; 4) vertinimas, ar tikslo siekimui galėtų būti pasitelktos mažiau darbuotojo privatumą ribojančios priemonės; 5) stebėjimo pasekmių darbuotojui vertinimas; 6) apsaugos priemonių darbuotojui užtikrinimas.[188]

Taigi, nors įsigaliojus Darbo kodekso 27 straipsnio pakeitimams išliks vos kelios su darbuotojo asmens duomenų apsauga susijusios normos, darbdaviai, nustatydami darbuotojų asmens duomenų rinkimo ir tvarkymo priemones, turės vadovautis Reglamente ir Duomenų apsaugos įstatyme įtvirtintais principais ir taisyklėmis. Be to, turėtų būti vadovaujamasi 29 str. darbo grupės *Nuomone 2/2017 dėl duomenų tvarkymo darbe*, kurioje plačiai pateikiamas įvairių situacijų vertinimas. Taip pat, siekiant dar labiau užtikrinti darbuotojų asmens duomenų apsaugą su darbo santykiais susijusiame kontekste, konkretesnės duomenų apsaugos taisyklės galėtų būti nustatomos kolektyvinėse sutartyse.

[186] ES 29 str. duomenų apsaugos darbo grupė. *2017 m. birželio 8 d. Nuomonė 2/2017 dėl duomenų tvarkymo darbe*. Nr. 17/LT WP 249, p. 3.
[187] Ibid., p. 13-15.
[188] Europos Žmogaus Teisių Teismas. 2017 m. rugsėjo 5 d. sprendimas byloje *Barbulescu prieš Rumuniją*, Nr. 61496/08. ECHR:2017:0905JUD006149608.

3.4. Reglamentas ir 29 straipsnio darbo grupės šaltiniai

Reglamente yra įtvirtinta daug abstrakčių ir individualaus vertinimo reikalaujančių normų. Konkretumo trūksta ypač tose srityse, kuriose Reglamentas numato asmens duomenų apsaugos naujoves. Nors naujoji duomenų apsaugos sistema grindžiama galiojančiais teisės aktais, jos poveikis bus labai platus ir tam tikrus aspektus reikės iš esmės pakoreguoti. Dėl šios priežasties ir buvo numatytas 2 metų pereinamasis laikotarpis, trunkantis iki 2018 m. gegužės 25 d., kai bus pradėtas taikyti Reglamentas, kad per šį laikotarpį valstybės narės ir suinteresuotieji subjektai galėtų tinkamai pasiruošti naujajam teisiniam reguliavimui.[189]

Rengiantis tinkamai taikyti Reglamentą yra ypač svarbi 29 str. darbo grupės veikla, kurią aktyviai remia Europos Komisija. Ši darbo grupė, sudaryta pagal Duomenų apsaugos direktyvos 29 str.,[190] susidedanti iš kiekvienos valstybės narės priežiūros institucijos atstovų, Europos duomenų apsaugos priežiūros pareigūno ir Komisijos atstovo, turi vieną svarbiausių užduočių ruošiantis efektyviam Reglamento taikymui – parengti gaires, skirtas visiems suinteresuotiems subjektams, kurios detaliai išaiškintų konkrečius Reglamento turinio aspektus, pateikdamos aktualiausių situacijų pavyzdžius ir patarimus tikslingam naujų taisyklių įgyvendinimui.

29 str. darbo grupė yra nepriklausomas Europos Sąjungos patariamasis organas duomenų apsaugos ir privatumo klausimais. Šios darbo grupės funkcijos iš pradžių buvo susijusios su Duomenų apsaugos direktyvos klausimais, tačiau darbo grupė taip pat gali savo iniciatyva siūlyti rekomendacijas visais klausimais, susijusiais su asmens apsauga tvarkant asmens duomenis Europos Sąjungoje, todėl jos veikla tapo ypač svarbi ir rengiantis taikyti Reglamentą.

29 str. darbo grupė rengia nuomones, rekomendacijas ir kitą medžiagą, susijusią su asmens duomenų apsauga. Konkrečiai Reglamento taikymui yra ruošiamos gairės įvairiais jo turinio aiškinimo klausimais. Nors gairės neturi privalomosios galios ir nėra formaliai įpareigojantis šaltinis, tačiau neatitikimas jo turiniui dažniausiai lemia Europos Sąjungos duomenų apsaugos teisės pažeidimus.[191] Todėl visos 29 str. darbo grupės gairės, susijusios su Reglamentu, turėtų būti laikomos autoritetingais teisės šaltiniais.

---

[189] Europos Komisija. Didesnė apsauga, naujos galimybės. Komisijos gairės dėl tiesioginio Bendrojo duomenų apsaugos reglamento taikymo nuo 2018 m. gegužės 25 d. *Komisijos komunikatas Europos Parlamentui ir Tarybai COM(2018) 43 galutinis*, 2018, Briuselis, p. 1.

[190] 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo. *OL* 2004 m. specialusis leidimas, 13 skyrius, 15 tomas, p. 355–374.

[191] European Union Agency for Network and Information Security. *Article 29 Working Party*. 2018. [interaktyvus; žiūrėta 2018 m. sausio 16 d.]. Prieiga per internetą:

Šiuo metu jau yra parengtos gairės dėl poveikio duomenų apsaugai vertinimo; pranešimo apie asmens duomenų apsaugos pažeidimą; duomenų apsaugos pareigūnų; teisės į duomenų perkeliamumą; vadovaujančios priežiūros institucijos; administracinių baudų taikymo ir nustatymo; skaidrumo; sutikimo; automatizuoto atskirų sprendimų priėmimo, įskaitant profiliavimą. Vis dar rengiamos gairės dėl sertifikavimo ir akreditavimo, duomenų valdytojams privalomų taisyklių bei duomenų tvarkytojams privalomų taisyklių. Taip pat svarbi yra 2017 m. nuomonė dėl duomenų tvarkymo darbe, parengta atsižvelgiant tiek į Duomenų apsaugos direktyvos, tiek ir į Reglamento kontekstą. Aktualumo vis dar nepraranda ir 2007 metų nuomonė dėl asmens duomenų sampratos.

29 str. darbo grupės rengiama medžiaga yra naudinga visiems suinteresuotiems subjektams. Visų pirma, gairėmis praktikoje remsis nacionalinės priežiūros institucijos, atsakingos už Reglamento taikymo stebėseną, kad būtų apsaugotos fizinių asmenų pagrindinės teisės ir laisvės tvarkant duomenis. Be to, jos konsultuos suinteresuotus asmenis, todėl būtina, jog priežiūros institucijos tinkamai suprastų visus Reglamento ypatumus, užtikrintų nuoseklų aiškinimą ir palaikytų teisinį tikrumą.

Taip pat gairės labai aktualios duomenų valdytojams, kuriems dėl abstrakčių Reglamento nuostatų kyla daugiausiai neaiškumų. Duomenų valdytojams, priklausomai nuo Reglamento normų vertinimo, gali kilti konkrečių pareigų, pavyzdžiui, pareiga paskirti duomenų apsaugos pareigūną, atlikti poveikio duomenų apsaugai vertinimą ar pranešti apie asmens duomenų saugumo pažeidimą. Jeigu tam tikros normos nebus tinkamai suprantamos ir įtvirtintos pareigos neįgyvendintos, tai gali lemti didelių administracinių baudų skyrimą.

Taigi, 29 str. darbo grupės rengiamos gairės ir kita aiškinamoji medžiaga padeda užtikrinti, jog Reglamento taikymui būtų tinkamai pasiruošta ir jame nustatytos naujovės būtų efektyviai įgyvendinamos, užtikrinant teisinį tikrumą visose ES valstybėse narėse. Dėl abstrakčių Reglamento nuostatų gausos neužtenka analizuoti vien tik paties Reglamento turinio, kartu turėtų būti vadovaujamasi ir gairėmis, kuriose pateikti išaiškinimai turi tiesioginę praktinę reikšmę nacionalinėms priežiūros institucijoms, įvairioms organizacijoms bei duomenų subjektams, siekiantiems pasinaudoti Reglamento suteikiamais privalumais. 29 str. darbo grupės darbą nuo 2018 m. gegužės 25 d. perims Reglamentu įsteigiama Europos duomenų apsaugos valdyba.

<https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/laws-regulation/data-protection-privacy/article-29-working-party>.

IŠVADOS

1. Tarptautiniu lygmeniu teisė į duomenų apsaugą vis dar yra laikoma sudėtine teisės į privatų gyvenimą, įtvirtintos Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencijos 8 str., dalimi. Tuo tarpu Europos Sąjungoje teisė į duomenų apsaugą yra viena iš pagrindinių žmogaus teisių, įtvirtinta Pagrindinių teisių chartijos 8 str. ir Sutarties dėl Europos Sąjungos veikimo 16 str. bei kurios apsauga yra pagrindinis Bendrojo duomenų apsaugos reglamento tikslas.
2. Po Duomenų apsaugos direktyvos priėmimo tokie veiksniai kaip spartus technologijų vystymasis ir suaktyvėjusi globalizacija lėmė didėjantį pavojų asmens duomenų saugumui. Todėl atsirado poreikis duomenų apsaugos teisės reformai ES, kurios pagrindu yra Bendrasis duomenų apsaugos reglamentas, dar labiau įtvirtinantis teisės į duomenų apsaugą savarankiškumą ir atskirtį nuo teisės į privatumą.
3. Bendrasis duomenų apsaugos reglamentas skatina didelę ES duomenų apsaugos teisės pažangą. Pirma, atnaujinamos duomenų apsaugos taisyklės. Antra, užtikrinamas vienodų duomenų apsaugos taisyklių taikymas visose ES valstybėse narėse. Trečia, Bendrasis duomenų apsaugos reglamentas paveiks net ir už ES ribų veikiančias organizacijas, kurios, norėdamos tvarkyti ES esančių duomenų subjektų asmens duomenis, privalės laikytis ES duomenų apsaugos teisės standartų.
4. Bendruoju duomenų apsaugos reglamentu yra sustiprinamos duomenų subjektų teisės. Teisė būti pamirštam ir teisė apriboti duomenų tvarkymą yra išplečiamos ir detaliau reglamentuojamos, o teisė į duomenų perkeliamumą yra visiškai nauja teisė, užkertanti kelią duomenų susaistymo efektui ir leidžianti laisviau pereiti prie kito duomenų valdytojo bei skatinanti organizacijų konkurenciją. Atnaujintų ir sustiprintų teisių visuma sudaro galimybes asmenims dar geriau kontroliuoti savo asmens duomenis.
5. Bendrasis duomenų apsaugos reglamentas didina duomenų valdytojų atsakomybę ir savarankiškumą. Jiems skiriamos naujos pareigos, tokios kaip pranešimas apie asmens duomenų saugumo pažeidimą, poveikio duomenų apsaugai vertinimas, išankstinės konsultacijos su priežiūros institucija, duomenų apsaugos pareigūno skyrimas, gali padidinti duomenų subjektų pasitikėjimą duomenų valdytojais, su sąlyga, jog šios pareigos bus vykdomos tinkamai.
6. Galima numatyti, jog duomenų apsaugos pareigūnas bus ypač svarbi naujojo duomenų apsaugos teisinio reguliavimo dalis. Jis atliks Bendrojo duomenų apsaugos reglamento eksperto funkcijas, padėdamas užtikrinti, jog duomenų valdytojai tinkamai įgyvendintų

jiems numatomus reikalavimus ir laikytųsi naujojo atskaitomybės principo. Taip pat duomenų apsaugos pareigūnas bus svarbus duomenų subjektams, kurie galės į jį kreiptis visais su jų asmens duomenų tvarkymu susijusiais klausimais.

7. Bendrasis duomenų apsaugos reglamentas turėtų būti taikomas kaip duomenų apsaugos teisės šaltinių sistemos dalis. Tokiose srityse kaip duomenų tvarkymas darbo santykių kontekste ar nacionalinio asmens identifikavimo numerio tvarkymas, valstybėms narėms suteikiamas lankstumas konkrečiau apibrėžti Bendrajame duomenų apsaugos reglamente nustatytas taisykles. Todėl nacionaliniai duomenų apsaugos įstatymai ir kiti teisės aktai, susiję su duomenų apsauga, išliks svarbi duomenų apsaugos teisės šaltinių sistemos dalis ir bus taikomi kartu su Bendruoju duomenų apsaugos reglamentu.
8. Dėl abstrakčių Bendrojo duomenų apsaugos reglamento normų, reikalaujančių kompetentingo vertinimo, gausos, neužtenka vadovautis vien tik jų turiniu. Siekiant tinkamai įgyvendinti naujojo duomenų apsaugos teisinio reguliavimo nuostatas, turėtų būti vadovaujamasi ES 29 straipsnio duomenų apsaugos darbo grupės gairėmis, turinčiomis tiesioginę praktinę reikšmę Bendrojo duomenų apsaugos reglamento taikymui.

LITERATŪROS IR KITŲ ŠALTINIŲ SĄRAŠAS

Norminiai teisės aktai

1. Lietuvos Respublikos Konstitucija. *Valstybės žinios*, 1992, nr. 33-1014.
2. 1950 m. lapkričio 4 d. Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencija. *Valstybės žinios*, 1995-05-16, nr. 40-987.
3. 1981 m. sausio 28 d. Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (Konvencija Nr. 108). *Valstybės žinios*, 2001-04-13, nr. 32-1059.
4. Sutartis dėl Europos Sąjungos veikimo (suvestinė redakcija). *OL* C 202, 2016 6 7, p. 1-388.
5. Lisabonos sutartis, iš dalies keičianti Europos Sąjungos sutartį ir Europos bendrijos steigimo sutartį. *OL* C 306, 2007 12 13, p. 1-273.
6. Europos Sąjungos pagrindinių teisių chartija. *OL* C 326, 2012 10 26, p. 391-407.
7. 2000 m. gruodžio 18 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 45/2001 dėl asmenų apsaugos Bendrijos institucijoms ir įstaigoms tvarkant asmens duomenis ir laisvo tokių duomenų judėjimo (ES institucijų duomenų apsaugos reglamentas). *OL* L 8, 2001 1 12, p. 1-22.
8. 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). *OL* L 119, 2016 5 4, p. 1–88.
9. 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo. *OL 2004 m. specialusis leidimas*, 13 skyrius, 15 tomas, p. 355–374.
10. 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių). *OL* L 201, 2002 7 31, p. 37–47.
11. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/680 dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo tikslais ir dėl laisvo tokių duomenų

judėjimo, ir kuriuo panaikinamas Tarybos pamatinis sprendimas 2008/977/TVR. *OL* L 119, 2016 5 4, p. 89-131.

12. 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, p. 1–30.
13. 2008 m. lapkričio 27 d. Tarybos pamatinis sprendimas 2008/977/TVR dėl asmens duomenų, tvarkomų vykdant policijos ir teisminį bendradarbiavimą baudžiamosiose bylose, apsaugos (Duomenų apsaugos pamatinis sprendimas). *OL* L 350, 2008 12 30, p. 60-71.
14. Lietuvos Respublikos civilinis kodeksas (su pakeitimais ir papildymais). *Valstybės žinios*, 2000-09-06, nr. 74-2262.
15. Lietuvos Respublikos darbo kodeksas (su pakeitimais ir papildymais). *TAR*, 2016-09-19, nr. 23709.
16. Lietuvos Respublikos darbo kodekso 27 straipsnio pakeitimo įstatymo projektas. 2018-02-15, nr. 18-1820.
17. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas (su pakeitimais ir papildymais). *Valstybės žinios*, 1996-07-03, nr. 63-1479.
18. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo Nr. I-1374 pakeitimo įstatymo projektas. 2018-02-15, nr. 17-7645(2).
19. Lietuvos Respublikos asmens duomenų, tvarkomų vykdant policijos ir teisminį bendradarbiavimą baudžiamosiose bylose, teisinės apsaugos įstatymas (su pakeitimais ir papildymais). *Valstybės žinios*, 2011-05-03, nr. 52-2511.
20. Lietuvos Respublikos elektroninių ryšių įstatymas (su pakeitimais ir papildymais). *Valstybės žinios*, 2004-04-30, nr. 69-2382.
21. Duomenų valdytojų pranešimo apie duomenų tvarkymą taisyklės, patvirtintos Lietuvos Respublikos Vyriausybės 2002 m. vasario 20 d. nutarimu Nr. 262 (su pakeitimais ir papildymais). *Valstybės žinios*, 2002, nr. 20-768; *TAR*, 2015-09-11, nr. 13748.

Specialioji literatūra

22. CASTELLANO, Pere Simon. The right to be forgotten under European Law: a Constitutional debate. *Lex Electronica*, 2012, vol. 16.1, p. 1-30.
23. CIVILKA, Mindaugas; ŠLAPIMAITĖ, Lina. Asmens duomenų samprata elektroninėje erdvėje. *Teisė*, 2015, t. 96, p. 126-148.

24. DEŠRIŪTĖ, Justina. Esminiai asmens duomenų apsaugos baudžiamajame procese reformos Europos Sąjungoje aspektai ir jų įtaka nacionaliniam teisiniam reguliavimui. *Teisės problemos*, 2016, nr. 1 (91), p. 25-51.
25. DE HART, Paul *et al*. The right to data portability in the GDPR: Towards user-centric interoperability of digital services. *Computer Law and Security Review*, 2017, p. 1-11.
26. DE TERWANGNE, Cecile. *Internet Privacy and the Right to Be Forgotten/Right to Oblivion*. 2012, No. 13, p. 109-121.
27. DOWNING, Robbie. Overview of EU General Data Protection Regulation. *Thomson Reuters*, 2017, p. 1-39.
28. ENGELS, Barbara. Data portability among online platforms. *Internet Policy Review: Journal on Internet Regulation*, 2016, t. 5(2), p. 1-17.
29. YOO, Christopher. When Antitrust Met Facebook. *Penn Law: Legal Scholarship Repository – Faculty Scholarship*, 2012, t. 422, p. 1146-1162.
30. KINGSTON, John. Using artificial intelligence to support compliance with the general data protection regulation. *Artificial Intelligence and Law*, 2017, Vol. 25, No. 4, p. 429–443.
31. KIŠKIS, Mindaugas. *Data Protection in Lithuania // Data Protection Laws of the World*. London: Sweet & Maxwell, 2007, 12th ed.
32. LACHAUD, Eric. Should the DPO be certified? *International Data Privacy Law*, 2014, Vol. 4, No. 3, p. 189-202.
33. MACENAITE, Milda. From universal towards child-specific protection of the right to privacy online: Dilemmas in the EU General Data Protection Regulation. *New Media and Society*, 2017, Vol. 19(5), p. 765-779.
34. NEVILLE, Andrew. Is it a Human Right to be Forgotten? Conceptualizing the World View. *Santa Clara Journal of International Law*, 2017, Vol. 15, No. 2, p. 156-172.
35. PETRAITYTĖ, Ilona. Asmens duomenų apsauga ir teisė į privatų gyvenimą. *Teisė*, 2011, t. 80, p. 163-174.
36. PETRAITYTĖ, Ilona. Asmens duomenų apsaugos teisinis reguliavimas Lietuvos teisės sistemoje. *Teisė*, 2011, t. 79, p. 125-138.
37. PETRAITYTĖ, Ilona. *Asmens duomenų teisinės apsaugos principai*: daktaro disertacija. Socialiniai mokslai, teisė (01S). Vilnius: Vilniaus universitetas, 2013.

38. TIKKINEN-PIRI, Christina; ROHUNEN, Anna; MARKKULA, Jouni. EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law and Security Review*, 2018, t. 34, p. 134-153.
39. VAN DER AUWERMEULEN, Barbara. How to attribute the right to data portability in Europe: A comparative analysis of legislations. *Computer Law and Security Review*, 2017, t. 33, p. 57–72.
40. VAN HOBOKEN, Joris. *The Proposed Right to be Forgotten Seen from the Perspective of Our Right to Remember, Freedom of Expression Safeguards in a Converging Information Environment (Prepared for the European Commission)*. Amsterdam, 2013, p. 1-30.
41. WEISS, Stefan. Privacy Threat Model for Data Portability in Social Network Applications. *Americas Conference on Information Systems (AMCIS) 2008 Proceedings*, 2008, t. 84, p. 1-8.
42. ZALESKIS, Julius. Duomenų apsaugos pareigūno veiklos pagrindai pagal ES bendrąjį duomenų apsaugos reglamentą. *Teisė*, 2017, t. 104, p. 159–170.
43. ZALESKIS, Julius. ES Bendrasis duomenų apsaugos reglamentas: reikšmė duomenų apsaugos teisei. *Teisė*, 2017, t. 103, p. 45–54.
44. ZANFIR, Gabriela. The right to Data portability in the context of the EU data protection reform. *International Data Privacy Law*, 2012, Vol. 2, No. 3, p. 149–162.

Teismų praktika

45. Lietuvos Respublikos Konstitucinis Teismas. 2000 m. gegužės 8 d. nutarimas byloje Nr. 12/99-27/99-29/99-1/2000-2/2000.
46. Europos Žmogaus Teisių Teismas. 1997 m. vasario 25 d. sprendimas byloje *Z. prieš Suomiją*, Nr. 22009/93, ECHR:1997:0225JUD002200993.
47. Europos Žmogaus Teisių Teismas. 2008 m. gruodžio 4 d. sprendimas byloje *S. ir Marper prieš Jungtinę Karalystę*, Nr. 30562/04 ir 30566/04, ECHR:2008:1204JUD003056204.
48. Europos Žmogaus Teisių Teismas. 2017 m. rugsėjo 5 d. sprendimas byloje *Barbulescu prieš Rumuniją*, Nr. 61496/08, ECHR:2017:0905JUD006149608.
49. Europos Sąjungos Teisingumo Teismas. 2010 m. lapkričio 9 d. sprendimas sujungtose bylose *Volker und Markus Schecke GbR (C-92/09) ir Hartmut Eifert (C-93/09) prieš Land Hessen*, EU:C:2010:662.

50. Europos Sąjungos Teisingumo Teismas. 2011 m. spalio 25 d. sprendimas sujungtose bylose *eDate Advertising GmbH prieš X ir Olivier Martinez, Robert Martinez prieš MGN Limited* C-509/09 ir C-161/10, EU:C:2011:685.
51. Europos Sąjungos Teisingumo Teismas. 2011 m. lapkričio 24 d. sprendimas sujungtose bylose *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) ir Federación de Comercio Electrónico y Marketing Directo (FECEMD) prieš Administración del Estado* C-468/10 ir C-469/10, EU:C:2011:777.
52. Europos Sąjungos Teisingumo Teismas. 2014 m. gegužės 13 d. sprendimas byloje *Google Spain SL ir Google Inc. prieš Agencia Española de Protección de Datos (AEPD) ir Mario Costeja González* C-131/12, EU:C:2014:317.
53. Lietuvos vyriausiasis administracinis teismas. 2012 m. liepos 26 d. nutartis administracinėje byloje *UADBB „Edrauda“ v. Valstybinė duomenų apsaugos inspekcija*, Nr. A-858-2133-12.
54. Vilniaus miesto apylinkės teismas. 2014 m. vasario 26 d. nutarimas administracinio teisės pažeidimo byloje Nr. A2.11.-1793-295/2014.

***Soft law* šaltiniai**

55. Article 29 Data Protection Working Party. *2017 October 3 Guidelines on Personal data breach notification under Regulation 2016/679*. 17/EN WP 250, p. 1-30.
56. Article 29 Data Protection Working Party. *Opinion 4/2007 on the concept of personal data*. 01248/07/EN WP 136, p. 1-26.
57. ES 29 str. duomenų apsaugos darbo grupė. *2016 m. gruodžio 13 d. Duomenų apsaugos pareigūnų gairės* (su paskutiniais pakeitimais 2017 m. balandžio 5 d.). Nr. 16/LT WP 243, 1-oji peržiūrėta versija, p. 1-29.
58. ES 29 str. duomenų apsaugos darbo grupė. *2016 m. gruodžio 13 d. Teisės į duomenų perkeliamumą gairės* (su paskutiniais pakeitimais 2017 m. balandžio 5 d.). Nr. 16/LT WP 242, 1-oji peržiūrėta versija, p. 1-22.
59. ES 29 str. duomenų apsaugos darbo grupė. *2017 m. balandžio 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. 17/LT WP 248, 1-oji peržiūrėta versija, p. 1-25.
60. ES 29 str. duomenų apsaugos darbo grupė. *2017 m. birželio 8 d. Nuomonė 2/2017 dėl duomenų tvarkymo darbe*. Nr. 17/LT WP 249, p. 1-26.

61. Europos Komisija. Didesnė apsauga, naujos galimybės. Komisijos gairės dėl tiesioginio Bendrojo duomenų apsaugos reglamento taikymo nuo 2018 m. gegužės 25 d. *Komisijos komunikatas Europos Parlamentui ir Tarybai COM(2018) 43 galutinis*, 2018, Briuselis, p. 1-17.
62. Europos Komisija. Europos Parlamento ir Tarybos reglamentas dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo (Bendrasis duomenų apsaugos reglamentas). *Pasiūlymas COM(2012) 11 galutinis*, 2012, Briuselis, p. 1-122.
63. Europos Komisija. Privatumo apsauga glaudžiai susijusiame pasaulyje: Europos duomenų apsaugos reglamentavimo pagrindai XXI amžiuje. *Komisijos komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui COM(2012) 9 galutinis*, 2012, Briuselis, p. 1-12.
64. Europos Komisija. Visapusiškas požiūris į asmens duomenų apsaugą Europos Sąjungoje. *Komisijos komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialiniu reikalų komitetui ir Regionų komitetui COM(2010) 609 galutinis*, 2010, Briuselis, p. 1-19.
65. Europos Parlamentas. *Asmens duomenų apsauga*. [interaktyvus; žiūrėta 2018 m. vasario 6 d.]. Prieiga per internetą: <http://www.europarl.europa.eu/atyourservice/lt/displayFtu.html?ftuId=FTU_4.2.8.html>.
66. Europos Sąjungos pagrindinių teisių agentūra (FRA); Europos Taryba; Europos Žmogaus Teisių Teismas. *Europos duomenų apsaugos teisės vadovas*. Liuksemburgas: Europos Sąjungos leidinių biuras, 2014.
67. Europos Sąjungos Taryba. Pirmininkaujančios valstybės narės pranešimas Nuolatinių atstovų komitetui / Tarybai. *Teisė būti pamirštam ir Teisingumo Teismo sprendimas dėl „Google“ – Politiniai debatai*. Briuselis, 2014, Nr. 13619/14.
68. European Anti-Fraud Office. *OLAF Data Protection Officer: Summaries of EU Court Decisions Relating to Data Protection 2000-2015*. Belgium, 2016, p. 44. 1-61.
69. European Data Protection Supervisor. *Data Protection*. [interaktyvus; žiūrėta 2018 m. vasario 6 d.]. Prieiga per internetą: <https://edps.europa.eu/data-protection/data-protection_en>.

70. European Union Agency for Network and Information Security. *Article 29 Working Party*. 2018. [interaktyvus; žiūrėta 2018 m. sausio 16 d.]. Prieiga per internetą: <https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/laws-regulation/data-protection-privacy/article-29-working-party>.
71. Valstybinė duomenų apsaugos inspekcija. *Asmens duomenų teisinės apsaugos įstatymo komentaras*. Vilnius, 2005, p. 1-278.
72. Valstybinė duomenų apsaugos inspekcija. *Jūsų teisės asmens duomenų apsaugos srityje*. (Viešoji konsultacija), 2017 m. liepos 11 d. [interaktyvus; žiūrėta 2018 m. sausio 14 d.]. Prieiga per internetą: <https://www.ada.lt/go.php/JUSU-TEISES770>.
73. Visuotinė žmogaus teisų deklaracija. Jungtinės Tautos (JT), 1948. *Valstybės žinios*, 2006, nr. 68-2497.

Kiti šaltiniai

74. Baker & McKenzie. *EU Data Protection Officer - Must Have, Nice to Have or Safe to Ignore?* 2016.
75. Baker & McKenzie. *EU General Data Protection Regulation in 13 Game Changers*. 2016.
76. CIVILKA, Mindaugas. *Teisė būti pamirštam: mitologija ir tikrovė*. 2016. [interaktyvus; žiūrėta 2018 m. vasario 4 d.]. Prieiga per internetą: <https://www.linkedin.com/pulse/teis%C4%97-b%C5%ABti-pamir%C5%A1tam-mitologija-ir-tikrov%C4%97-mindaugas-civilka>.
77. Europos Komisija. *29 straipsnio darbo grupė* (interneto puslapio skiltis) [interaktyvus; žiūrėta 2018 m. vasario 17 d.]. Prieiga per internetą: <http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083>.
78. Europos Komisija. *Kada turėčiau pasinaudoti savo teise apriboti savo asmens duomenų tvarkymą?* [interaktyvus; žiūrėta 2018 m. kovo 2 d.]. Prieiga per internetą: <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/my-rights/when-should-i-exercise-my-right-restriction-processing-my-personal-data_lt>.

79. Google. *Paieškoje indeksuoto turinio pašalinimo užklausa, pateikta atsižvelgiant į Europos duomenų apsaugos įstatymus*. [interaktyvus; žiūrėta 2018 m. vasario 5 d.]. Prieiga per internetą: <https://www.google.com/webmasters/tools/legal-removal-request?complaint_type=rtbf&visit_id=1-636557183438938250-1427818002&hl=lt&rd=1>.
80. Google. *Skaidrumo ataskaita: Paieškos rezultatų pašalinimas dėl Europos privatumo įstatymo pažeidimų*. [interaktyvus; žiūrėta 2018 m. vasario 18 d.]. Prieiga per internetą: <https://transparencyreport.google.com/eu-privacy/overview>.
81. Lietuvos Respublikos Teisingumo ministerija. *Teisės aktai, reguliuojantys asmens duomenų apsaugą*. [interaktyvus; žiūrėta 2018 m. vasario 5 d.]. Prieiga per internetą: <http://www.tm.lt/teisineinfo/teisesaktas/52>.
82. London Economics. *Study on the economic benefits of privacy-enhancing technologies (PETs): Final Report to The European Commission, DG Justice, Freedom and Security*. 2010, London. Prieiga per internetą: <https://londoneconomics.co.uk/wp-content/uploads/2011/09/17-Study-on-the-economic-benefits-of-privacy-enhancing-technologies-PETs.pdf>.
83. Ryšių reguliavimo tarnyba. *RRT teikia rekomendacijas dėl debesų kompiuterijos paslaugų saugumo*. [interaktyvus; žiūrėta 2018 m. sausio 7.]. Prieiga per internetą: <http://www.rrt.lt/lt/vartotojui/tinklu-informacijos-saugumas-vartotojui/debesu-kompiuterija.html>.
84. The Economist. *What is the Streisand effect?* 2013. [interaktyvus; žiūrėta 2018 m. vasario 18 d.]. Prieiga per internetą: <https://www.economist.com/blogs/economist-explains/2013/04/economist-explains-what-streisand-effect>.

SANTRAUKA

Didėjantis pavojus asmens duomenų saugumui, sukeltas spartaus technologijų vystymosi ir suaktyvėjusios globalizacijos, lėmė poreikį ES duomenų apsaugos teisės reformai – 2018 m. gegužės 25 d. bus pradėtas taikyti Bendrasis duomenų apsaugos reglamentas, pakeisiantis dabar galiojančią Duomenų apsaugos direktyvą ir tapsiantis pagrindiniu duomenų apsaugos teisės šaltiniu visose ES valstybėse narėse. Todėl šio darbo tikslas yra atskleisti Bendrojo duomenų apsaugos reglamento reikšmę ir įtaką duomenų apsaugos teisei bei nustatyti jo vietą duomenų apsaugos teisės šaltinių sistemoje.

Magistro darbe apžvelgiama dabartinė duomenų apsaugos teisės sistema, atskleidžiamos ES duomenų apsaugos teisės reformos priežastys ir tikslai, nagrinėjamos Bendruoju duomenų apsaugos reglamentu nustatomos naujovės, analizuojama jų svarba ir taikymo ypatumai, taip pat atskleidžiamas Bendrojo duomenų apsaugos reglamento santykis su kitais duomenų apsaugos teisės šaltiniais. Atlikus išsamią analizę nustatoma, jog Bendrasis duomenų apsaugos reglamentas dar labiau įtvirtina teisės į duomenų apsaugą savarankiškumą ir atskirtį nuo teisės į privatumą bei skatina didelę ES duomenų apsaugos teisės pažangą, nustatant atnaujintų ir suvienodintų duomenų apsaugos taisyklių taikymą visose ES valstybėse narėse.

Svarbiausi Bendrojo duomenų apsaugos reglamento privalumai apima duomenų subjektų teisių sustiprinimą, duomenų valdytojų atsakomybės ir savarankiškumo padidinimą, privalomo duomenų apsaugos pareigūno instituto įtvirtinimą. Sustiprintų duomenų subjektų teisių visuma sudaro galimybes asmenims dar geriau kontroliuoti savo asmens duomenis. Duomenų valdytojams skiriamos naujos pareigos gali padidinti duomenų subjektų pasitikėjimą, su sąlyga, jog šios pareigos bus vykdomos tinkamai. Duomenų apsaugos pareigūnas atliks Bendrojo duomenų apsaugos reglamento eksperto funkcijas ir bus ypač svarbi naujojo duomenų apsaugos teisinio reguliavimo dalis.

Išanalizavus Bendrąjį duomenų apsaugos reglamentą buvo nustatyta, jog jis turėtų būti taikomas kaip duomenų apsaugos teisės šaltinių sistemos dalis. Srityse, kuriose suteikiamas lankstumas konkrečiau apibrėžti Bendrajame duomenų apsaugos reglamente nustatytas taisykles, išliks svarbūs nacionaliniai duomenų apsaugos teisės aktai. Be to, abstrakčios Bendrojo duomenų apsaugos reglamento normos lemia poreikį vadovautis ES 29 straipsnio duomenų apsaugos darbo grupės gairėmis, turinčiomis tiesioginę praktinę reikšmę tinkamam naujojo duomenų apsaugos teisinio reguliavimo nuostatų įgyvendinimui.

SUMMARY

The European Union General Data Protection Regulation as a Legal Source of Data Protection Law

Growing threat to personal data security, caused by rapid technological development and intensified globalization, has led to the need for an EU data protection law reform – on 25th May 2018 the General Data Protection Regulation will replace the current Data Protection Directive and will become the main source of data protection law in all EU Member States. Therefore, the aim of the Master's thesis is to reveal the significance and impact of the General Data Protection Regulation on data protection law and to determine its place in the system of sources of data protection law.

The Master's thesis reviews the current legal framework for data protection, reveals the causes and objectives of the EU data protection law reform, examines innovations set out in the General Data Protection Regulation, analyzes their importance and peculiarities of application, and reveals the relation between the General Data Protection Regulation and other sources of data protection law. A comprehensive analysis shows that the General Data Protection Regulation further consolidates the right to data protection and the distinction from the right to privacy, and encourages significant progress of the EU data protection law, by setting updated and uniform data protection rules for all EU Member States.

The main benefits of the General Data Protection Regulation include strengthening the rights of data subjects, increasing the responsibility and independence of data controllers, and establishing a mandatory data protection officer. Enhanced data subjects' rights allow individuals to have better control over their personal data. New responsibilities for data controllers, if carried out properly, can increase the confidence of data subjects. The data protection officer will perform the functions of an expert of the General Data Protection Regulation and will be particularly relevant to the new legal framework of data protection.

Analysis of the General Data Protection Regulation determines that it should be applied as part of the system of data protection law sources. In the areas where flexibilities to set out more specific rules of the General Data Protection Regulation are provided, national data protection laws will continue to be important. Moreover, abstract provisions of the General Data Protection Regulation lead to the need to follow the guidelines of the EU Article 29 Data Protection Working Party, that have a direct practical significance for the proper implementation of the new data protection legal framework.