

DUOMENŲ APSAUGOS PAREIGŪNO VEIKLOS PAGRINDAI PAGAL ES BENDRAJĄ DUOMENŲ APSAUGOS REGLAMENTĄ

Julius Zaleskis

Vilniaus universiteto Teisės fakulteto
Viešosios teisės katedros lektorius
socialinių mokslų daktaras
Saulėtekio al. 9, I rūmai, LT-10222 Vilnius, Lietuva
Tel. (+370 5) 236 61 75
El. paštas: <julius.zaleskis@gmail.com>

Naujasis ES Bendrasis duomenų apsaugos reglamentas įtvirtina duomenų apsaugos pareigūno institutą, kuris turėtų būti duomenų apsaugos reguliavimo centre, tačiau palieka neaiškumų dėl jo turinio. Darbe atskleidžiamos naujojo duomenų apsaugos pareigūno veiklos reguliavimo naujovės, pagrindų paskirti duomenų apsaugos pareigūną turinys, apibrėžiami principai, kuriais grindžiama duomenų apsaugos pareigūnų veikla.

The new EU General Data Protection Regulation sets forth a body of rules on data protection officer, which should be at the centre of the new legal framework, however, provides for uncertainty regarding content thereof. The article reveals new developments of the regulation on data protection officers, the content of grounds for appointment of the data protection officer, defines principles upon which activities of the data protection officer should be based.

Įvadas

Europos Sąjungos (toliau – ES) Reglamentas dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (angl. *General Data Protection Regulation – GDPR*)¹ reformuoja ES duomenų apsaugos teisės reguliavimą nuo 2018 m. gegužės 25 d.² Mažindamas priežiūros institucijų kišimąsi į kasdienę duomenų tvarkymo veiklą naujasis reguliavimas perkelia daugiau atsakomybės už duomenų apsaugą asmens duomenis renkančioms ir naudojančioms organizacijoms. Autoritetinga ES asmens duomenų apsaugos 29 straipsnio darbo grupė (toliau – ES 29 str. darbo grupė) žada, kad daugeliui organizacijų duomenų apsaugos pareigūnai bus naujojo teisinio reguliavimo centre. Duomenų apsaugos pareigūnas – tai darbuotojas ar išorės ekspertas (paslaugos teikėjas), kuris prižiūri duomenų valdytojo³ ar duomenų tvarkytojo⁴ atitiktį Bendrajam duomenų apsaugos reglamentui ir padeda ją užtikrinti

¹ 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.

² ZALESKIS, Julius. ES Bendrasis duomenų apsaugos reglamentas: reikšmė duomenų apsaugos teisei. *Teisė*, 2017, t. 103, p. 45–54 [interaktyvus. Žiūrėta 2017 m. liepos 26 d.]. Prieiga per internetą: <<http://www.zurnalai.vu.lt/teisė/article/view/10779>>

³ Duomenų valdytojas – fizinis arba juridinis asmuo, valdžios institucija, agentūra ar kita įstaiga, kuris vienas ar drauge su kitais nustato duomenų tvarkymo tikslus ir priemones (Bendrojo duomenų apsaugos reglamento 4 str. 7 p.).

⁴ Duomenų tvarkytojas – fizinis arba juridinis asmuo, valdžios institucija, agentūra ar kita įstaiga, kuri duomenų valdytojo vardu tvarko asmens duomenis (Bendrojo duomenų apsaugos reglamento 4 str. 8 p.).

(Bendrojo duomenų apsaugos reglamento 37 str. 6 d., 38 str. 1 d., 39 str. 1 d.). Duomenų apsaugos pareigūno paskyrimas duomenų valdytojams ir duomenų tvarkytojams turi didelę praktinę reikšmę: padeda užtikrinti atitiktį naujesiems reikalavimams, nulemia poreikį peržiūrėti organizacinę struktūrą, žmogiškuosius ir finansinius išteklius.

Šio straipsnio *tikslas* – apibrėžti duomenų apsaugos pareigūnų veiklos pagrindus pagal Bendrąjį duomenų apsaugos reglamentą. Keliami tokie *uždaviniai*: (1) palyginti šiuo metu galiojančią duomenų apsaugos teisės reguliavimą su Bendroju duomenų apsaugos reglamentu duomenų apsaugos pareigūnų veiklos reguliavimo aspektu, (2) atskleisti pagrindų paskirti duomenų apsaugos pareigūną turinį, (3) apibrėžti duomenų apsaugos pareigūno veiklos principus.

Tyrimo *objektas* – Bendrajame duomenų apsaugos reglamente numatytas ir dabartinis teisinis duomenų apsaugos pareigūnų veiklos reguliavimas.

Svarbiausi tyrimo *metodai* yra lyginamasis, sisteminis, kritinės analizės. Lyginamasis metodas naudojamas sugretinant Bendrojo duomenų apsaugos reglamento nuostatas su dabar galiojančiu duomenų apsaugos teisės reguliavimu. Sisteminis metodas leidžia nagrinėti duomenų apsaugos pareigūno institutą kaip Bendrojo duomenų apsaugos reglamento reguliavimo sistemos dalį. Kritinės analizės metodas padeda atskleisti probleminius teisinio reguliavimo aspektus.

Darbo aktualumą nulemia Bendrojo duomenų apsaugos reglamento naujumas. Duomenų apsaugos pareigūnų veiklos reguliavimas pagal Bendrąjį duomenų apsaugos reglamentą pasižymi abstraktumu ir vertinamųjų kriterijų gausa⁵. Tai didina šias normas aiškinančios teisės doktrinos aktualumą.

Autoritetinga teisės doktrina dar nepasižymi duomenų apsaugos pareigūnų veiklos reguliavimo tyrimų gausa. Moksliniuose darbuose aptarti pavieniai su duomenų apsaugos pareigūnų veiklos reguliavimu susiję aspektai. Clara Fritsch nagrinėjo duomenų apsaugos pareigūno reikšmę užtikrinant darbuotojų duomenų apsaugą⁶. Ericas Lachaudas nagrinėjo duomenų apsaugos pareigūnų kompetenciją patvirtinančio sertifikavimo problematiką ir perspektyvas⁷. Šiuo straipsniu siekiama papildyti esamą teisės doktriną sistemiskai analizuojant svarbiausius, bendrus duomenų apsaugos pareigūnų veiklos aspektus: išskirti konkrečias reguliavimo naujoves, atskleisti pareigos paskirti duomenų apsaugos pareigūną apimtį, apibrėžti duomenų apsaugos pareigūnų veiklos principus. Lietuvos teisės doktrinoje duomenų apsaugos pareigūno veiklos reguliavimas nebuvo nagrinėtas.

Pagrindiniai tyrimo šaltiniai yra Bendrasis duomenų apsaugos reglamentas ir šiuo metu duomenų apsaugą reguliuojantys 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 (toliau – Duomenų apsaugos direktyva)⁸ ir ją įgyvendinantis Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas (toliau – Duomenų apsaugos įstatymas)⁹. Tyrime remiamasi

⁵ Vien ko vertos Bendrojo duomenų apsaugos reglamento formuluotės, nustatančios pareigą paskirti duomenų apsaugos pareigūną. Pavyzdžiui, paskirti duomenų apsaugos pareigūną yra privaloma, jeigu 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 (Bendrojo duomenų apsaugos reglamento 37 str. 1 d. b p.). Šios nuostatos elementai Bendrajame duomenų apsaugos reglamente neapibrėžti ir gali būti viešai ir plačiai interpretuojami. Žr. šio straipsnio 2 dalį.

⁶ FRITSCH, Clara. Data Processing in Employment Relations; Impacts of the European General Data Protection Regulation Focusing on the Data Protection Officer at the Worksites. In GUTWIRTH, Serge; LEENES, Ronald; DE HERT, Paul (eds.). *Reforming European Data Protection Law*. Springer, 2015, p. 147–170.

⁷ LACHAUD, Eric. Should the DPO be certified? *International Data Privacy Law*, 2014, Vol. 4, No. 3, p. 189–202 [interaktyvus. Žiūrėta 2017 m. liepos 1 d.]. Ribojama prieiga per internetą: <<https://doi.org/10.1093/idpl/ipu008>>.

⁸ 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.

⁹ Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas. *Valstybės žinios*, 1996, Nr. 63-1479; 2000, Nr. 64-1924; 2003, Nr. 15-597; 2008, Nr. 22-804.

ES 29 str. darbo grupės priimtomis Gairėmis dėl duomenų apsaugos pareigūnų kaip autoritetingu Bendrojo duomenų apsaugos reglamento normas aiškinančiu *soft law* šaltiniu.

1. Esamas duomenų apsaugos pareigūno veiklos reguliavimas

Galiojantis duomenų apsaugos teisės reguliavimas nenumato pareigos paskirti duomenų apsaugos pareigūną. Pamatus nacionaliniam duomenų apsaugos reguliavimui padėjusi Duomenų apsaugos direktyva įtvirtino kelias su duomenų apsaugos pareigūnais susijusias nuostatas.

Pirma, Duomenų apsaugos direktyva numato ES valstybėms narėms galimybę supaprastinti reikalavimą pranešti apie duomenų tvarkymą priežiūros institucijai arba atleisti nuo jo, kai duomenų valdytojas paskiria pareigūną asmens duomenų apsaugai, kuris privalo nepriklausomai veikdamas užtikrinti, kad duomenų valdytojas laikytųsi nacionalinių duomenų apsaugos įstatymų, ir pildyti duomenų valdytojo atliktų tvarkymo operacijų registrą (Duomenų apsaugos direktyvos 18 str. 2 d. 2–4 įtraukos).

Antra, šiuo metu ES duomenų apsaugos teisė leidžia valstybėms narėms pasirinkti, kas atliks išankstines duomenų tvarkymo operacijų, kurios gali kelti konkretų pavojų duomenų subjekto teisėms ir laisvėms, patikras – priežiūros institucija, gavusi pranešimą iš duomenų valdytojo, arba duomenų apsaugos pareigūnas, kuris, kilus abejonų, privalo tartis su priežiūros institucija (Duomenų apsaugos direktyvos 20 str. 2 d.).

Lietuvos įstatymų leidėjas pasirinko nacionalinėje teisėje įtvirtinti už duomenų apsaugą atsakingo asmens ar padalinio institutą (Duomenų apsaugos įstatymo 32 str.). Tačiau iš įstatymo parengiamosios medžiagos¹⁰ ir už duomenų apsaugą atsakingo asmens ar padalinio instituto funkcijų (Duomenų apsaugos įstatymo 32 str. 2 d.) galima suprasti, kad jie vaidina duomenų apsaugos pareigūno vaidmenį ES duomenų apsaugos teisės prasme – padeda duomenų valdytojams užtikrinti atitiktį duomenų apsaugos reguliavimui (Duomenų apsaugos įstatymo 32 str. 2 d.). Duomenų apsaugos įstatymas įtvirtina teisę, bet ne pareigą paskirti tokį subjektą (Duomenų apsaugos įstatymo 32 str. 1 d.).

Tuo atveju, jei duomenų valdytojas pagal Duomenų apsaugos įstatymo 31 straipsnį turi pateikti Valstybinei duomenų apsaugos inspekcijai pranešimą apie duomenų tvarkymą ir yra paskyręs už duomenų apsaugą atsakingą asmenį (-is), jam gali būti taikoma supaprastinta pranešimo tvarka¹¹. Tai – iš esmės vienintelė pagal dabartinį nacionalinį reguliavimą numatyta duomenų apsaugos pareigūno paskyrimo nauda duomenų valdytojui. Valstybinė duomenų apsaugos inspekcija nėra paskelbusi metodinės medžiagos, kuri duomenų valdytojams padėtų geriau suprasti duomenų apsaugos pareigūno paskyrimo pranašumus ir jo funkcijų esmę¹².

Duomenų apsaugos pareigūno institutas įtvirtintas ir kai kuriose kitose ES valstybių narių jurisdikcijose. Duomenų apsaugos pareigūną paskirti pagal dabartinius duomenų apsaugos įstatymus pri-

¹⁰ Duomenų apsaugos įstatymo parengiamoji medžiaga rodo, kad įstatymu siekta sureguliuoti už duomenų apsaugą atsakingo asmens ar padalinio teisinį statusą atsižvelgiant į paminėtą Duomenų apsaugos direktyvos 18 straipsnį bei į ES valstybių patirtį. Žr. Įstatymų projektų Reg. Nr. XP-1350(2), XP-2363, XP-2364 aiškinamasis raštas [interaktyvus. Žiūrėta 2017 m. liepos 1 d.]. Prieiga per internetą: <<https://e-seimas.lrs.lt/portal/legalAct/lt/TAK/TAIS.300170?jfwid=x5bl5e0m3>>.

¹¹ Duomenų valdytojų pranešimo apie duomenų tvarkymą taisyklės, patvirtintos Lietuvos Respublikos Vyriausybės 2002 m. vasario 20 d. nutarimu Nr. 262, 8 punktas. *Valstybės žinios*, 2002, Nr. 20-768; 2005, Nr. 144-5249; *TAR*, 2015-09-11, Nr. 2015-13748).

¹² Konsultacijoje už duomenų apsaugą atsakingo asmens ar padalinio klausimu Valstybinė duomenų apsaugos inspekcija pateikė šio asmens ar padalinio funkcijų ir veiklos garantijų apibendrinimą. Žr. Valstybinė duomenų apsaugos inspekcija. Už duomenų apsaugą atsakingas asmuo ar padalinys – kas jis? (viešojo konsultacija), 2014 m. balandžio 1 d. [interaktyvus. Žiūrėta 2017 m. liepos 1 d.]. Prieiga per internetą: <<https://www.ada.lt/go.php/lit/2-uz-duomenu-apsauga-atsakingas-asmuo-ar-padalins--kas-jis-2014-04-01->>>.

valoma Vokietijoje ir Kroatijoje. Ispanijoje, Graikijoje, Vengrijoje ir Slovakijoje paskirti duomenų apsaugos pareigūnų reikalaujama tik tam tikruose sektoriuose¹³.

2. Duomenų apsaugos pareigūno vieta Bendrojo duomenų apsaugos reglamento sistemoje

Kitaip nei dabartiniuose Lietuvos, ES ir daugumos ES valstybių narių duomenų apsaugos įstatymuose, Bendrojo duomenų apsaugos reglamento 37 straipsnio 1 dalyje numatyta, kad dalis duomenų valdytojų ir tvarkytojų privalo paskirti duomenų apsaugos pareigūnų. Duomenų apsaugos pareigūno instituto vietą pagal naująjį reguliavimą galima atskleisti analizuojant Bendrąjį duomenų apsaugos reglamentą sisteminiu metodu.

Kaip fundamentalią naujojo reguliavimo naujovę galima išskirti tai, kad jis skatina pasitikėjimą duomenų valdytojais įpareigodamas juos prisiimti daugiau atsakomybės už duomenų tvarkymą ir mažina priežiūros institucijos kišimąsi į kasdienę duomenų tvarkymo veiklą¹⁴. Šiuo požiūriu yra reikšmingas naujas įtvirtinamas atskaitomybės principas. Pagal šį principą, duomenų valdytojas ne tik yra atsakingas už duomenų apsaugos teisės reikalavimų laikymąsi, bet ir turi sugebėti įrodyti, kad jos laikomasi (Bendrojo duomenų apsaugos reglamento 5 str. 2 d.). Atskaitomybės principu siekiama sustiprinti duomenų valdytojų vaidmenį ir sugriežtinti jų atsakomybę, paskatinti juos pasirinkti priemones atitinkamai užtikrinti¹⁵.

Bendrajame duomenų apsaugos reglamente daugybė pareigų formuluojama abstrakčiai, su vertinamaisiais kriterijais, paliekama nuožiūros laisvė patiems duomenų valdytojams pasirinkti reguliavimo interpretavimą ir pareigų įgyvendinimo būdus. Pavyzdžiui, pagal naują pritaikytosios ir standartizuotosios duomenų apsaugos (angl. *data protection by design* ir *data protection by default*) principą, duomenų valdytojui keliamas abstraktus reikalavimas įgyvendinti tinkamas technines ir organizacines priemones, kuriomis siekiama veiksmingai įgyvendinti duomenų apsaugos principus ir į duomenų tvarkymą integruoti būtinas apsaugos priemones, kad jis atitiktų duomenų apsaugos teisės reikalavimus, taip pat užtikrinti, kad standartizuotai būtų tvarkomi tik tie asmens duomenys, kurie yra būtini kiekvienam konkrečiam duomenų tvarkymo tikslui (Bendrojo duomenų apsaugos reglamento 25 str. 1 ir 2 d.).

Numatyta abstrakti pareiga įgyvendinti tinkamas technines ir organizacines priemones, kad būtų užtikrintas pavojų atitinkančio lygio saugumas, atsižvelgiant į techninių galimybių išsivystymo lygį, įgyvendinimo sąnaudas bei duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus, taip pat duomenų tvarkymo keliamus įvairios tikimybės ir rimtumo pavojus fizinių asmenų teisėms ir laisvėms (Bendrojo duomenų apsaugos reglamento 32 str. 1 d.).

Naujuoju reguliavimu nustatoma pareiga prieš pradėdant konkrečias duomenų tvarkymo operacijas įvertinti, ar duomenų tvarkymas gali sukelti didelį pavojų asmenų interesams, ir tokio galimo pavojaus atveju atlikti išankstinį poveikio duomenų apsaugai vertinimą (Bendrojo duomenų apsaugos reglamento 35 str. 1 d.). Jei poveikio duomenų apsaugai vertinimo išvada patvirtina didelį pavojų duomenų apsaugai, kyla kita nauja pareiga – iš anksto konsultuotis su priežiūros institucija (Bendrojo duomenų apsaugos reglamento 36 str. 1 d.). Bendrasis duomenų apsaugos reglamentas eksplicitiškai nustato, kad duomenų apsaugos pareigūnas turi būti įtrauktas į tokį vertinimą – jeigu jis yra paskirtas (Bendrojo duomenų apsaugos reglamento 35 str. 2 d.).

¹³ Baker & McKenzie. Appointment of a Data Protection Officer („DPO“) (Summary), 2017.

¹⁴ ZALESKIS, J. ES Bendrasis <...>, p. 50–51.

¹⁵ ES 29 str. darbo grupė. 2010 m. liepos 13 d. Nuomonė 3/2010 dėl atskaitomybės principo, Nr. WP173, p. 18 [interaktyvus. Žiūrėta 2015 m. balandžio 1 d.]. Prieiga per internetą: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp173_lt.pdf>.

Sisteminė Bendrojo duomenų apsaugos reglamento reguliavimo analizė leidžia daryti išvadą, kad duomenų apsaugos pareigūnui tenka svarbus vaidmuo interpretuojant ir įgyvendinant abstrakčius, principinius naujojo reguliavimo reikalavimus, grindžiamus vertinamaisiais kriterijais.

Pirma, pagal atskaitomybės principą, pats duomenų valdytojas turi įsivertinti savo atitiktį abstraktiems naujojo reguliavimo reikalavimams ir subėgti ją įrodyti. Minėtoms nuostatomis interpretuoti ir įgyvendinti reikia specialių žinių ir ekspertinės duomenų apsaugos teisės kompetencijos – būtent toks reikalavimas keliamas duomenų apsaugos pareigūnui (Bendrojo duomenų apsaugos reglamento 37 str. 5 d.).

Antra, įtvirtinamos duomenų apsaugos pareigūno funkcijos konsultuoti duomenų valdytoją arba duomenų tvarkytoją ir duomenis tvarkančius darbuotojus apie abstrakčius naujojo reguliavimo reikalavimus (39 str. 1 d. a p.), stebėti atitiktį ir rūpintis atitikties auditais (39 str. 1 d. a p.).

Trečia, duomenų apsaugos pareigūno kertinį vaidmenį Bendrojo duomenų apsaugos reglamento sistemoje patvirtina autoritetingi *soft law* šaltiniai. 29 str. darbo grupė duomenų apsaugos pareigūno paskyrimą išskiria kaip svarbią atskaitomybės principo įgyvendinimo priemonę¹⁶. Duomenų valdytojams ir duomenų tvarkytojams, kuriems nekyla pareigos paskirti duomenų apsaugos pareigūną, rekomenduojama tai padaryti dėl naudos įgyvendinant teisinius reikalavimus¹⁷.

3. Pareigos paskirti duomenų apsaugos pareigūną įtvirtinimo būdas

Bendrojo duomenų apsaugos reglamento 37 straipsnio 1 dalyje numatoma, kad duomenų apsaugos pareigūną paskirti privalo:

- 1) valdžios institucijos arba įstaigos, išskyrus teismus, kai jie vykdo teismo funkcijas;
- 2) duomenų valdytojai arba duomenų tvarkytojai, kurių pagrindinė veikla yra duomenų tvarkymo operacijos, dėl kurių pobūdžio, aprėpties ir (arba) tikslų būtina reguliariai ir sistemingai dideliu mastu stebėti duomenų subjektus; arba
- 3) duomenų valdytojai arba duomenų tvarkytojai, kurių pagrindinė veikla yra specialių kategorijų duomenų, duomenų apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas tvarkymas dideliu mastu.

Bendrasis duomenų apsaugos reglamentas nustato svarbią pareigą paskirti duomenų apsaugos pareigūną duomenų valdytojams ir duomenų tvarkytojams palikdamas pilkąją zoną interpretuoti pareigos pagrindus. Kyla klausimas, ar toks abstraktus, vertinamaisiais kriterijais pagrįstas pareigos paskirti duomenų apsaugos pareigūną įtvirtinimas yra racionalus.

Viena vertus, duomenų apsaugos teisė pasižymi abstrakčiais, principiniais reikalavimais, kurie leidžia sureguliuoti itin įvairias su informacijos apie asmenis naudojimu susijusias situacijas. Abstrakčios formulotės leidžia užtikrinti technologinio neutralumo principo veikimą. Siekiant, kad būtų išvengta rimtos teisės aktų apėjimo grėsmės, fizinių asmenų apsauga turėtų būti neutrali technologijų atžvilgiu ir turėtų nepriklausyti nuo taikomų metodų (Bendrojo duomenų apsaugos reglamento preambulės 15 p.). Teisės moksle duomenų apsauga apibrėžiama būtent abstrakčiais asmeninės informacijos tvarkymo principais¹⁸. Tradicija asmens duomenų apsaugos teisės reikalavimus vadinti principais yra nusistovėjusi teisės doktrinoje¹⁹.

¹⁶ ES 29 str. darbo grupė. *2010 m. liepos 13 d. Nuomonė 3/2010 <...>*, p. 6, 9.

¹⁷ ES 29 str. darbo grupė. *Gairės <...>*, p. 4.

¹⁸ BYGRAVE, Lee A. *Data Protection Law. Approaching Its Rationale, Logic and Limits*. Dordrecht: Kluwer Law International, 2002, p. 22.

¹⁹ PETRAITYTĖ, Ilona. *Asmens duomenų teisinės apsaugos principai*: daktaro disertacija. Socialiniai mokslai, teisė (01S). Vilnius: Vilniaus universitetas, 2013, p. 90–91.

Kita vertus, kritinės analizės metodas leidžia išryškinti aptarto reguliavimo būdo trūkumus. Teisės norminiu reguliavimu neapibrėžus pamatinių duomenų apsaugos pareigūnų veiklos reguliavimo sąvokų, kyla rizika, kad duomenų valdytojas gali pasirinkti normų interpretavimą, kuris neatitiks priežiūros institucijos požiūrio. Pareigos paskirti duomenų apsaugos pareigūną kontekste reguliavimo atvirumą plačiai interpretacijai galima vertinti kritiškai dėl kelių priežasčių.

Pirma, atlikta sisteminė Bendrojo duomenų apsaugos reglamento normų analizė rodo, kad duomenų apsaugos pareigūnas yra kritinė naujojo reguliavimo figūra, nuo kurios priklauso atitiktis kitiems teisiniams reikalavimams. Duomenų apsaugos pareigūno paskyrimas nulemia Bendrojo duomenų apsaugos reglamento įgyvendinimo procesą, poreikį peržiūrėti organizacinę struktūrą, žmogiškuosius ir finansinius išteklius. Jeigu įsivertinti kitų abstrakčių teisės normų atitiktį duomenų valdytojui ar duomenų tvarkytojui turi padėti duomenų apsaugos pareigūnas, kyla klausimas, kas turi padėti duomenų valdytojui ar duomenų tvarkytojui įsivertinti, ar jam reikalingas pats duomenų apsaugos pareigūnas.

Antra, sisteminė Bendrojo duomenų apsaugos reglamento analizė rodo, kad duomenų apsaugos klausimai gali būti reguliuojami ir aukštesnio lygio apibrėžtumą užtikrinančia juridine technika. Pavyzdžiui, naujuoju reguliavimu nustatoma pareiga prieš pradėdant konkrečias duomenų tvarkymo operacijas, galinčias sukelti didelį pavojų asmenų interesams, atlikti išankstinį poveikio duomenų apsaugai vertinimą (Bendrojo duomenų apsaugos reglamento 35 str. 1 d.). Ši abstrakti ir plačiai interpretacijai atvira norma detalizuota, įvardijant kelis didelį pavojų asmenų interesams galinčių sukelti duomenų tvarkymo operacijų pavyzdžius (Bendrojo duomenų apsaugos reglamento 35 str. 3 d.). Nustatyti ir viešai paskelbti išsamų duomenų tvarkymo operacijų, kurioms taikomas reikalavimas atlikti poveikio duomenų apsaugai vertinimą, rūšių sąrašą pavesta priežiūros institucijai (Bendrojo duomenų apsaugos reglamento 35 str. 4 d.), kuri gali paskelbti ir vertinimo nereikalaujančių operacijų sąrašą (35 str. 5 d.).

Trečia, nėra neįmanoma išgryninti konkretesnių pareigos paskirti duomenų apsaugos pareigūną kriterijų. 29 str. darbo grupė jau pasiūlė autoritetingus reguliavimo normų išaiškinimus, nulemiančius pareigą paskirti duomenų apsaugos pareigūną. Jos nuomonė laikoma autoritetingu norminio reguliavimo aiškinimo šaltiniu²⁰.

Ketvirta, duomenų apsaugos teisės reguliavimas riboja komercinės veiklos laisvę kaip pamatinę žmogaus laisvę²¹. Žmogaus teisių ribojimams keliami kokybiniai, apibrėžtumo reikalavimai. Pagal Europos Žmogaus Teisių Teismo praktiką, ribojimai turi būti formuluojami taip, kad leistų asmenims suprasti savo teisių ir pareigų aprėptį ir atitinkama linkme kreipti savo elgesį²². Kyla abejonė, kiek aptartas reguliavimas leidžia duomenų valdytojams ir duomenų tvarkytojams suvokti savo pareigos paskirti duomenų apsaugos pareigūną apimtį.

Penkta, esminių Bendrojo duomenų apsaugos reglamento normų turinio atskleidimas tik 29 str. darbo grupės išaiškinimais gali būti vertinamas kritiškai. Ši patariamoji darbo grupė teikia formaliai neprivalomas ES duomenų apsaugos teisės reguliavimo rekomendacijas (Duomenų apsaugos direktyvos 29 str. 1 d., 30 str. 3 d.). Jos nesaisto ES teisėkūros procedūros. 29 str. darbo grupės rekomendacijos nėra prienamos lietuvių kalba ir yra nebūtinai žinomos plačiajai visuomenei.

²⁰ KUNER, Christopher. *European Data Protection Law: Corporate Compliance and Regulation (Second Edition)*. Oxford University Press: 2007, p. 10. Pavyzdžiui, Lietuvos vyriausiasis administracinis teismas, sprenddamas duomenų apsaugos teisės aiškinimo klausimus, 29 str. darbo grupės nuomonėmis remiasi itin plačiai kaip Duomenų apsaugos direktyvos turinį ir jo aiškinimo praktiką atskleidžiančių šaltiniu. Žr. Lietuvos vyriausiasis administracinis teismas. 2012 m. liepos 26 d. nutartis adm. byloje Nr. A858-2133/2012 EDRAUDA, UADBB v. Valstybinė duomenų apsaugos inspekcija.

²¹ Lietuvos Respublikos Konstitucija (su pakeitimais ir papildymais). *Valstybės žinios*, 1992, Nr. 33-1014; *Lietuvos Aidas*, 1992, Nr. 220, 46 str. 1 d. [interaktyvus. Žiūrėta 2017 m. liepos 1 d.]. Prieiga per internetą: <<https://www.e-tar.lt/portal/lt/legalAct/TAR.47BB952431DA/bHVIIIKgQy>>.

²² VAN DIJK, Pieter, et al. (eds.). *Theory and Practice of the European Convention on Human Rights. Fourth Edition*. Oxford: Intersentia, 2006, p. 336–337.

Šešta, daugiau teisinio apibrėžtumo neturėtų atsirasti priėmus naujos redakcijos Duomenų apsaugos įstatymą, kuriuos siekiama užtikrinti aukštą asmens duomenų apsaugos lygį taikant Bendrąjį duomenų apsaugos reglamentą (projekto 1 str. 1 d.). Paskelbtame naujojo Duomenų apsaugos įstatymo projekte nėra numatoma jokių nuostatų, kurios papildytų ar paaiškintų Bendrajame duomenų apsaugos reglamente įtvirtintą duomenų apsaugos pareigūnų veiklos reguliavimą²³.

4. Duomenų apsaugos pareigūno paskyrimo pagrindų turinys

Pareiga paskirti duomenų apsaugos pareigūną mažiau klausimų pagal Bendrąjį duomenų apsaugos reglamentą kelia valdžios institucijoms ir įstaigoms. Kas yra valdžios institucijos ir įstaigos, turi būti nustatoma pagal nacionalinę ES valstybių narių teisę.

Sisteminė paminėtų nuostatų analizė rodo, kad kitais atvejais pareiga paskirti duomenų apsaugos pareigūną kyla, kai duomenų valdytojai arba tvarkytojai pagal Bendrojo duomenų apsaugos reglamento 37 straipsnio 2 dalies 2 ir 3 punktus atitinka tris galimus išskirti – (1) didesnio pavojaus duomenų tvarkymo, (2) pagrindinės veiklos ir (3) duomenų tvarkymo masto – kriterijus.

Pagal Bendrajame duomenų apsaugos reglamente numatytą didesnio pavojaus duomenų tvarkymo kriterijų, pareiga paskirti duomenų apsaugos pareigūną gali kilti duomenų valdytojams ir tvarkytojams, kurie užsiima viena iš dviejų veiklų: (1) reguliariai ir sistemingai stebi duomenų subjektus arba (2) tvarko jautresnius duomenis – specialių kategorijų duomenis²⁴, duomenis apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas.

Reguliavimas neapibrėžia duomenų subjektų stebėsenos, tik nurodo vartotojų elgesiu grindžiamą reklamą kaip tokios veiklos pavyzdį (Bendrojo duomenų apsaugos reglamento preambulės 24 p.). Kad nulemtų pareigą paskirti duomenų apsaugos pareigūną, duomenų subjektų stebėseną turi būti reguliari ir sisteminga.

Reguliarai galima laikyti tokią veiklą, kuri yra tebetrunkanti ar pasikartojanti tam tikrą laiką tam tikrais periodais, atsinaujinanti ar besikartojanti nustatytu laiku arba vykstanti nuolat ar periodiškai. Sąvoka „sisteminga“ aiškinama kaip vykstanti pagal sistemą arba iš anksto nustatyta, organizuota ar metodinė, arba vykstanti kaip bendro duomenų rinkimo plano dalis ar strategijos dalis. Reguliarai ir sisteminga duomenų subjektų stebėseną gali būti laikoma tokia veikla: asmenų profiliavimas rizikos vertinimo tikslais (pavyzdžiui, kreditingumo vertinimo, draudimų įmokų nustatymo, pinigų plovimo prevencijos tikslais), asmens buvimo vietos stebėjimas mobiliųjų telefonų programėlėmis, lojalumo programų vykdymas, daiktų interneto (angl. *internet of things*), išmaniųjų skaitiklių, automobilių, namų valdymas²⁵.

Pagal Bendrojo duomenų apsaugos reglamento lietuvišką tekstą, pagrindinės veiklos kriterijus reiškia, kad reguliari ir sisteminga asmens stebėseną arba specialių kategorijų duomenų, duomenų apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas tvarkymas yra „duomenų valdytojo arba duomenų tvarkytojo pagrindinė veikla“ (Bendrojo duomenų apsaugos reglamento 37 str. 1 d. b ir c punktai). Kritinė reguliavimo teksto kitomis kalbomis analizė ir autoritetinga jo aiškinimo praktika leidžia manyti, kad paminėta formuluotė netiksliai atspindi teisės normos esmę.

Pirma, Bendrojo duomenų apsaugos reglamento tekstai kitomis kalbomis rodo, kad pagrindinė duomenų valdytojo arba duomenų tvarkytojo veikla turi ne būti paminėtas duomenų tvarkymas, o susidėti, būti sudaryta iš tokio duomenų tvarkymo, jį apimti. Pavyzdžiui, angliškame tekste vartojama

²³ Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo Nr. I-1374 pakeitimo įstatymo projektas [interaktyvus. Žiūrėta 2017 m. liepos 1 d.]. Prieiga per internetą: <http://www.lrs.lt/pls/proj/dokpaieska.showdoc_l?p_id=1237785&p_org=8&p_fix=y>.

²⁴ Tai – duomenys, atskleidžiantys rasinę ar etninę kilmę, politines pažiūras, religinius ar filosofinius įsitikinimus ar narystę profesinėse sąjungose, taip pat tvarkyti genetinius duomenis, biometrinius duomenis, siekiant konkrečiai nustatyti fizinio asmens tapatybę, sveikatos duomenis arba duomenis apie fizinio asmens lytinį gyvenimą ir lytinę orientaciją (Bendrojo duomenų apsaugos reglamento 9 str. 1 d.).

²⁵ ES 29 str. darbo grupė. *Gairės* <...>, p. 8–9.

formuluotė „*the core activities of the controller or the processor consist of processing*“²⁶. Prancūziška- me reglamento tekste vartojama angliškam tekstui analogiška formuluotė – „*consistent en*“.

Antra, paminėtas vertimas tiksliau atspindi nuostatos logiką, kurią atskleidė 29 str. darbo grupės nuomonė. Pagal ją, pagrindinės veiklos nuostata neturi būti aiškinama kaip neapimanti veiklos, kai duomenų tvarkymas yra neatsiejama duomenų valdytojo ar tvarkytojo veiklos dalis. Pateikiami du duomenų tvarkymo atvejai, kurie reikalaujant paskirti duomenų apsaugos pareigūną, tačiau nebūtinai yra pagrindinė atitinkamo duomenų valdytojo arba duomenų tvarkytojo veikla pagal lietuviško Bendrojo duomenų apsaugos reglamento teksto prasmę. Tai – sveikatos priežiūros įstaigų veikla ir apsaugos bendrovių atliekamas vaizdo stebėjimas prekybos centruose²⁷.

Normų analizė suponuoja, kad griežčiau yra reguliuojamas toks didesnį pavojų keliantis duomenų tvarkymas, kuris duomenų valdytojui ar duomenų tvarkytojui leidžia pasiekti komercinius, profesinius ar kitus svarbiausius tikslus, tačiau ne personalo valdymo, saugumo ar kitus administracinius tikslus. Bendrojo duomenų apsaugos reglamento preambulėje patikslinama, kad aptariamoms nuostatomis neapima atvejų, kai duomenų tvarkymas duomenų valdytojui arba duomenų tvarkytojui yra papildoma veikla (preambulės 97 punktą).

Duomenų tvarkymo masto kriterijus reiškia, kad paminėtas duomenų tvarkymas turi ne tik būti pagrindinė duomenų valdytojo ar tvarkytojo veiklos dalis, bet ir vykti dideliu mastu. Reguliavimas neapibrėžia, kada duomenų tvarkymo mastas yra laikomas dideliu. Pats duomenų valdytojas arba tvarkytojas turi nustatyti, ar jo atliekamo duomenų tvarkymo mastas yra didelis.

Siekiant įvertinti duomenų tvarkymo mastą, reikėtų atsižvelgti į tokius kriterijus: (1) duomenų subjektų, kurių duomenys tvarkomi, skaičius arba dalis; (2) tvarkomų duomenų kiekis ir jo svyravimai; (3) duomenų tvarkymo trukmė ir nuolatinumas; (4) duomenų tvarkymo geografinė aprėptis. Didelio masto duomenų tvarkymu gali būti laikomas pacientų duomenų tvarkymas įprastoje sveikatos priežiūros įstaigos veikloje, duomenų apie asmenų keliones naudojantis miesto viešojo transporto sistema tvarkymas (pvz., naudojantis keleivio kortelėmis), klientų duomenų tvarkymas įprastoje finansų įstaigų veikloje, duomenų tvarkymas vartotojų elgesiu grindžiamos reklamos tikslais paieškos sistemoje, telefonijos arba interneto paslaugų teikėjo atliekamas duomenų (turinio, srauto, buvimo vietos) tvarkymas²⁸.

5. Duomenų apsaugos pareigūno veiklos principai

Bendruoju duomenų apsaugos reglamentu nustatomas duomenų apsaugos pareigūnų veiklos reguliavimas ne griežtai apibrėžia aiškias konkrečias elgesio taisykles, bet numato bendresnes elgesio gaires, palikdamas nuožiūros laisvę pasirinkti konkretų elgesio modelį. Tokios normos, vadovaujantis Ronaldo Dworkino teorija, panašesnės ne į įprastas teisės normas, kurioms būdingas „viskas arba nieko“ veikimas, leidžiantis iš karto lengvai nustatyti, ar norma buvo pažeista, bet į abstraktesnius teisės principus, reikalaujančius vertybių balansavimo kiekvienu konkrečiu atveju²⁹.

Sisteminė Bendrojo duomenų apsaugos reglamento nuostatų analizė pirmiausia leidžia išskirti ekspertinės kompetencijos principą. Duomenų apsaugos pareigūnas turi būti skiriamas remiantis profesinėmis savybėmis, visų pirma duomenų apsaugos teisės ir praktikos ekspertinėmis žiniomis, taip pat gebėjimu atlikti nustatytas teisinio reguliavimo užduotis (Bendrojo duomenų apsaugos reglamento 37 str. 5 d.). Būtinai ekspertinių žinių lygis turėtų būti nustatomas visų pirma atsižvelgiant į atliekamas

²⁶ Angliška Bendrojo duomenų apsaugos reglamento tekste vartojamas veiksmažodis *consist* į lietuvių kalbą vėriamas „susidėti“, „susidaryti“. Žr. Alkonas. Žodynas internete [interaktyvus. Žiūrėta 2017 m. liepos 1 d.]. Prieiga per internetą: <<http://www.alkonas.lt/zodzio/consist/vertimas>>.

²⁷ ES 29 str. darbo grupė. *Gairės* <...>, p. 7.

²⁸ ES 29 str. darbo grupė. *Gairės* <...>, p. 7–8.

²⁹ DWORKIN, Ronald. *Taking Rights Seriously*. Cambridge: Harvard University Press, 1978, p. 22–28.

duomenų tvarkymo operacijas ir duomenų valdytojo arba duomenų tvarkytojo tvarkomų asmens duomenų reikiamą apsaugą (Bendrojo duomenų apsaugos reglamento preambulės 97 punktą).

Bendrasis duomenų apsaugos reglamentas nenustato konkretesnių reikalavimų duomenų apsaugos pareigūnų kompetencijai. Teisės doktrinoje pasisakoma, kad duomenų apsaugos pareigūnų sertifikavimas labiau užtikrintų priežiūros institucijas ir duomenų valdytojus ir tvarkytojus apie duomenų apsaugos pareigūnų atitiktį keliamiems reikalavimams, leistų užtikrinti aukštesnį ir nuoseklesnį duomenų apsaugos lygį visoje ES³⁰.

Vis dėlto Bendrajame duomenų apsaugos reglamente nebuvo nustatyta privalomo duomenų apsaugos pareigūnų kompetencijos patvirtinimo mechanizmo. Ekspertinių žinių reikalavimas pirmiausia suponuoja teisinės žinias, nes duomenų apsaugos pareigūnas turi išmanyti europinius ir nacionalinius duomenų apsaugos įstatymus (ne tik Bendrąjį duomenų apsaugos reglamentą) ir turėti gilų Bendrojo duomenų apsaugos reglamento supratimą. Duomenų apsaugos pareigūnui taip pat padėtų bendros informacinių sistemų, duomenų saugumo, verslo sektoriaus, kuriame veikia duomenų valdytojas ar duomenų tvarkytojas, žinios³¹.

Atsižvelgiant į atskaitomybės principą (Bendrojo duomenų apsaugos reglamento 5 str. 2 d.), pats duomenų valdytojas ar duomenų tvarkytojas turi patikrinti, ar duomenų apsaugos pareigūnas turi reikiamų duomenų apsaugos teisės ir praktikos ekspertinių žinių ir sugebėti tai įrodyti jam prieinamomis priemonėmis, pavyzdžiui, duomenų apsaugos pareigūno išsilavinimo, kvalifikacijos tobulinimo, dalyvavimo įvairiuose duomenų apsaugos teisės seminaruose ir konferencijose pažymomis ar patikrinimų rezultatais³².

Antra, galima išskirti nepriklausomumo principą, reiškiantį, kad duomenų apsaugos pareigūnas neturi gauti nurodymų dėl savo užduočių vykdymo. Duomenų valdytojas arba duomenų tvarkytojas negali jo atleisti arba bausti dėl jam nustatytų užduočių atlikimo. Duomenų apsaugos pareigūnas tiesiogiai atsiskaito duomenų valdytojo arba duomenų tvarkytojo aukščiausio lygio vadovybei (Bendrojo duomenų apsaugos reglamento 38 str. 3 d.). Duomenų apsaugos pareigūno nepriklausomumas nėra įmanomas be tinkamo pareigūno aprūpinimo. Duomenų apsaugos pareigūnui turi būti suteikti jo užduotims atlikti būtini išteklių, galimybė susipažinti su asmens duomenimis, dalyvauti duomenų tvarkymo operacijose ir išlaikyti savo ekspertines žinias (Bendrojo duomenų apsaugos reglamento 38 str. 2 d.).

Trečia, iš Bendrojo duomenų apsaugos reglamento normų galima išvesti interesų konflikto vengimo principą. Jis svarbus tuo, kad duomenų apsaugos pareigūnas gali vykdyti kitas užduotis ir pareigas. Duomenų valdytojas arba duomenų tvarkytojas užtikrina, kad dėl bet kokių tokių užduočių ir pareigų nekiltų interesų konfliktas (Bendrojo duomenų apsaugos reglamento 38 str. 6 d.). Interesų konfliktas gali kilti, jeigu duomenų apsaugos pareigūno funkcijas atliekantis asmuo dalyvautų priimančiam duomenų valdytojo ar tvarkytojo sprendimus dėl duomenų tvarkymo. Pavyzdžiui, su duomenų apsaugos pareigūno funkcijomis sunkiai suderinamos organizacijos ar jos žmogiškųjų išteklių, informacinių technologijų, rinkodaros ar finansų vadovų pareigos³³.

Ketvirta, galima išskirti prieinamumo principą. Jis nulemia, kad duomenų apsaugos pareigūnas turi būti pasiekiamas visiems suinteresuotiems asmenims: duomenų valdytojams ir tvarkytojams, jų vadovams ir darbuotojams, duomenų subjektams, priežiūros institucijoms. Duomenų valdytojas arba duomenų tvarkytojas paskelbia duomenų apsaugos pareigūno kontaktinius duomenis ir praneša juos

³⁰ LACHAUD, E. Should <...>, p. 191–192.

³¹ ES 29 str. darbo grupė. *Gairės* <...>, p. 11.

³² Duomenų apsaugos pareigūnų kvalifikacija, kaip ir atitiktis kitiems Bendrojo duomenų apsaugos reglamento reikalavimams, ateityje gali būti savanoriškai tvirtinama pagal bendrą sertifikavimo procedūrą (Bendrojo duomenų apsaugos reglamento 42 str.)

³³ ES 29 str. darbo grupė. *Gairės* <...>, p. 16.

priežiūros institucijai (Bendrojo duomenų apsaugos reglamento 37 str. 7 d.). Duomenų subjektai gali kreiptis į duomenų apsaugos pareigūną visais klausimais, susijusiais su jų asmeninių duomenų tvarkymu ir naudojimu savo teisėmis (Bendrojo duomenų apsaugos reglamento 38 str. 4 d.).

Penkta, reguliavimo analizė leidžia išskirti duomenų apsaugos pareigūno veiklos formos laisvės principą. Duomenų valdytojai ir tvarkytojai gali pasirinkti patikėti duomenų apsaugos pareigūno funkcijas darbuotojui ar tokią paslaugą pagal sutartį teikiančiam fiziniam ar juridiniam asmeniui (Bendrojo duomenų apsaugos reglamento 37 str. 6 d.).

Iš duomenų apsaugos pareigūno remiantis Bendruoju duomenų apsaugos reglamentu reikalaujama teisinės kompetencijos. Duomenų apsaugos pareigūno paskirtis yra padėti ir patarti, kaip užtikrinti duomenų valdytojų ir duomenų tvarkytojų atitiktį konkrečiam teisės aktui – Bendrajam duomenų apsaugos reglamentui – ir kitiems teisės šaltiniams duomenų apsaugos srityje (Bendrojo duomenų apsaugos reglamento 39 str. 1 d. b p.). Savo esme tai yra teisės konsultacijos (patarimai teisės klausimais), teisinę reikšmę turinčių dokumentų rengimas. Tokio pobūdžio paslaugos patenka į advokatų teikiamų teisinių paslaugų apibrėžimą (Lietuvos Respublikos advokatūros įstatymo³⁴ 2 str. 1 d.). Todėl duomenų apsaugos pareigūno paslaugas galėtų teikti ir Lietuvos advokatūros reguliavimo nustatyta tvarka veikiantys advokatai.

Kita vertus, ribas advokatų teikiamoms duomenų apsaugos pareigūno paslaugoms apibrėžia ne tik advokatūros reguliavimas, bet ir išskirti duomenų apsaugos pareigūno veiklos principai. Advokatas galėtų teikti duomenų apsaugos pareigūno paslaugas, jeigu atitinka visus aptartus principus, įskaitant ekspertinės kompetencijos principą, reiškiantį, kad advokatas turėtų specializuotis duomenų apsaugos teisės srityje. Advokato teikiamos duomenų apsaugos pareigūno paslaugos taip pat neturėtų pažeisti interesų konflikto vengimo principo. Pavyzdžiui, interesų konfliktas galėtų kilti, jei duomenų apsaugos pareigūno paslaugas teikiantis advokatas būtų paprašytas atstovauti duomenų valdytojui ar tvarkytojui teisiniuose ginčuose dėl duomenų apsaugos³⁵. Tokiu atveju tas pats advokatas, viena, prižiūrėtų atitiktį duomenų apsaugos reguliavimui ir, kita, siektų ją apginti.

Išvados

1. Sisteminė Bendrojo duomenų apsaugos reglamento analizė leidžia prognozuoti, kad duomenų apsaugos pareigūno institutas užims centrinę naujojo reguliavimo vietą. Tokią prognozę nulemia naujai įtvirtinamas atskaitomybės principas, reikalaujantis, kad duomenų valdytojai prisiimtų daugiau atsakomybės už atitiktį, reguliavimo reikalavimų formulavimas abstrakčiu būdu, reikalaujančiu iš duomenų valdytojų ekspertinės kompetencijos interpretuojant ir įgyvendinant paminėtus reikalavimus, ir duomenų apsaugos pareigūnui keliamas reikalavimas turėti tokią kompetenciją.
2. Bendrojo duomenų apsaugos reglamento nuostatas, nustatančias kriterijus, pagal kuriuos yra privaloma paskirti duomenų apsaugos pareigūną, galima vertinti kritiškai dėl teisinio apibrėžtumo, aiškumo trūkumo. Būtų tikslinga detalizuoti teisinio reguliavimo atvejus, kada reikia paskirti duomenų apsaugos pareigūną.
3. Tam, kad duomenų valdytojams ir duomenų tvarkytojams (be valdžios institucijų ir įtaigų) kiltų pareiga paskirti duomenų apsaugos pareigūną, jie turi atitikti tris akumuliatyvias sąlygas, kurias leidžia išskirti reguliavimo analizė: (1) didesnės rizikos veiklos sąlygą (reiškiančią, kad duomenų valdytojas ar duomenų tvarkytojas turi užsiimti specialią kategorijų duomenų, duomenų apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas tvarkymu arba asmenų stebėseną);

³⁴ Lietuvos Respublikos advokatūros įstatymas. *Valstybės žinios*, 2004-04-06, Nr. 50-1632 [interaktyvus. Žiūrėta 2017 m. liepos 1 d.]. Prieiga per internetą: <<https://www.e-tar.lt/portal/lt/legalAct/TAR.9F4371AB03A3/ZvymHaHLJk>>.

³⁵ ES 29 str. darbo grupė. *Gairės* <...>, p. 16.

- (2) veiklos masto sąlygą (reiškiančią, kad paminėtas duomenų tvarkymas turi vykti dideliu mastu);
- (3) pagrindinės veiklos sąlygą (reiškiančią, kad pagrindinė duomenų valdytojo ar duomenų tvarkytojo veikla turi apimti paminėtą duomenų tvarkymą).
4. Pagrindinės veiklos kriterijaus lietuviškame Bendrojo duomenų apsaugos reglamente formuluotė galima vertinti kaip netikslią. Tam, kad kiltų pareiga paskirti duomenų apsaugos pareigūną, pagrindinė duomenų valdytojo arba duomenų tvarkytojo veikla turėtų būti ne didesnės rizikos duomenų tvarkymas, kaip numatyta lietuviškame tekste, o apimti tokių duomenų tvarkymą.
 5. Bendrojo duomenų apsaugos reglamento analizė rodo, kad duomenų apsaugos pareigūnų veiklos reguliavimas yra grindžiamas ne detaliais, konkretų elgesio modelį nustatančiais reikalavimais, o bendresniais principais. Galima išskirti tokius duomenų apsaugos pareigūnų veiklos principus: ekspertinės kompetencijos, nepriklausomumo, interesų konflikto vengimo, prieinamumo, veiklos formos laisvės.

LITERATŪRA

Norminiai teisės aktai

1. Lietuvos Respublikos Konstitucija (su pakeitimais ir papildymais). *Valstybės žinios*, 1992, nr. 33-1014; *Lietuvos Aidas*, 1992, nr. 220, 46 str. 1 d. [interaktyvus. Žiūrėta 2017 m. liepos 1 d.]. Prieiga per internetą: <<https://www.e-tar.lt/portal/lt/legalAct/TAR.47BB952431DA/bHVIIIKgQy>>.
2. 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.
3. 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.
4. Lietuvos Respublikos advokatūros įstatymas. *Valstybės žinios*, 2004, nr. 50-1632 [interaktyvus. Žiūrėta 2017 m. liepos 1 d.]. Prieiga per internetą: <<https://www.e-tar.lt/portal/lt/legalAct/TAR.9F4371AB03A3/ZvgmHaHLJk>>.
5. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas. *Valstybės žinios*, 1996, nr. 63-1479; 2000, nr. 64-1924; 2003, nr. 15-597; 2008, nr. 22-804.
6. Duomenų valdytojų pranešimo apie duomenų tvarkymą taisyklės, patvirtintos Lietuvos Respublikos Vyriausybės 2002 m. vasario 20 d. nutarimu Nr. 262. *Valstybės žinios*, 2002, nr. 20-768; 2005, nr. 144-5249; *TAR*, 2015-09-11, nr. 2015-13748).

Specialioji literatūra

7. BYGRAVE, Lee A. *Data Protection Law. Approaching Its Rationale, Logic and Limits*. Dordrecht: Kluwer Law International, 2002.
8. FRITSCH, Clara. Data Processing in Employment Relations; Impacts of the European General Data Protection Regulation Focusing on the Data Protection Officer at the Worksite. In GÜTWIRTH, Serge; LEENES, Ronald; DE HERT, Paul (eds.). *Reforming European Data Protection Law*. Springer, 2015, p. 147–170.
9. KUNER, Christopher. *European Data Protection Law: Corporate Compliance and Regulation (Second Edition)*. Oxford University Press: 2007.
10. LACHAUD, Eric. Should the DPO be certified? *International Data Privacy Law*, 2014, Vol. 4, No. 3, p. 189–202 [interaktyvus. Žiūrėta 2017 m. liepos 1 d.]. Ribota prieiga per internetą: <<https://doi.org/10.1093/idpl/ipu008>>.
11. PETRAITYTĖ, Ilona. *Asmens duomenų teisinės apsaugos principai*: daktaro disertacija. Socialiniai mokslai, teisė (01S). Vilnius: Vilniaus universitetas, 2013.
12. VAN DIJK, Pieter, et al. (eds.). *Theory and Practice of the European Convention on Human Rights. Fourth Edition*. Oxford: Intersentia, 2006, p. 336–337.
13. ZALESKIS, Julius. ES Bendrasis duomenų apsaugos reglamentas: reikšmė duomenų apsaugos teisei. *Teisė*, 2017, t. 103, p. 45–54 [interaktyvus. Žiūrėta 2017 m. liepos 26 d.]. Prieiga per internetą: <<http://www.zurnalai.vu.lt/teis/article/view/10779>>.

Teismų praktika

14. Lietuvos vyriausiasis administracinis teismas. 2012 m. liepos 26 d. nutartis adm. byloje Nr. A⁸⁵⁸-2133/2012 EDRAUDA, UADBB v. Valstybinė duomenų apsaugos inspekcija.

Soft law šaltiniai

15. ES 29 str. darbo grupė. 2016 m. gruodžio 13 d. *Gairės dėl duomenų apsaugos pareigūnų (DAP)*, Nr. WP 243, p. 4 [interaktyvus. Žiūrėta 2017 m. balandžio 1 d.]. Prieiga per internetą: <http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf>.

16. ES 29 str. darbo grupė. 2010 m. liepos 13 d. *Nuomonė 3/2010 dėl atskaitomybės principo*, Nr. WP173, p. 6 [interaktyvus. Žiūrėta 2017 m. liepos 1 d.]. Prieiga per internetą: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp173_lt.pdf>.

17. Valstybinė duomenų apsaugos inspekcija. Už duomenų apsaugą atsakingas asmuo ar padalinys – kas jis? (viešoji konsultacija), 2014 m. balandžio 1 d. [interaktyvus. Žiūrėta 2017 m. liepos 1 d.]. Prieiga per internetą: <<https://www.ada.lt/go.php/lit/2-uz-duomenu-apsauga-atsakingas-asmuo-ar-padaliny--kas-jis-2014-04-01->>.

Kiti šaltiniai

18. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo Nr. I-1374 pakeitimo įstatymo projektas [interaktyvus. Žiūrėta 2017 m. liepos 1 d.]. Prieiga per internetą: <http://www.lrs.lt/pls/proj/dokpaieska.showdoc_l?p_id=1237785&p_org=8&p_fix=y>.

19. Įstatymų projektų Reg. Nr. XP-1350(2), XP-2363, XP-2364 aiškinamasis raštas [interaktyvus. Žiūrėta 2017 m. liepos 1 d.]. Prieiga per internetą: <<https://e-seimas.lrs.lt/portal/legalAct/lt/TAK/TAIS.300170?jfwid=-x5b15e0m3>>.

20. Baker & McKenzie. Appointment of a Data Protection Officer („DPO”) (Summary), 2017.

21. Alkonas. Žodynas internete [interaktyvus. Žiūrėta 2017 m. liepos 1 d.]. Prieiga per internetą: <<http://www.alkonas.lt/>>.

DATA PROTECTION OFFICER: REGULATORY FRAMEWORK UNDER THE EU GENERAL DATA PROTECTION REGULATION

Julius Zaleskis

S u m m a r y

The new EU General Data Protection Regulation sets forth a body of rules on a data protection officer, as a matter of a significant novelty, however, provides for uncertainty regarding content thereof. The article reveals new developments of the regulation on data protection officers, the content of grounds for appointment of the data protection officer, defines principles upon which the regulation of activities of the data protection officer are based.

Systematic analysis of the General Data Protection Regulation allows one to predict that the institution of the data protection officer will take the central position within the new legal framework. This prediction is based on the newly established principle of accountability requiring data controllers to take greater responsibility for data protection compliance, formulation of regulatory requirements in an abstract way that requires for expert competence from data controllers in interpreting and implementing such requirements and a requirement for such a competence imposed to the data protection officer.

The provisions of the General Data Protection Regulation providing for grounds for obligatory appointment of the data protection officer can be assessed critically due to lack of legal certainty.

In order data controllers and data processors (besides public authorities and bodies) would be obligated to appoint the data protection officer, three accumulative conditions should be met: (1) the condition of a higher risk activity (meaning that the data controller or the data processor engages in processing of special categories of data or data relating to criminal convictions and offences); (2) the condition of activity scale (meaning that the said data processing should take place on a large scale); and (3) the condition of main activities (meaning that the core activities of the controller or the processor consist of the said data processing).

Analysis of the General Data Protection Regulation reveals that the regulation of data protection officer's activities is based not on detail requirements imposing particular type of conduct, but on principles of more general nature. One can distinguish such principles of data protection officer's activities as expert competence, independence, avoidance of a conflict of interests, accessibility, freedom of a form of the activities.

Iteikta 2017 m. liepos 9 d.

Priimta publikuoti 2017 m. liepos 31 d.