KAUNO TECHNOLOGIJOS UNIVERSITETAS

SOCIALINIŲ, HUMANITARINIŲ MOKSLŲ IR FAKULTETAS

Agnė Vitartaitė

ASMENS DUOMENŲ APSAUGOS UŽTIKRINIMAS TEIKIANT ADMINISTRACINES PASLAUGAS: LIETUVOS SAVIVALDYBIŲ ATVEJIS

Baigiamasis magistro projektas

Vadovė

Doc. dr. Eglė Gaulė

KAUNAS, 2018

KAUNO TECHNOLOGIJOS UNIVERSITETAS

SOCIALINIŲ, HUMANITARINIŲ MOKSLŲ IR MENŲ FAKULTETAS

ASMENS DUOMENŲ APSAUGOS UŽTIKRINIMAS TEIKIANT ADMINISTRACINES PASLAUGAS: LIETUVOS SAVIVALDYBIŲ ATVEJIS

Baigiamasis magistro projektas

Viešasis administravimas (kodas 621N70001)

Vadovas

(parašas) Doc. dr. Eglė Gaulė

(data)

Recenzentas

(parašas) Doc. dr. Algis Junevičius

(data)

Projektą atliko

(parašas) Agnė Vitartaitė

(data)

KAUNAS, 2018

KAUNO TECHNOLOGIJOS UNIVERSITETAS

Socialinių, humanitarinių mokslų ir menų

(Fakultetas)

Agnė Vitartaitė

(Studento vardas, pavardė)

Viešasis administravimas, III kursas

(Studijų programa, kursas)

Baigiamojo projekto „Asmens duomenų apsaugos užtikrinimas teikiant administracines paslaugas: Lietuvos savivaldybių atvejis“

AKADEMINIO SĄŽININGUMO DEKLARACIJA

20 18 m. Sausio 9 d.

Kaunas

Patvirtinu, kad mano, **Agnės Vitartaitės**, baigiamasis projektas tema „Asmens duomenų apsaugos užtikrinimas teikiant administracines paslaugas: Lietuvos savivaldybių atvejis“ yra parašytas visiškai savarankiškai ir visi pateikti duomenys ar tyrimų rezultatai yra teisingi ir gauti sąžiningai. Šiame darbe nei viena dalis nėra plagijuota nuo jokių spausdintinių ar internetinių šaltinių, visos kitų šaltinių tiesioginės ir netiesioginės citatos nurodytos literatūros nuorodose. Įstatymų nenumatytų piniginių sumų už šį darbą niekam nesu mokėjęs.

Aš suprantu, kad išaiškėjus nesąžiningumo faktui, man bus taikomos nuobaudos, remiantis Kauno technologijos universitete galiojančia tvarka.

(vardą ir pavardę įrašyti ranka) *(parašas)*

Vitartaitė, Agnė. *Ensuring Protection of Personal Data in Administrative Services Delivery: Case Study of Lithuanian Municipalities*: Master's thesis in Public Administration / supervisor assoc. prof. Eglė Gaulė. The Faculty of Social Sciences, Arts and Humanities, Kaunas University of Technology.

Research area and field: 03 S

Key words: personal data, data protection, privacy, administrative service, municipalities.

Kaunas, 2018. 70 p.

SUMMARY

The project analyzes one of the basic human rights – the protection of personal data and its assurance while providing administrative services in the municipalities of Lithuania. Public sector collects data on residents in large scales. The aim of the project is to examine on the basis of analysis of Lithuanian municipalities' case how personal data protection is ensured while providing administrative services. The following objectives have been raised in order to achieve the set aim: to base the necessity of personal data protection in the context of cyber security and to analyze international legal regulation of personal data protection; to base the necessity of personal data protection and to identify the means of personal data protection applicable in the processes of public administration (especially while providing administrative services); to analyze legal regulation of personal data protection and to identify the means of personal data protection applied while providing administrative services in Lithuania; to analyze the situation of personal data protection while providing administrative services in the municipalities of Lithuania. The recent technological development is visible in public sector as well. Municipalities optimize administrative processes and create metadata, and increasingly transfer administrative services to electronic space. The problem of this thesis - how personal data protection is assured while providing administrative services within municipalities of Lithuania. The present thesis has revealed that this process is not smooth enough. Informants have identified systemic mistakes that not only reduce consumer confidence in the services provided, but also raise concerns about the security of personal data. Although the number of incidents in the public sector is significantly lower than in the private sector, the data in the public sector are particularly sensitive, and it is therefore necessary to create a safe environment that reduces the risk posed by cyber incidents. The first part of the project analyzes the necessity of assurance of personal data protection, it presents international regulation of personal data protection. The second part analyzes legal acts that ensure personal data protection in Lithuania. It analyzes the role of Lithuanian institutions while ensuring personal data protection. On the 25th of May 2018 General Data Protection Regulation will start being applied, which already now makes a very big influence on public institutions in the area of personal data protection. Personal data protection will be regulated even tighter, and institutions will start having officers working in the area of personal data protection. Thus the issue of personal data protection will

be more and more often solved not only in public management institutions but also it will be discussed in the society as well. However, there is a lack of comprehensive researches in the field of personal data protection in Lithuania. Most of researches that have been carried out are no longer relevant because of changes in the external environment, use of new technological opportunities, renewal of the legal basis. This project reveals the situation of personal data assurance in public sector, its problems and the gaps of provision of administrative services. The project used the following research methods: analysis of scientific literature, comparative analysis, analysis of legislation. Semi-structured interview method and content analysis were used to carry out the research.

TURINYS

PAVEIKSLĖLIŲ SĄRAŠAS

LENTENTELIŲ SĄRAŠAS

PAGRINDINĖS SĄVOKOS

Asmens duomenys – bet kuri informacija, susijusi su fiziniu asmeniu – duomenų subjektu, kurio tapatybė yra žinoma arba gali būti tiesiogiai ar netiesiogiai nustatyta pasinaudojant tokiais duomenimis kaip asmens kodas, vienas arba keli asmeniui būdingi fizinio, fiziologinio, psichologinio, ekonominio, kultūrinio ar socialinio pobūdžio požymiai (Asmens duomenų teisinės apsaugos įstatymas, 1996).

Duomenų tvarkytojas – juridinis ar fizinis (kuris nėra duomenų valdytojo darbuotojas) asmuo, duomenų valdytojo įgaliotas tvarkyti asmens duomenis. Duomenų tvarkytojas ir (arba) jo skyrimo tvarka gali būti nustatyti įstatymuose ar kituose teisės aktuose (Asmens duomenų teisinės apsaugos įstatymas, 1996).

Duomenų valdytojas – juridinis ar fizinis asmuo, kuris vienas arba drauge su kitais nustato asmens duomenų tvarkymo tikslus ir priemones. Jeigu duomenų tvarkymo tikslus nustato įstatymai ar kiti teisės aktai, duomenų valdytojas ir (arba) jo skyrimo tvarka gali būti nustatyti tuose įstatymuose ar kituose teisės aktuose (Asmens duomenų teisinės apsaugos įstatymas, 1996).

Duomenų tvarkymas – bet kuris su asmens duomenimis atliekamas veiksmas: rinkimas, užrašymas, kaupimas, saugojimas, klasifikavimas, grupavimas, jungimas, keitimas (papildymas ar taisymas), teikimas, paskelbimas, naudojimas, loginės ir (arba) aritmetinės operacijos, paieška, skleidimas, naikinimas ar kitoks veiksmas arba veiksmų rinkinys (Asmens duomenų teisinės apsaugos įstatymas, 1996).

Didieji duomenys - tai iš masinio įvairių duomenų srauto technologijų pagalba išgaunami didelę vertę turintys duomenys (Gantz, Reinsel, 2012).

Administracinė paslauga – viešojo administravimo subjekto veiksmai, apimantys leidimų, licencijų ar dokumentų, kuriais patvirtinamas tam tikras juridinis faktas, išdavimą, asmenų deklaracijų priėmimą ir tvarkymą, asmenų konsultavimą viešojo administravimo subjekto kompetencijos klausimais, įstatymų nustatytos viešojo administravimo subjekto informacijos teikimą asmenims, administracinės procedūros vykdymą (Viešojo administravimo įstatymas, 2006).

ĮVADAS

Asmens duomenų apsauga yra viena iš pamatinių žmogaus teisių. Duomenys yra neatsiejama įvairių gyvenimo sričių dalis. Žmonės naudojasi vis didesniais skaitmeninių duomenų kiekiais, todėl asmens privatumas, ypač atsižvelgiant į jų asmeninius duomenis, kelia vis didesnį susirūpinimą. Asmens duomenų teisiniame reguliavime trūksta nuoseklumo, tai kelia sunkumų teisės aktų leidėjams, mokslo bendruomenei bei paslaugų tiekėjams. Duomenys, kaip elementai, gali būti transformuojami į informaciją, o apdorojant informaciją, kuriamos žinios. Jei duomenys sisteminami, klasifikuojami ir transformuojami į informaciją, tokiu atveju gali iškilti grėsmė asmens privatumui.

Didėjant informacijos kiekiams ir srautams organizacijos priverstos priimti optimalius sprendimus ir aktyviai reaguoti į aplinkos pokyčius. Informacinės technologijos suteikia visuomenei daugiau lankstumo ir patogumo įvairiose situacijose, tačiau informacija yra generuojama skaitmeninėje terpėje. Dabar mes galime prisijungti prie savo paskyrų, sukurtų internetinėse svetainėse, mokėti mokesčius bei gauti kitas administracines paslaugas. Duomenų skaitmenizacija pagreitina tradicinius administravimo, paslaugų suteikimo bei informacijos apsikeitimo būdus. Nepaisant geografinių ribų, organizacijos, institucijos, viešosios įstaigos gali greitai ir efektyviai komunikuoti vidinių kanalų dėka. Informacinės technologijos įtakoja paslaugų kokybę, optimizuojami informaciniai srautai, didinamas operatyvumas, pagreitinamas problemų sprendimas. Todėl vienas svarbiausių veiksnių organizacijose – procesų valdymo optimalumo užtikrinimas, nuo kurio priklauso organizacijos veiklos rezultatų kokybė.

Lietuvos savivaldybių administracijose yra kaupiama ir saugojama informacija apie savivaldybės gyventojams suteikiamas paslaugas. Šiuo metu vis daugiau Lietuvos savivaldybių teikiamų administracinių paslaugų yra perkeliama į elektroninę erdvę. Suteikiant gyventojams galimybę gauti reikiamas paslaugas elektroniniu būdu, būtina užtikrinti pateiktų duomenų saugumą. Tačiau beveik pusė savivaldybėse teikiamų administracinių paslaugų yra teikiama ne elektroniniu būdu, kurioms institucijos naudoja vidinius tinklus, dokumentų valdymo sistemas, kurios taip pat gali būti kibernetinių atakų objektas.

Technologijos, atnešdamos naudą, patogumą, praktiškumą, neša ir grėsmę. Kibernetinės atakos vyksta nuolat, viešojoje erdvėje galima išgirsti vis daugiau pranešimų apie kibernetinės erdvės pažeidimus, svarbių valstybės institucijų internetinių svetainių sutrikimus ir kt. Tai, kad elektroninė erdvė gali būti pažeista galėjome įsitikinti per pastarųjų metų incidentus (SODRA, INFOSTATYBA), todėl svarbu ne tik kas yra daroma įvykus tokiai atakai, bet ir kokios saugumo priemonės yra taikomos siekiant užkirsti joms kelią visuose viešojo valdymo lygiuose. Nors asmens duomenų apsaugos klausimas vis dažniau sprendžiamas ne tik viešojo valdymo institucijose, bet ir aptariamas

visuomenėje. Tačiau visapusiškų tyrimų Lietuvoje asmens duomenų apsaugos srityje trūksta. Dauguma atliktų tyrimų, dėl pasikeitusios išorinės aplinkos, naujų technologinių galimybių panaudojimo, teisinės bazės atsinaujinimo yra nebeaktualūs.

Darbo objektas – asmens duomenų užtikrinimas teikiant administracines paslaugas.

Tikslas – atlikus Lietuvos savivaldybių atvejo analizę, išanalizuoti, kaip yra užtikrinama asmens duomenų apsauga, teikiant administracines paslaugas.

Problema: kaip užtikrinama asmens duomenų apsauga teikiant administracines paslaugas Lietuvos savivaldybėse?

Uždaviniai:

1. pagrįsti asmens duomenų apsaugos poreikį kibernetinio saugumo kontekste ir išanalizuoti tarptautinį asmens duomenų apsaugos teisinį reguliavimą;
2. pagrįsti asmens duomenų apsaugos užtikrinimo poreikį ir identifikuoti asmens duomenų apsaugos priemones taikytinas viešojo administravimo procesuose (ypač teikiant administracines paslaugas);
3. išanalizuoti asmens duomenų apsaugos teisinį reguliavimą ir nustatyti administracinių paslaugų teikime taikomas asmens duomenų apsaugos priemones Lietuvoje;
4. ištirti asmens duomenų apsaugos priemonių taikymo administracinių paslaugų teikime Lietuvos savivaldybėse situaciją.

Darbo metodai: mokslinės literatūros analizė, lyginamoji analizė, teisės aktų analizė. Tyrimui atlikti buvo pasitelktas pusiau struktūrizuotas interviu metodas, atlikta turinio analizė.

1. ASMENS DUOMENŲ APSAUGOS POREIKIO ANALIZĖ KIBERNETINIO SAUGUMO GRĖSMIŲ KONTEKSTE

Šiame skyriuje pateikiamas asmens duomenų apsaugos poreikis. Sparti informacinių technologijų pažanga leido surenkamų ir generuojamų duomenų kiekį sparčiai padidinti visame pasaulyje, todėl asmens duomenų apsaugos užtikrinimas įgijo dar svarbesnę reikšmę. Supratus galimas grėsmes žmonių saugumui ši sritis buvo pradėta reguliuoti tarptautiniu lygiu. Kaip tai vyko skirtinguose pasaulio regionuose pateikiama antrame skyrelyje. Galiausiai analizuojamas asmens duomenų panaudojimas viešajame sektoriuje.

1.1. Asmens duomenų apsaugos užtikrinimo poreikis

Skaitmeniniai duomenys generuojami kiekvieną sekundę. Pagal tradicinę koncepciją skaitmeniniai duomenys yra neatsiejama visuomenės dalis. Socialiniai tinklai, mokyklos, ligoninės, teisėsaugos agentūros, pramogų ir kino organizacijos, vyriausybinės įstaigos, mažos ir didelės įmonės, tyrimų bendrovės renka, kaupia ir generuoja duomenis. Anot Jastiugino (2011, p. 7), „informacijos saugumo problematika sena kaip pati informacija, informacijos saugumo aktualumas išryškėjo atsiradus poreikiui saugoti, perduoti ir kitaip tvarkyti informaciją“. Tačiau būtina pažymėti tai, kad duomenų ir informacijos sąvokos negali būti sutapatinamos. Pasak Zinso (2007) duomenys tampa informacija tik tada, kai juos gauna žmogus, jei jie apima tai, kas anksčiau nebuvo žinoma gavėjui. Taigi duomenys yra „žaliava”, kuri duomenų apdorojimo procese paverčiama informacija. Todėl informacija šiame darbe bus suprantama kaip duomenys, kurie yra susisteminti ir reikšmingi juos gaunančiam asmeniui.

Nagrinėjant asmens duomenų apsaugos poreikio kilmę, ją galima susieti su teisės į privatumą atsiradimu. Pirmosios teisės į privatumą koncepcijos pradėjo formuotis XIX a. pab. Jungtinėse Amerikos Valstijose (JAV) pripažįstant individualizmo principą kaip vieną iš pagrindinių žmogaus teisių (Malinauskaitė, 2015). 1890 m. teisininkai Louisas Brandeisas ir Samuelis Warrenas priėjo prie teisės į privatumą koncepcijos, kurią aprašė žymiame darbe „The right to privacy“. Jame pažymima, kad privatumas – tai teisė būti vienam, teisė kontroliuoti asmeninę informaciją ir laisvė nuo priežiūros (Agarwal, 2005). Žiobienės (2015, p. 34) teigimu „šis straipsnis turėjo įtakos ne tik šimtams bylų sprendimų, bet ir suformulavo teisės į privatumą doktriną (...) privatumas traktuotas kaip absoliuti, prigimtinė, neatimama teisė“.

Ilgainiui privatumo koncepcija vystėsi. 1960 metais Williamas Prosseris išskyrė keturis pagrindinius privatumo interesus (Malinauskaitė, 2015):

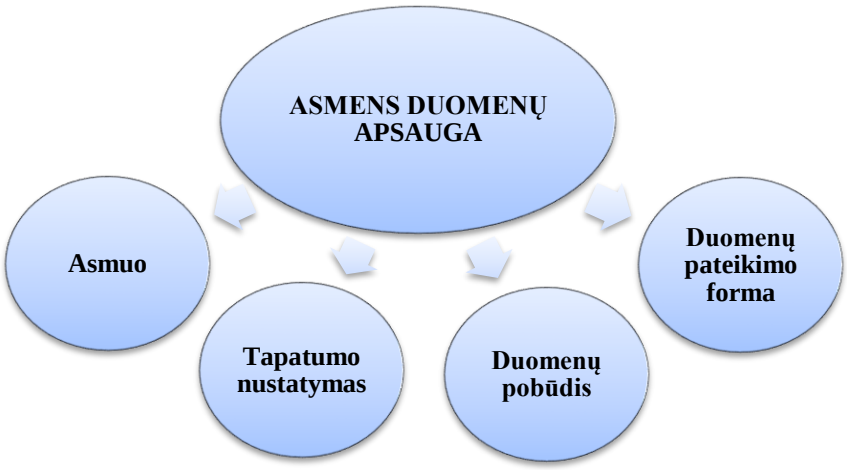
1. įsiveržimas į asmens pasitraukimą ar vienatvę, arba į jo asmeninius reikalus;

2. gėdingų asmeninių faktų apie individą viešas atskleidimas;
3. asmens viešas šmeižimas visuomenės akyse;
4. informacijos apie asmenį panaudojimas siekiant pranašumo.

Kaip matoma, privatumo interesai gali būti skirtingi, tačiau pagrindinis aspektas – kaip informacija apie asmenį bus pateikiama visuomenei. Anot Lankausko (2007) autoriai atkreipė dėmesį į privataus gyvenimo apsaugos būtinybę, bet kartu ir pripažino, jog ši teisė nėra absoliuti ir gali būti ribojama viešo intereso naudai. 1966 m. buvo priimtas Tarptautinis pilietinių ir politinių teisių paktas, kuriame buvo nurodyta, kad „niekas neturi patirti savavališko ar neteisėto kišimosi į jo asmeninį ir šeimyninį gyvenimą, jo būsto neliečiamybę, susirašinėjimo slaptumą, neteisėto kėsinimosi į jo garbę ir orumą“. Petraitytė (2010, p. 165) teigia, kad „garantuojant asmens teisę į privatų gyvenimą, kartu garantuojama ir jo asmens duomenų apsauga, o kita vertus – užtikrinant asmens duomenų apsaugą yra saugomas ir asmens privatus gyvenimas“.

XX a. pab. teisės į privatumą koncepcija pradėjo kisti ir įgavo naują reikšmę. Nuo 1990 metų daugelyje organizacijų išryškėjo didėjanti rizika, susijusi su duomenų rinkimu ir tvarkymu. Telekomunikacijų, informacinių technologijų, sveikatos apsaugos, vartotojų apsaugos srityse dirbančios organizacijos pradėjo vystyti privatumo apsaugos rizikos valdymą (Malinauskaitė, 2015).

XXI a. naujų ir jau esamų technologijų dėka visuomenės privatumas, atsižvelgiant į jų asmeninius duomenis, vis dažniau kelia susirūpinimą. „Globalus elektroninės erdvės pobūdis ir specifinės jos savybės leidžia teisės pažeidėjams veikti gana saugioje aplinkoje, nukreipti savo veiksmus bet kuria linkme ir veikti bet kurioje vietoje, veikas atlikti labai plačiu mastu, visiškai nepaisant valstybių sienų ir jurisdikcijos“ (Štitilis, Pakutinskas, Laurinaitis ir Dauparaitė, 2011, p. 155). Žmonės sąveikauja su vis plačiau teikiamomis elektroninėmis paslaugomis ir ši sąveika nėra taip gerai kontroliuojama bei užtikrinama, kaip tuo norėtų tikėti vartotojai. Individuali asmeninė informacija tampa prieinama visiems žmonėms (pvz., nusikaltėliams), įmonėms (pvz., „Google“) ir vyriausybinėms įstaigoms. Teisinėje sistemoje asmens duomenų sąvoka apibrėžiama kaip informacija, susijusi su fiziniu asmeniu, kurio tapatybė yra nustatyta arba kurio tapatybę galima nustatyti. Petraitytė (2010, p. 165) teigia, kad „informaciją apie fizinį asmenį (vardas, pavardė, gyvenamoji vieta, išsilavinimas, narystė vienoje ar kitoje organizacijoje, įsitikinimai ir pan.) įprasta vadinti asmens duomenimis“. Tačiau asmens duomenų sąvoka yra sudėtingesnė. Toliau bus aiškinami pagrindiniai asmens duomenų apsaugos koncepciją sudarantys aspektai (1 pav.).



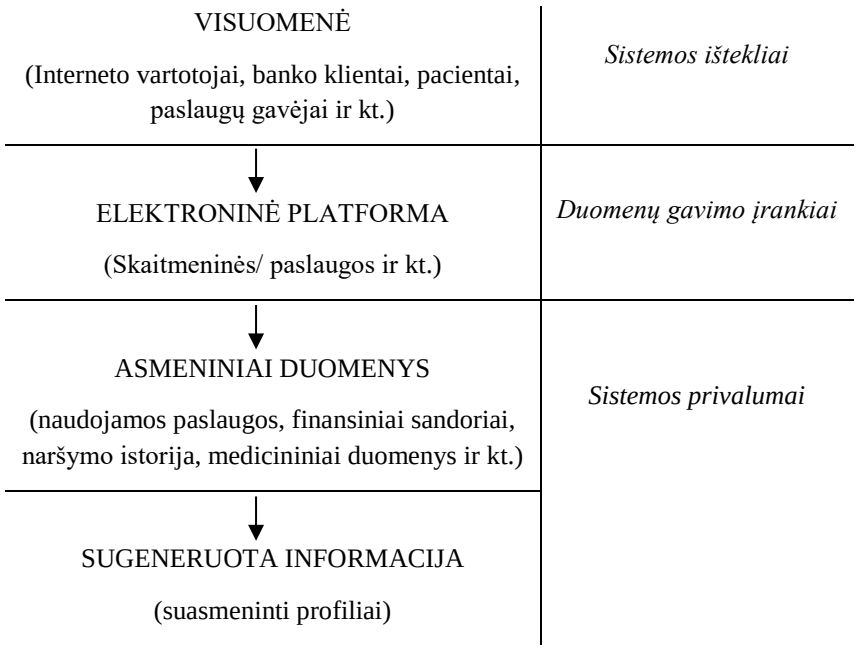
1 pav. Pagrindiniai asmens duomenų sąvokos aspektai (sudaryta autorės remiantis Europos duomenų apsaugos teisiniu vadovu)

Jau buvo akcentuota, kad asmens duomenų apsauga yra tapatinama su privataus gyvenimo gerbimu, kurio pagrindinė ašis – žmogus. Todėl duomenų apsauga visų pirma naudojasi fiziniai asmenys. Tapatybei nustatyti reikalingi elementai, kuriuose asmuo aprašomas taip, kad jį galima atskirti nuo visų kitų asmenų ir atpažinti kaip konkretų asmenį. Asmens vardas ir pavardė yra pagrindinis tokio aprašymo elemento pavyzdys. Kadangi dauguma vardų ir pavardžių nėra unikalūs, nustatant asmens tapatybę gali prireikti papildomų žymenų, kurie padėtų nesupainioti asmens su kuriuo nors kitu asmeniu. Teigiama, kad asmens tapatybę galima nustatyti, jeigu informacijoje yra susijusių duomenų, kuriais remiantis galima tiesiogiai arba netiesiogiai nustatyti asmens tapatybę. Išmaniųjų technologijų amžiuje asmenų tapatybei nustatyti vis dažniau naudojami biometriniai duomenys, pvz., pirštų atspaudai, skaitmeninės nuotraukos arba akies rainelės atvaizdo duomenys. Kitas svarbus asmens duomenų sąvokos aspektas – duomenų pobūdis. Duomenys gali būti susiję su asmenimis, jeigu tai atsispindi informacijos turinyje (pvz., informacija apie objektą arba įvykį taip pat turi būti laikoma asmens duomenimis). Pagal pateikimo pobūdį asmens duomenys gali būti pateikiami rašytiniuose arba žodiniuose pranešimuose, atvaizduose (apsauginių vaizdo stebėjimo sistemų įrašai), elektroninėje informacijos laikmenoje (Europos duomenų apsaugos teisinis vadovas, 2014, p. 35-41).

Spartūs pokyčiai informacinių technologijų srityje leido į asmeninius duomenis pažvelgti dar plačiau, dėl to atsirado naujas terminas „didieji duomenys“ (ang. *big data*). Dideli duomenys – tai paskelbti vaizdai socialiniuose tinkluose, jutiklių rodmenys, GPS signalai iš išmaniųjų telefonų, kurie dabar teikia milžiniškus duomenų srautus, susietus su žmonėmis, jų atliekama veikla ir vietovėmis. Organizacijos naudodamos informacijos analizės ir duomenų valdymo priemones gauna išsamią informaciją apie vartotojų elgseną. Tai paprasta formulė: naudojant „didžiuosius duomenis“ galima geriau prognozuoti, o geresnės prognozės leidžia priimti geresnius sprendimus (McAfee, Brynjolfsson,

& Davenport, 2012). Informacijos apie vartotojus rinkimas tapo el. verslo dalimi. Apsilankymas interneto svetainėje kompiuterio naudotojo duomenis (pvz., IP adresas, nustatyta kalba, laiko zona, programinė įranga, slapukai ir kt.) siunčia kelioms skirtingose valstybėse veikiančioms rinkodaros, reklamos ir kita veikla besiverčiančioms bendrovėms (Civilka ir Šlapimaitė, 2015, p. 128). Tačiau ne tik verslas suinteresuotas duomenų rinkimu. Išskiriamos kelios „didžiųjų duomenų“ taikymo sritys: E. prekyba ir rinkos informacija; E. valdžia ir politika; E. sveikata ir gerovė; visuomenės saugumo sritis (Chen, Chiang & Storey, 2012).

Renkami duomenys nuolat auga „visos šiuolaikinės vidutinės ir didelės įmonės personalo duomenų sistemoms, bazėms kurti, administruoti ir planuoti naudoja kompiuterizuotas asmens duomenų kaupimo, perdavimo ir pan. sistemas“ (Civilka, 2001, p. 6). Pasak vienos technologinių tyrimų įmonės viceprezidento Stepheno Goldo, per pastaruosius metus buvo sukurta 90 proc. visų duomenų. „Didžiuosius duomenis“ jis prilygina tokiems ištekliams kaip kuras, teigdamas, jei duomenys nebus analizuojami, tai jie neturės didelės vertės, tačiau duomenis apdorojant ir analizuojant naujais būdais, rezultatas tampa unikalus (Uddin & Gupta, 2014). McDermott‘as (2017) teigia, kad „Snowden“ duomenų skandalas parodė, kokio masto duomenų stebėjimai vyksta, to neįtariant patiems duomenų valdytojams. Toliau pateikiama asmens duomenų kaip sistemos išteklių schema (2 pav.). Schemoje pavaizduota, kaip asmens (visuomenės) duomenys gali būti veikiami ir apdorojami pasitelkiant informacines technologijas.

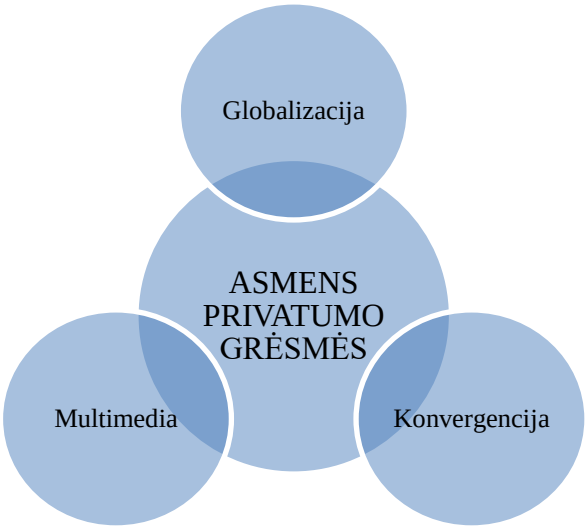


2 pav. Asmens duomenų srauto ir išteklių sistema (sudaryta autorės remiantis Purtova, 2015)

Visuomenė yra šios išteklių sistemos esmė. Užsiimant įprasta veikla galima pateikti informaciją, kuri pasakoja tam tikrus faktus: kas mes esame, ką mes darome ir kas mums patinka. Iki šiuolaikinių duomenų apdorojimo technologijų paplitimo, vienintelis būdas sužinoti faktus apie žmones buvo

stebėjimas, apklausa žodžiu ir raštu bei šių šaltinių analizavimas. Šiuo metu egzistuoja daugybė elektroninių platformų. Įrenginiai ir programinė įranga atlieka už mus stebėjimą, įrašymą ir išvadų formavimą. Daugelio Europos šalių piliečių judėjimas užfiksuojamas milijardais vaizdo stebėjimo kamerų, interneto vartotojų elgesys internete yra stebimas slapukais. Atsižvelgiant į didelę ekonominę asmens duomenų vertę, daugelis verslo modelių grindžiami elektroninių platformų asmens duomenų surinkimu. Visi su asmenimis susiję duomenys yra saugomi duomenų saugyklose, kuriose vėliau analizuojami, prireikus gali pateikti išsamią informaciją apie mus, pvz., personalizuotus profilius, pagrįstus anksčiau gautais duomenimis. Kadangi elektroninių platformų naudojimas tampa įprastu reiškiniu, asmeninių duomenų „bankai“ tampa vis išsamesni ir sudėtingesni, o kitų žinios apie mus tampa vis tobulesnės ir visapusiškesnės (Purtova, 2015).

Asmens duomenų koncepcija lyginant su jos ištakomis ir teise į privatumą stipriai keitėsi. To priežastis – išorinės aplinkos pokyčiai. Paveikslėlyje (3 pav.) pateiktos pagrindinės grėsmės asmens duomenims.



3 pav. Grėsmių asmens privatumui šaltiniai (sudaryta autorės remiantis Civilka, 2001).

Anot Civilkos (2001), didžiausią grėsmę asmens duomenų saugumui kelia globalizacija, konvergencija ir multimedija. Internetas yra geriausias stiprėjančios globalizacijos pavyzdys. Internetinėje erdvėje dingsta geografiniai suvaržymai, valstybių sienos. Laisvai judėti gali ir su fiziniais asmenimis susiję duomenys. Veikiant konvergencijai yra eliminuojami technologiniai barjerai tarp sistemų, kadangi sistemos yra tarpusavyje suderinamos. Galiausiai multimedia – sumaišo ir sujungia kelias asmeninės informacijos perdavimo formas ir tokiu būdu informacija, surinkta vienoje formoje, gali būti lengvai išversta/performatuota į kitą (Civilka, 2001, p. 10 – 11).

Apibendrinant galima teigti, kad asmens duomenų apsauga yra specifinė sritis, kuri yra stipriai veikiama išorinės aplinkos pokyčių. Kaip seniau buvo suteikta teisė į asmens privatumą, taip šiais

laikais atsiranda būtinybė užtikrinti asmens duomenų apsaugą. Sparti technologinė pažanga, beribė internetinė erdvė šią užduotį dar labiau sunkina. Asmeniniai duomenys įgauna visiškai naują reikšmę, kadangi esamos technologijos jau leidžia iš masinio duomenų srauto sugeneruoti atitinkamą informaciją, kuri suinteresuotoms šalims neša ekonominę naudą. Galima teigti, kad ateinančiais metais asmens duomenys įgis dar didesnę reikšmę.

1.2. Tarptautinis asmens duomenų apsaugos reguliavimas

Prieš pradedant aptarti teisės aktus reglamentuojančius asmens duomenų apsaugą, būtina paminėti tai, kad ilgą laiką ES teisėje nebuvo dokumento, kuris užtikrintų visapusišką asmens duomenų apsaugą. Visuotinė žmogaus teisių deklaracija (1948) yra vienas pirmųjų tarptautinių teisinių dokumentų, kuriame ginama žmogaus teisės į privatumą. 12 straipsnyje teigiama, kad niekas neturi patirti savavališko kišimosi į jo privatumą, šeimos gyvenimą, buitį ar susirašinėjimą arba kėsinimosi į jo garbę ir reputaciją. Svarbu atsižvelgti į tai, kad Visuotinės žmogaus teisių deklaracijos paskelbimas turėjo didelės įtakos tolesniam žmogaus teisių apsaugos vystymuisi visame pasaulyje. Jau 1950 m. buvo priimta Europos žmogaus teisių ir pagrindinių laisvių konvencija (EŽTK), kurioje teigiama, kad kiekvienas turi teisę į tai, kad būtų gerbiamas jo asmeninis ir jo šeimos gyvenimas, buto neliečiamybė ir susirašinėjimo slaptumas. EŽTK pagrindu vyko žmogaus teisių gynyba Europos regione. Dokumentą yra pasiraišusios ir ratifikavusios visos keturiasdešimt septynios Europos tarybos valstybės narės. Pirmasis nacionaliniu lygiu asmens duomenų apsaugą reglamentuojantis teisės aktas buvo priimtas Švedijoje 1973 metais, vėliau asmens duomenų apsaugos sritį reglamentuojantį įstatymą priėmė Prancūzija (1978 m.). Tačiau tarptautiniu lygiu nebuvo nei vieno dokumento, kuris apibrėžtų asmens duomenų ar informacijos privatumo sąvokas (Europos duomenų apsaugos teisinis vadovas, 2014).

Europos Tarybos Konvencija „Dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu“ (1981) tai pirmoji tarptautinė priemonė, kuri, įpareigoja apsaugoti asmenį nuo piktnaudžiavimo renkant ir tvarkant asmens duomenis. Šiame dokumente jau aiškiai apibrėžiama asmens duomenų, duomenų valdytojo ir kitos susijusios sąvokos. Būtina paminėti, kad Konvencijos nuostatos veikė tik Europos Bendrijos šalių teritorijose ir kiti regionai, kaip JAV, Australija ar Azija tuo metu dar neturėjo privatumą reguliuojančių teisės aktų. Kaip teigia Točickienė (2003, p. 117) buvo tikimasi, kad Europos Bendrijos valstybės narės gana greitai ratifikuos Europos Tarybos konvenciją, (...) tačiau iš visų tuometinių valstybių narių tik Prancūzija ir Vokietija pateisino šiuos lūkesčius.

Kibernetinė erdvė neturi sienų, dėl savo universalumo visoje privatumo politikoje ir skirtingų tarptautinių ir regioninių teisinių dokumentų, duomenų apsaugos įstatymus dažniausiai lemia nacionaliniai parlamentai. Kadangi, ankščiau minėti dokumentai yra rekomenduojamojo pobūdžio,

todėl išryškėjo asmens duomenų apsaugos teisinio reglamentavimo skirtumai nacionaliniais lygmenimis. 1995 metais, siekiant pašalinti laisvo duomenų judėjimo kliūtis ir nepakenkti duomenų saugumui, buvo priimta direktyva „Dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo“ (toliau – *Duomenų apsaugos direktyva*), harmonizuojanti nacionalinius teisės aktus šioje srityje. Tai svarbus dokumentas, kuris turėjo užtikrinanti lygiavertę asmens duomenų apsaugą ES ribose. Pasak Točickienės (2003) duomenų apsaugos direktyva iškėlė du pagrindinius tikslus: apsaugoti pagrindines žmogaus laisves ir teises, susijusias su asmens privačiu gyvenimu ir nevaržyti laisvo asmens duomenų judėjimo tarp ES valstybių narių.

Nors duomenų apsaugos direktyvos tikslas buvo užtikrinti lygiavertį duomenų apsaugos lygį ES, buvo pastebimas didelis skirtumas, kaip jos nuostatos buvo taikomos atskirose ES valstybėse narėse (Pearce, 2017). Pavyzdžiui Jungtinėje Karalystėje ir Airijoje duomenų apsauga laikoma privatumo teisės dalimi, nes teismai atsisako taikyti duomenų apsaugos teisės aktus situacijose, kai teisė į privatumą nėra įtraukta. Vokietijos Konstitucinis Teismas yra konstatavęs, kad duomenų apsaugos teisės kyla iš asmens teisės į "informacinį apsisprendimą" ir priešingai nei Jungtinė Karalystė ir Airija – nesusieja asmens duomenų apsaugos taisyklių su teise į privatumą (Lynskey, 2014).

Įsigaliojus duomenų apsaugos direktyvai (1995) taip pat atsirado kliūčių duomenų perdavimui į trečiąsias šalis. 60 straipsnyje nurodoma, kad duomenys į trečiąsias šalis, visais atvejais perduodami griežtai laikantis pagal šią direktyvą valstybių narių priimtų nuostatų. Pagrindinis reikalavimas yra tas, kad trečioji šalis užtikrintų tinkamą ES valstybių narių piliečių asmens duomenų apsaugą. Anot Agarwal (2005) apsaugos lygio „tinkamumo“ vertinamas atsižvelgia į visas duomenų perdavimo aplinkybes: duomenų pobūdį, siūlomos tvarkymo operacijos tikslą ir trukmę, šalį, taip pat trečiojoje šalyje galiojančias bendrąsias teisės normas bei saugumo priemones, kurių laikomasi toje šalyje.

JAV taikomas kitoks požiūris į privatumą nei Europos Sąjungoje, čia vyrauja sektorinis pobūdis, grindžiamas visuotinio federalinio teisės akto ir savireguliacijos. Įstatymo, kuris aiškiai reglamentuotų asmens duomenų apsaugą šioje šalyje nebuvo. Atsižvelgiant į šiuos skirtumus, daugelis JAV organizacijų išreiškė susirūpinimą dėl ES reikalaujamo „tinkamumo standarto“ poveikio asmens duomenų perdavimui iš Europos Sąjungos į JAV. Valstybės pastebėjo, kad ekonominis interesas išlaikyti minimalias kliūtis prekybai ir informacijos judėjimui gali kelti grėsmę nacionalinėms normoms. Transatlantinis ginčas dėl asmens duomenų privatumo, buvo kritinis atvejis, kuris iššaukė globalizacijos klausimo nagrinėjimą. Po beveik dvejų metų derybų buvo pasiektas kompromisas, vadinamas saugaus uosto (ang. *safe harbour*) susitarimu (Long & Quek, 2011). Siekdamas sumažinti asmens duomenų perdavimo neapibrėžtumą, JAV Prekybos departamentas išleido principus, skatinančius plėtoti tarptautinę prekybą. Principai buvo parengti konsultuojantis su pramonės atstovais ir visuomene, siekiant palengvinti prekybą tarp Jungtinių Amerikos Valstijų ir Europos Sąjungos.

Taisyklės skirtos JAV organizacijoms, gaunančioms duomenis iš Europos Sąjungos asmens, norint įgyti teisę į saugųjį uostą (Agarwal, 2005). Nuo 2016 m. rugpjūčio 21 d. saugųjį uostą pakeitė privatumo skydo programa. Sprendimu „Dėl ES ir JAV „privatumo skydo“ užtikrinamos apsaugos tinkamumo“ pripažįstama, kad ES ir JAV privatumo skydas, kurį sudaro sertifikuotoms JAV organizacijoms (įmonėms) taikomi privatumo principai ir JAV komercijos departamento bei įvairių kitų JAV institucijų prisiimti susiję įsipareigojimai, užtikrina tinkamą apsaugos lygį asmens duomenims, kuriuos tokios organizacijos gauna iš ES. Tai reiškia, kad asmens duomenis galima laisvai perduoti JAV esančioms organizacijoms, kurios yra įtrauktos į „privatumo skydo sąrašą“. Šį sąrašą tvarko ir viešai skelbia JAV komercijos departamentas.

Duomenų apsaugos direktyva (1995) turėjo išspręsti tuo metu kilusias problemas susijusias su asmens duomenų apsaugos užtikrinimu. Tačiau po jos priėmimo pasaulyje vyko spartūs technologiniai pokyčiai, kurių nebuvo galima numatyti. Internetinė erdvė tapo vientisa ir jokios sienos čia neegzistavo, šie pokyčiai lėmė, kad teisinė duomenų apsaugos bazė smarkiai atsiliko. Lentelėje (1 lentelė) pateikiama kaip po Duomenų apsaugos direktyvos priėmimo, ES toliau reagavo į informacinių technologijų pokyčius pasaulyje.

1 lentelė. Asmens duomenų apsaugos reguliavimo teisiniai pokyčiai

Nr.	Priėmimo data	Dokumento pavadinimas	Priėmusi institucija
1.	1997 m. gruodžio 15 d	Direktyva 97/66/EB dėl asmens duomenų apdorojimo ir privatumo apsaugos telekomunikacijų sektoriuje	Europos Parlamentas ir Taryba
2.	2002 m. liepos 12 d.	Direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje	Europos Parlamentas ir Taryba
3.	2006 m. kovo 15 d.	Direktyva 2006/24/EB dėl duomenų, generuojamų arba tvarkomų teikiant viešai prieinamas elektroninių ryšių paslaugas arba viešuosius ryšių tinklus, saugojimo	Europos Parlamentas ir Taryba
4.	2009 m. lapkričio 25 d.	Direktyva 2009/136/EB iš dalies keičianti tris direktyvas ir reglamentą Nr. 2006/2004 dėl nacionalinių institucijų, atsakingų už vartotojų apsaugos teisės aktų vykdymą	Europos Parlamentas ir Taryba
5.	2012 m. spalio 26 d.	Europos Sąjungos pagrindinių teisių chartija	Europos Komisija, Parlamentas, Taryba
6.	2016 m. balandžio 27 d.	Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 (Bendrasis duomenų apsaugos reglamentas)	Europos Parlamentas ir Taryba

1997 metais Europos Parlamentas ir Taryba išleido direktyvą 97/66/EB „Dėl asmens duomenų apdorojimo ir privatumo apsaugos telekomunikacijų sektoriuje“. Šia direktyva siekta, kad elektroninių ryšių paslaugų rinkoje ir technologijų raidos kontekste būtų užtikrinta asmens duomenų ir privatumo apsauga visiems elektroninių ryšių paslaugų vartotojams. Kintant išorinei aplinkai buvo siekiama

užtikrinti vienodą asmens duomenų ir privatumo apsaugos lygį visiems viešųjų elektroninių ryšių paslaugų naudotojams. Todėl direktyvoje 2002/58/EB „Dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje“ numatyta, kad asmens duomenų apsaugos pažeidimo ar pakenkimo asmens duomenims atveju paslaugų teikėjai apie pažeidimą informuotų kompetentingą nacionalinę duomenų apsaugos instituciją, o tam tikrais atvejais ir susijusius abonentus bei fizinius asmenis. Pagrindinis tikslas – adaptuoti ir atnaujinti buvusią direktyvą 97/66/EB, taip pritaikant prie technologinių realijų. Kaip matoma lentelėje (1 lentelė) ES nuosekliai vykdė teisinius pakeitimus reaguodama į išorinės aplinkos pokyčius. Direktyvos buvo papildytos ir iš dalies pakeistos dar ir 2006 ir 2009 metais. Kai 2012 m. buvo priimta Europos Sąjungos pagrindinių teisių chartija, asmens duomenų apsaugos reikalavimai tapo aiškiai suformuluoti.

Po keliasdešimt metų trukusių teisės aktų priėmimų siekiant visapusiškai užtikrinti asmens duomenų apsaugą, siekdama išvengti naujai kylančių grėsmių ES nusprendė iš esmės keisti asmens duomenų apsaugos reguliavimą. Šiuo reglamentu ES piliečiams sudaroma galimybė geriau kontroliuoti savo asmens duomenis. Juo taip pat atnaujinamos ir suvienodinamos taisyklės, leidžiančios įmonėms sumažinti biurokratizmą ir užsitikrinti didesnį vartotojų pasitikėjimą (4 pav.).

Nustatomas „vieno langelio“ principas	•Vadovaujanti priežiūros institucija yra vienintelė institucija, su kuria duomenų valdytojas arba duomenų tvarkytojas palaiko ryšius, kai jie vykdo tarpvalstybinį duomenų tvarkymą.
Išplėsta teritorinė Reglamento taikymo sritis	•Reglamentas taikomas kai ES esančių duomenų subjektų asmens duomenis tvarko ES neįsisteigęs duomenų valdytojas arba duomenų tvarkytojas ir jo veikla susijusi su prekių arba paslaugų siūlymu duomenų subjektams ES arba elgesio, kai jie veikia ES, stebėsena.
Pirmą kartą ES teisėje reglamentuojamas nepilnamečio iki 16 m. asmens duomenų tvarkymas	•Pažeidusiam Reglamento nuostatas, gali būti skiriamos administracinės baudos, priklausomai nuo Reglamento pažeidimo pobūdžio bauda gali siekti nuo 2 iki 4 proc. ankstesnių finansinių metų bendros metinės pasaulinės apyvartos, arba nuo 10 mln. iki 20 mln. EUR.
Įtvirtinamos naujos duomenų subjekto teisės	•Teisė į duomenų perkeliamumą (duomenų subjektas turės teisę gauti susijusius su juo asmens duomenis, kuriuos jis pateikė duomenų valdytojui susistemintu, įprastai naudojamu ir kompiuterio skaitomu formatu, ir persiųsti tuos duomenis kitam duomenų valdytojui) •Teisė būti pamirštam.
Įtvirtinamas duomenų subjektų atstovavimas	•Duomenų subjektas turi teisę įgalioti įstaigą ar organizaciją jo vardu pateikti skundą ir jo vardu naudotis jam tam tikromis Reglamente numatytomis teisėmis.
Asmens duomenų apsaugos pareigūnas	•Pagrindinės duomenų apsaugos pareigūnų užduotys yra duomenų valdytojo arba duomenų tvarkytojo informavimas apie jų prievoles, stebėjimas, kaip laikomasi Reglamento (ES) 2016/679 nuostatų, duomenų valdytojų, duomenų tvarkytojų, duomenų subjektų konsultavimas, bendradarbiavimas su priežiūros institucija.

4 pav. Pagrindinės ES duomenų apsaugos reformos kryptys (sudaryta autorės)

Reformą lėmė ryškūs išorinės aplinkos pokyčiai. 1995 m. kai buvo priimta Duomenų apsaugos direktyva, interneto vartotojų skaičius tesiekė 1 proc. Šiuo metu internetu naudojasi beveik 40 proc. visų pasaulio gyventojų (Interneto vartotojai pasaulyje, 2017). 2016 m. buvo priimtas Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 „Dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo“ (toliau – *Bendrasis duomenų apsaugos reglamentas*), kuriuo panaikinama Direktyva 95/46/EB. Būtinybę turėti visose ES valstybėse narėse vienodus ir atnaujintus asmens duomenų apsaugą reglamentuojančius teisės aktus paskatino siekis užtikrinti vieną iš pagrindinių žmogaus teisių – teisę į asmens duomenų apsaugą, sudaryti sąlygas skaitmeninės ekonomikos plėtrai ir sustiprinti kovą su nusikalstamumu ir terorizmu.

Šiuo metu plačiai pripažįstama, kad nereguliuojamas asmens duomenų apdorojimas turėjo didelės įtakos pagrindinėms žmogaus teisėms, tokioms kaip privatumas, orumas, vientisumas ir savarankiškumas. 2003 m. buvo pradėtas plėtoti Azijos ir Ramiojo vandenyno šalių privatumo standartas, kuris turėjo apimti Australiją, Kanadą, Kiniją, Honkongą, Japoniją, Korėją, Malaiziją, Naująją Zelandiją, Tailandą ir Jungtines Amerikos Valstijas. 2004 m. lapkričio mėn. buvo patvirtinta Azijos ir Ramiojo vandenyno šalių privatumo sistema ir įgyvendinimo mechanizmai, įskaitant mechanizmus, susijusius su tarpvalstybiniais duomenų srautais (Privacy and Human Rights Report, 2006). Nors kiti pasaulio regionai, priimdami duomenų apsaugos priemones, ėmėsi bendrų veiksmų, siekdami apsaugoti asmenų teises (pvz. ES), Afrika apskritai atsiliko. Globalizacija ir didėjanti valstybių tarpusavio priklausomybė paskatino sudaryti tarpregionines sutartis, reguliuojančius klausimus, kurie iki šiol nebuvo reglamentuojami pagal nacionalinę teisę (Abdulrauf & Fombad, 2016). Suvokiant šiandieninę informacijos galią, galimą jos rinkimo ir panaudojimo poveikį žmogaus pagrindinėms teisėms ir laisvėms, Afrikos lyderiai priėmė konvenciją „Dėl kibernetinio saugumo ir asmens duomenų apsaugos“ (2014). Pagrindinis konvencijos tikslas – sureguliuoti informacinių ryšių ir technologijų sektoriaus problemas, kylančias dėl didėjančios interneto prieigos ir kibernetinio nusikalstamumo lygio (Abdulrauf & Fombad, 2016). Per pastaruosius metus vis daugiau pasaulio valstybių priėmė arba ruošiasi priimti naujus teisės aktus susijusius su asmens duomenų apsauga. 2011 m. duomenų apsaugos įstatymus buvo priėmusios 76 šalys. 2015 m. su duomenų apsauga susiję įstatymai jau buvo priimti 109 šalyse (Greenleaf, 2015).

Apibendrinant galima teigti, kad ilgą laiką asmens duomenų apsauga neturėjo teisinio reguliavimo nei vienoje šalyje. Asmens teisę į privatumą konstatavo Europos žmogaus teisių ir pagrindinių laisvių konvencija. Tik nuo 1980 metų imtos taikyti tarptautinės priemonės. Galima teigti, kad Europa, skirtingai nei kiti žemynai asmens duomenų teisiniame reguliavime pažengė labiausiai. Kai 1995 m. duomenų apsaugos direktyvoje buvo numatyti reikalavimai užtikrinti asmens duomenų apsaugą perduodant duomenis į trečiąsias šalis, kilo daug nesusipratimų dėl „tinkamumo“ standarto.

Labiausiai tai palietė ES ir JAV santykius, kadangi šis reikalavimas daugybei organizacijų nešė finansinius nuostolius. Tuo pat metu išryškėjo ir globalizacijos proceso klausimai. Internetinė erdvė, buvo ta sritis, kuri panaikino geografinius atstumus ir tarpvalstybines sienas. Priimant duomenų apsaugos direktyvą nebuvo galima numatyti, koks spartus technologinis šuolis įvyks. Kad būtų užtikrinama visapusiška asmens duomenų apsauga, teisinę bazę, atsižvelgiant į šiuos pokyčius, teko nuolat atnaujinti. Tačiau tenka pripažinti, kad teisiniai veiksmai, beveik visais atvejais, atsiliko mažiausiai vienu žingsniu. Galiausiai buvo priimtas bendrasis duomenų apsaugos reglamentas, jo taikymas palies visų ES valstybių narių tiek viešąjį tiek privatų sektorius.

1.3. Asmens duomenų panaudojimas viešajame administravime

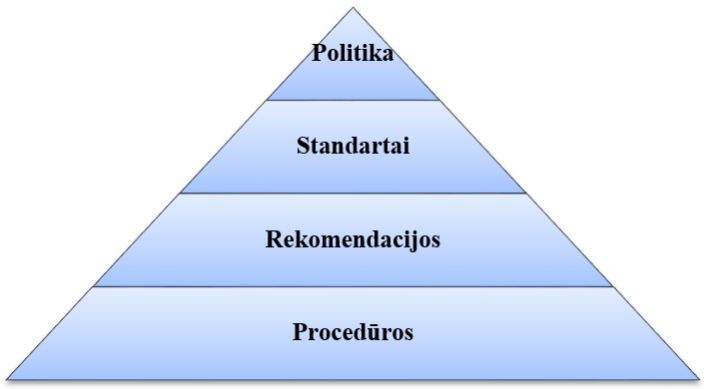
Tobulėjant informacinėms technologijoms kinta ir viešojo valdymo institucijų veiklos galimybės. Prieš technologinį šuolį visą svarbiausią informaciją įstaigos laikydavo ir saugodavo popieriniuose dokumentuose. Taip surinktų duomenų rūšiavimas, konkrečios informacijos ieškojimas reikalavo daug laiko sąnaudų. Šiuo metu informacijos apdorojimas ir saugojimas skaitmeniniu pavidalu leidžia greitai ir kokybiškai analizuoti duomenis bei laiku priimti atitinkamus sprendimus (Milė ir Junevičius, 2013). Visos įstaigos naudoja kompiuterizuotas personalo informacines sistemas, skirtas administraciniams ir planavimo tikslams. Ligoninės ir kitos sveikatos sektoriaus įstaigos saugo ir apdoroja pacientų duomenis. Mokyklų ir universitetų duomenų įrašų kontingentas – mokiniai ir studentai. Policija yra suinteresuota kaupti įtartina veikla užsiimančių asmenų pirštų atspaudus, genetinio patikrinimo duomenis bei kontroliuojamus informacinių ryšių ir telekomunikacijų duomenis. Mokesčių inspekcijos renka mokesčius pagal gyventojų gaunamas pajamas, šeimos statusą ar asmenų vykdomą verslo veiklą. Taigi, galima įžvelgti tendenciją, kad asmens duomenys yra neatsiejama viešojo administravimo dalis.

Anot Valackienės ir Trofimovo (2015) moksliniuose šaltiniuose dažniausiai viešasis sektorius yra suvokiamas kaip viešojo administravimo, viešosios politikos, viešojo valdymo sinonimas. Pasak Gaulės (2014, p. 374) „valstybę galima suvokti kaip sudėtingų sąveikų ir procesų bei valdymo tinklų visumą o viešąjį valdymą – kaip struktūras ir procesus, kuriuos naudodama valdžia priima sprendimus ir naudoja išteklius siekdama valdyti visuomenę ir ekonomiką“. Tačiau kaip ir kitus sektorius, viešasis administravimas, kaip valstybinės politikos įgyvendinimo sritis, yra veikiamas globalizacijos procesų. Dėl globalizacijos įtakos kokybiškai kintant atskirų šalių viešojo administravimo sistemoms, galimas valdžios institucijų modelių ir veiklos būdų supanašėjimas (Domarkas ir Masionytė, 2015, p. 16).

Markausko (2015) tvirtinimu, vertinant asmens duomenų apsaugą, viešasis sektorius yra labiau pažengęs ir labiau išvystęs šios srities apsaugos politiką nei privatus. Galima daryti prielaidą, kad pagrindinė viešojo sektoriaus pažangos asmens duomenų apsaugoje priežastis yra ta, kad viešasis

sektorius įgyvendina asmens duomenų apsaugos politiką nacionaliniu lygiu, o privatus sektorius – ją tik vykdo. Tačiau duomenų apsauga ir jos saugumo užtikrinimas yra ta sritis, kurioje viešojo administravimo institucijos turi rodyti pavyzdį privačiam sektoriui, kaip tinkamai taikyti ir laikytis pagrindinių duomenų apsaugos principų. Tačiau nėra argumentų, kurie paprastai ir vienareikšmiškai apibrėžtų, informacinių technologijų įtaką viešajam administravimui. Anot Barcevičiaus (2008, p. 85) tai yra besivystanti sritis, todėl jai dar labai trūksta nusistovėjusių terminų, analizės modelių.

Šiuo metu jau galima įžvelgti tendencijas, kad ryšys tarp technologijų plėtros ir institucinių pokyčių turi potencialą pakeisti iki šiol objektyviomis ir nekintamomis laikytas viešojo sektoriaus organizacijų savybes – fizinio atstumo ir laiko sąnaudų klausimus. Tai galimai turėjo įtakos duomenų perdavimo mastų išaugimui (Barcevičius, 2008). Tačiau keičiasi ne tik viešojo administravimo modeliai, bet ir pati informacija, jos surinkimo ir valdymo būdai. Veiklos procese viešojo sektoriaus institucijos renka, kuria ir kaupia informaciją, kurią sudaro statistiniai duomenys, teisės aktai ir teismų praktikos dokumentai, taip pat palydoviniai vaizdai ir žemėlapiai, patentų registrai ir kt. Viešojo sektoriaus sukurti ir surinkti duomenys tapo vienu iš didžiausių informacijos šaltinių Europoje (Petrauskas ir Selskaite, 2009, p. 91). Informacijos saugumo priemonių taikymas suteikia institucijoms tikrumo dėl saugumo tikslų ir uždavinių nustatymo, administracinių procedūrų įgyvendinimo ir kontrolės, taikomų informacijos saugumo technologijų patikimumo ir suderinamumo su kitomis organizacijomis.



5 pav. Informacijos saugumo valdymo dokumentų hierarchija (Jastiuginas, 2011, p. 16).

Paveikslėlyje (žr. 5 pav.) pateikiama informacijos saugumo valdymo dokumentų hierarchija. Pirmiausia institucijos informacijos saugumo politiką nusakančiame dokumente aprašomi bendrieji saugumo principai, įvardijama saugoma informacija ir ištekliai, nustatomi saugumo prioritetai. Informacijos saugumo politika įgyvendinama standartais, procedūromis, rekomendacijomis ir kitais žemesniojo valdymo lygio dokumentais, kurių paskirtis, sąryšiai ir nuorodos į juos taip pat išdėstomi informacijos saugumo politikos dokumente (Jastiuginas, 2011, p. 16-17).

Kadangi viešasis sektorius tarnauja visuomenei, todėl su asmenimis susijusių duomenų generavimo mastai yra didesni nei privačiajame sektoriuje. Komisijos komunikate „Dėl Europos sąveikumo sistemos įgyvendinimo strategijos“ (2017) teigiama, kad šiuo metu viešojo administravimo institucijos, taikydamos skirtingus duomenų tvarkymo metodus, tvarko didžiulius kiekius skirtingų formatų duomenų, saugo daug jų kopijų daugybėje skirtingų saugyklų ir dažnai skelbia juos įvairiuose Europos portaluose nederindamos jų turinio ir pateikimo būdo. Todėl jau turimą informaciją apie piliečius ir įmones jos pakartotinai panaudoja tik 48 proc. atvejų. 2017 m. Europos Parlamento rezoliucijoje „Dėl 2016–2020 m. ES e. valdžios veiksmų plano“ yra pabrėžiama atvirųjų duomenų svarba. Rezoliucijoje sakoma, kad tam tikra viešojo sektoriaus informacija gali būti naudojama pakartotinai, tačiau būtina taikyti griežtas duomenų apsaugos priemones, sumažinant neteisėtų veiksmų grėsmę. Atkreipiamas dėmesys į skaitmeninių viešųjų paslaugų visuotinės prieigos svarbą, manoma, kad iki 2020 m. viešojo administravimo institucijos taps atviros ir integralios.

Tarp organizacinės sistemos siekia padidinti informacijos vertę, kurios daugelyje vyriausybinių agentūrų valdo informacijos integravimo į organizacijos bei technologijų tobulinimo potencialą, leidžiant geriau pasiekti ir naudoti pateikiamą informaciją. Sėkminga tarp organizacinių informacinių sistemų plėtra stipriai priklauso nuo tarpvalstybinių duomenų mainų. Moksliniai tyrimai orientuojasi informacijos dalijimąsi, siekiant plėtoti tarp organizacines informacines sistemas bei nagrinėja veiksnius, kurie yra būtini sėkmingam informacijos dalinimuisi. Šis aspektas, dalijimasis duomenimis, labai svarbus ir apima sudėtingą organizacinę sąveiką, ypač daugiapakopėse valstybinėse sistemose (Pardo, Cresswell, Thompson & Zhang, 2006). Anot Dawes, Cresswell & Pardo (2009) kalbant apie viešojo valdymo institucijų duomenų dalijimosi intensyvumą, galima išskirti trys lygius:

- vidinius organizacinius tinklus, kuriuose žinių mainai vyksta skirtinguose to paties vieneto padaliniuose;
- tarp organizacinius tinklus, kurie priklauso vienam valdymo organui;
- tarp organizacinius tinklus, kurie kertasi su kitais lygiais ar valstybiniais sektoriais.

Paprastai platūs ir įvairialypiai organizaciniai tinklai turi didesnes galimybes duomenų dalinimuisi, tačiau didesnis dalyvių skaičius ir įvairovė kelia didesnį pavojų duomenų apsaugai ir didina finansines sąnaudas. Petrausko ir Selskaitės (2009, p. 91) teigimu informacinė visuomenės vystymas iššaukia viešojo sektoriaus informacijos pakartotinio naudojimo poreikį, todėl ES lygmeniu daug dėmesio yra skiriama teisinės sistemos tobulinimui. Šiuo metu literatūroje yra išskiriami įvairūs elektroninės valdžios paslaugų pakopų modeliai, tačiau detaliau bus aptariamas dažniausiai naudojamas Hiller & Belanger modelis.

2 lentelė. Hiller & Belanger elektroninės valdžios paslaugų pakopų modelis (sudaryta pagal Limba 2009, p. 35)

	PAKOPOS				
	I	**II**	**III**	**IV**	**V**
Tipas	**Informacija**	**Dvipusė komunikacija**	**Transakcijos**	**Integracija**	**Politinis dalyvavimas**
Valdžia piliečiams	Informacija apie pašalpas Rinkimų datos	Individuali informacija apie pašalpas Balsavimo biuleteniai	Mokesčių mokėjimas Išmokų gavimas	Visos paslaugos	Balsavimas internetu
Valdžia verslui	Teisės aktai Pirkimų pasiūlymai	Pirkimų pasiūlymų tikslinimas	Mokesčių mokėjimas Investicijos ir mokėjimai	Visa teisinė informacija	Lobistinė veikla
Valdžia valdžiai	Vidaus tvarkos taisyklės	Savivaldybių informavimas el. būdu	Elektroninių fondų pervedimai	-	-

Pagal šį modelį pirmoje pakopoje viešojo administravimo institucija savo internetinėje svetainėje pateikia informaciją apie savo veiklą gyventojams, verslo subjektams, politikams ir pan. Taip pat prižiūri, kad aktuali ir naujausia informacija būtų viešai prieinama. Antrojoje pakopoje įsijungia tiesioginis dvišalis bendravimas, kuomet asmuo pateikia užklausą valstybės tarnautojui, (pvz. el. paštu), o šis savo atsakymą (prireikus ir kitus duomenis, dokumentus) siunčia interesantui. Šioje pakopoje svarbiausia tai, kad išvengiama tiesioginio kreipimosi į viešojo administravimo instituciją, (pvz. savivaldybę), o asmuo, kuris pateikia užklausą ir valstybės tarnautojas bendrauja elektroniniu būdu. Transakcijų lygmenyje galimi tokie veiksmai kaip socialinių išmokų ir kompensacijų gavimas nuo prašymo pateikimo internetu iki bankinės lėšų pervedimo operacijos. Ketvirtoje pakopoje reikalinga tarp institucinė sistemų integracija, nes el. valdžios paslaugos pasiekiamos vienuose interneto vartuose ir vieninteliu prisijungimu. Kol kas nėra teikiama daug paslaugų priskiriamų penktai pakopai. Tačiau politinio dalyvavimo, nereikia tiesiogiai suprasti kaip rinkimų įgyvendinimo elektroninėje erdvėje. Šiuo atveju politinis dalyvavimo aspektas siejamas su galimybe gyventojui ar verslo ūkio subjektui pareikšti nuomonę dėl tam tikrų institucijoje priimamų valdymo sprendimų ir jų svarbos. Valstybės tarnautojo pareiga – priimant sprendimus atsižvelgti į šias internete pareikštas nuomones (Limba, 2009). Taigi, kiekvienoje pakopa pasižymi vis didesniu interaktyvumo lygiu. Pirmoji ir antroji pakopos reikalauja mažiausiai interaktyvumo, tačiau teikiant viešąsias paslaugas aukštesnėse pakopose jau yra reikalingas asmens tapatybės nuskaitymas. Tačiau nebūtina visas viešąsias paslaugas teikti aukščiausiu lygmeniu. Anot Milės ir Junevičiaus (2013, p. 462) „viešojo sektoriaus institucijos turi stengtis aukščiausiu lygmeniu teikti tas paslaugas, kurios piliečiams yra aktualiausios ir svarbiausios. Kitaip tariant, teikiant e. paslaugas svarbu ne perkelti šias paslaugas į elektroninę erdvę, o siekti plataus jų naudojimo“. Taigi, gerai suprojektuotos ir įgyvendintos informacinės sistemos gali supaprastinti duomenų valdymą, tobulinti informacinę infrastruktūrą, palengvinti integruotų paslaugų teikimą ir sustiprinti bendradarbiaujančių organizacijų tarpusavio

ryšius. Projektuojant ir įgyvendinant naujus įrankius, plėtojant bei tvarkant naujas strategines sritis tai reikalauja tikslių bei išsamių ir gerai ištirtų šių sričių žinių.

Apibendrinant skyrių galima teigti, kad per pastaruosius metus stipriai išaugęs interneto vartotojų skaičius bei sparti informacinių technologijų pažanga lėmė sukuriamų skaitmeninių duomenų didėjimą. Todėl asmens duomenų apsauga ėmė kelti vis didesnį susirūpinimą tiek viešojo valdymo institucijose, tiek visuomenėje. Išanalizavus tarptautinį asmens duomenų reguliavimą, paaiškėjo, kad tuose regionuose, kuriuose asmens duomenų apsauga nebuvo pakankamai arba išvis nebuvo reguliuojama kibernetinio nusikalstamumo lygis buvo labai aukštas. Todėl dar labiau išaugo poreikis sureguliuoti informacinių ryšių ir technologijų sektoriuje kylančias asmens duomenų apsaugos užtikrinimo problemas. Tačiau asmens duomenų apsaugos teisiniame reguliavime vis dar trūksta nuoseklumo, tai kelia sunkumų teisės aktų leidėjams, mokslo bendruomenei bei paslaugų tiekėjams. Šiuo metu itin pabrėžiama atvirųjų duomenų svarba, pakartotinis viešojo sektoriaus informacijos naudojimas, viešojo administravimo institucijų integralumas, todėl svarbus 2018 m. gegužės 25 d. įsigaliosiantis Bendrasis duomenų apsaugos reglamentas, kuris turės įtakos visiems duomenų valdytojams ir tvarkytojams. Asmens duomenų apsauga bus dar griežčiau reguliuojama, o apsaugos užtikrinimo reikalavimai suvienodinti visoms ES institucijoms.

2. ASMENS DUOMENŲ APSAUGA VIEŠOJO ADMINISTRAVIMO PROCESUOSE LIETUVOJE

Šiame skyriuje analizuojama asmens duomenų teisinė aplinka Lietuvoje. Tinkama ir sureguliuota įstatyminė bazė yra svarbi asmens duomenų apsaugos užtikrinimui. Todėl buvo ištirta Lietuvos institucinė sąranga asmens duomenų apsaugos užtikrinimo srityje, atskirų institucijų funkcijos ir veiklos sritys. Galiausiai buvo identifikuoti asmens duomenų užtikrinimo reikalavimai teikiant administracines paslaugas Lietuvoje.

2.1. Teisinis asmens duomenų apsaugos reglamentavimas Lietuvoje

Nacionaliniu mastu, žmogaus privatumas yra ginamas Lietuvos Respublikos Konstitucijos. 22 straipsnyje teigiama, kad informacija apie privatų asmens gyvenimą gali būti renkama tik motyvuotu teismo sprendimu ir tik remiantis įstatymu, kad niekas nepatirtų savavališko ar neteisėto kišimosi į asmeninį ir šeimos gyvenimą, garbę ir orumą. Tai – ne vienintelis teisinis šaltinis ginantis žmogaus privatumo teisę. Lietuvos Respublikos civilinis kodeksas (2000) saugo ne tik privatumo teisę, bet ir kitas asmenines neturtines teises ir vertybes. Tačiau pagrindinis teisės aktas užtikrinantis asmens duomenų apsaugą Lietuvoje yra Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas (1996), kurio vienas pagrindinių tikslų yra: „ginti žmogaus privataus gyvenimo neliečiamumo teisę ryšium su asmens duomenų tvarkymu". Šis įstatymas reglamentuoja santykius, atsirandančius tvarkant asmeninius duomenis. Penktame straipsnyje nurodoma, kad asmens duomenys turi būti apdorojami laikantis įstatymo ir numatomi teisėto tvarkymo kriterijai. Tačiau informacinių technologijų sklaida, lėmė tai, kad priimti teisės aktai, pasikeitus išorinei aplinkai, tapo nebe veiksmingi. Didėjant duomenų srautui, su fiziniais asmenimis susijusius duomenis imta tvarkyti ir privačiajame sektoriuje. Anot Petraitytės (2011, p. 128), „buvo tvarkoma vis gausesnė ir įvairesnė informacija. Tapo reikalingos privačiam sektoriui tinkamos, taip pat lankstesnį informacijos apie fizinius asmenis tvarkymo reguliavimą nustatančios taisyklės". Reaguojant į šiuos pokyčius 1998 m. buvo priimtos Asmens duomenų teisinės apsaugos įstatymo pataisos, kuriose numatyta, kad tvarkant informaciją susijusią su fiziniais asmenimis bet kurioje informacinėje sistemoje turi būti taikomas įstatymas.

Per kelis paskutiniuosius XX a. metus informacijai apie fizinius asmenis tvarkyti skirtas teisinis reguliavimas itin sparčiai vystėsi, plėtojosi, atsižvelgdamas į visuomeninio gyvenimo pokyčius, taip pat tobulėjo, perimdamas Europos Sąjungos šalių patirtį ir laimėjimus šioje srityje. Teisinio reguliavimo raida nesustojo ir peržengus amžių sandūros slenkstį (Petraitytė, 2011, p. 128). Prieš 20 metų priimtas Asmens duomenų apsaugos įstatymas jau buvo pakeistas 10 kartų, iš jų 3 kartus šis įstatymas buvo keistas iš esmės, išleidžiant naują redakciją. Pagrindinis ir svarbiausias įstatymo tikslas

– numatyti šios srities bendrą situaciją ir bendruosius asmens duomenų apsaugos principus, kad būtų galimybė jais vadovautis atsiradus naujovių, apie kurias galbūt nė nebuvo susimąstyta anksčiau (Valstybinė duomenų apsaugos inspekcija, 2017).

Asmens duomenų apsaugos įstatymas nėra vienintelis teisės aktas reguliuojantis asmens duomenų tvarkymą. Asmens duomenų apsauga ir privataus gyvenimo užtikrinimas yra specifinė sritis, kuri persipina į kitus sektorius. Pavyzdžiui – informacinių technologijų, sveikatos apsaugos, visuomenės informavimo, švietimo ar net nacionalinio saugumo sektorius. Lietuvos Respublikos Konstitucinio Teismo jurisprudencijoje teigiama, kad „privatus žmogaus gyvenimas – tai individo asmeninis gyvenimas: gyvenimo būdas, šeimyninė padėtis, gyvenamoji aplinka, santykiai su kitais asmenimis, individo pažiūros, įsitikinimai, įpročiai, jo fizinė bei psichinė būklė, sveikata, garbė, orumas ir kt.“ (Kiškis, Petrauskas, Rotomskis ir Štitilis, 2006, p. 115). Kaip ši sąveika atsispindi Lietuvos Respublikos įstatyminėje bazėje pateikiama lentelėje.

3 lentelė. **Įstatymai susiję su asmens duomenų apsauga Lietuvoje (sudaryta autorės)**

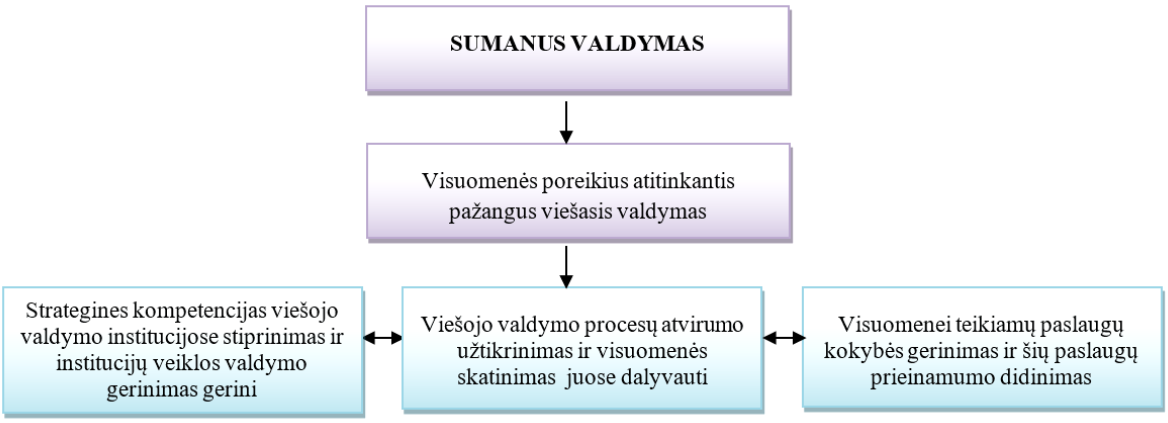
Priėmimo data	**Įstatymas**	**Kas jame sakoma**
1996 m. spalio 23 d.	Lietuvos Respublikos pacientų teisių ir žalos sveikatai atlyginimo įstatymas	Informacija apie paciento gyvenimo faktus gali būti renkama tik su paciento sutikimu, jei tai yra būtina ligai diagnozuoti, gydyti ar pacientui slaugyti. Sveikatos priežiūros įstaigose duomenys apie pacientą, atsižvelgiant į turinį ir naudojimo tvarką, turi būti užtikrinama paciento privataus gyvenimo apsauga.
2000 m. liepos 18 d.	Lietuvos Respublikos reklamos įstatymas	Reklama draudžiama jei joje, be fizinio asmens sutikimo minimas jo vardas, pavardė, pateikiama jo nuomonė, informacija apie jo privatų ar visuomeninį gyvenimą, turtą, naudojamas fizinio asmens atvaizdas.
2004 m. balandžio 15 d.	Lietuvos Respublikos elektroninių ryšių įstatymas	Viešųjų elektroninių ryšių paslaugų teikėjai privalo užtikrinti: 1) kad su asmens duomenimis galėtų susipažinti tik tokią teisę turintys paslaugų teikėjo įgalioti darbuotojai teisėtais tikslais; 2) tvarkomų asmens duomenų apsaugą nuo atsitiktinio arba neteisėto sunaikinimo, saugojimo, tvarkymo, susipažinimo ar atskleidimo.
2006 m. gegužės 25 d.	Lietuvos Respublikos informacinės visuomenės paslaugų įstatymas	Informacinės visuomenės paslaugų teikimo ir kitos paslaugų teikėjų veiklos reguliavimas yra grindžiamas asmens duomenų teisinės apsaugos principu. Elektroninio pristatymo paslaugos teikėjas privalo siuntėjui ir gavėjui garantuoti elektroninės siuntos turinio konfidencialumą ir susirašinėjimo slaptumą.
2006 m. rugsėjo 1 d.	Lietuvos Respublikos visuomenės informavimo įstatymas	Rengiant ir platinant viešąją informaciją, privaloma užtikrinti žmogaus teisę į privataus pobūdžio informacijos apsaugą. Informaciją apie privatų gyvenimą galima skelbti tik jei tas žmogus sutinka. Informacija apie viešojo asmens privatų gyvenimą gali būti skelbiama be jo sutikimo, jeigu ši informacija atskleidžia visuomeninę reikšmę turinčias privataus šio asmens gyvenimo aplinkybes ar asmenines savybes.

2011 m. balandžio 21 d.	Lietuvos Respublikos asmens duomenų, tvarkomų vykdant policijos ir teisminį bendradarbiavimą bylose, teisinės apsaugos įstatymas	Užtikrinti fizinių asmenų pagrindinių teisių, ypač teisės į privataus gyvenimo neliečiamumą ir teisės į asmens duomenų apsaugą, apsaugą tvarkant asmens duomenis vykdant policijos ir teisminį bendradarbiavimą baudžiamosiose bylose. Įstatymas reglamentuoja santykius, kurie atsiranda tvarkant asmens duomenis automatiniu būdu, taip pat neautomatiniu būdu tvarkant asmens duomenų susistemintas rinkmenas arba jų dalis.
2014 m. gruodžio 11 d.	Lietuvos Respublikos kibernetinio saugumo įstatymas	Šis įstatymas nustatytomis sąlygomis ir tvarka taikomas valstybės institucijoms, formuojančioms ir įgyvendinančioms kibernetinio saugumo politiką, viešojo administravimo subjektams, valdantiems ir tvarkantiems valstybės informacinius išteklius, ypatingos svarbos informacinės infrastruktūros valdytojams, viešųjų ryšių tinklų ir viešųjų elektroninių ryšių paslaugų teikėjams ir elektroninės informacijos paslaugų teikėjams, informacinių technologijų srityje veiklą vykdantiems verslo subjektams, mokslo ir studijų institucijoms.

Kaip matoma iš lentelėje pateiktų duomenų, asmens duomenų apsaugos teisinis reguliavimas yra įvairiapusis. Petraitytės teigimu (2011, p. 130) „tai išplėtota nevienodos teisinės galios susijusių teisės normų ir principų sistema. Ši sistema yra gyvybinga ir nuolat plečiasi, reaguodama į visuomeninio gyvenimo ir intereso tvarkyti informaciją apie fizinius asmenis pokyčius“. Nuo 2018 m. gegužės 25 d. Lietuvoje bus pradėtas taikyti Bendrasis duomenų apsaugos reglamentas. Anot Zaleskio (2017, p. 51) „efektyvų Bendrojo duomenų apsaugos reglamento taikymą Lietuvoje gali apsunkinti tai, kad Lietuvoje kol kas trūksta metodinės, aiškinamosios medžiagos, rekomendacijų, kaip turėtų būti suprantamos Bendrojo duomenų apsaugos reglamento naujovės ir kaip pasirengti jas įgyvendinti“. Kadangi šie pokyčiai palies ne tik valstybinį, bet ir privatų sektorių, būtina parengti rekomendacijas ir metodinę medžiagą, kad organizacijos lengviau galėtų prisitaikyti prie šių pasikeitimų.

Be ankščiau išvardintų teisės aktų, duomenų saugumo užtikrinimo svarba akcentuojama nacionalinio lygmens strateginiuose dokumentuose. Apie teisę į žmogaus privatumą kalbama septynioliktosios Lietuvos Respublikos vyriausybės programoje, kurioje numatoma vykdyti aktyvią žmogaus teisių švietimo politiką, siekiant veiksmingai ginti konstitucines teises, užtikrinančias asmens saugumą, privataus gyvenimo neliečiamumą. Taip pat numatoma stiprinti valstybės informacinius išteklius, duomenų saugą ir kibernetinį saugumą.

2014–2020 metų nacionalinės pažangos programoje (žr. 5 pav.) numatyta, kad efektyvus viešasis valdymas – svarbus šalies pažangą lemiantis veiksnys. Įgyvendinami pokyčiai viešajame valdyme turi padėti didinti visuomenės pasitikėjimą viešojo valdymo institucijomis bei užtikrinti šalies konkurencingumą. Anot Kiurienės (2014, p. 170) „į šalies pažangą orientuotas viešasis valdymas turi būti vystomas atsižvelgiant į visuomenės poreikius, esamą šalies viešojo valdymo situaciją ir sistemingai įgyvendinant viešojo sektoriaus inovacijas“. Pateiktame paveikslėlyje yra pavaizduota, kaip sumanus valdymas atsispindi nacionalinėje pažangos programoje.



6 pav. Sumanus valdymas 2014–2020 metų nacionalinės pažangos programoje (sudaryta autorės)

Įgyvendinant Informacinės visuomenės plėtros 2014–2020 metų programą 2015 m. buvo patvirtinta „Lietuvos Respublikos skaitmeninė darbotvarkė“. Joje teigiama, kad vis daugiau svarbių veiklų atliekama skaitmeninėje erdvėje, tačiau žmonės negeba internete elgtis saugiai, per mažai dėmesio skiria savo privatumo, duomenų, teisėtų interesų apsaugai. Programoje taip pat numatoma, kad saugios informacinių ryšių ir technologijų (IRT) infrastuktūros sukūrimas – būtina sąlyga, kad valstybė ir piliečiai galėtų sėkmingai naudotis IRT galimybėmis. Tam numatomos šios priemonės:

- plėtoti Valstybės informacinių išteklių sąveikumo platformą – užtikrinti e. paslaugų patogumą naudotojams, duomenų mainų efektyvumą, bendro naudojimo ir sudėtinių paslaugų teikimą;
- perkelti į skaitmeninę erdvę aktualias viešąsias ir administracines paslaugas ir tobulinti šių paslaugų teikimo procesą;
- naudojantis IRT kurti ir plėtoti elektroninių paslaugų, valstybės registrų ir informacinių sistemų tobulinimo sprendimus;
- plėtoti sąveikumo sprendinius e. valdžios, valstybės informacinių sistemų ir registrų srityse svarbos informacinės infrastruktūros ir valstybės informacinių išteklių kibernetinį saugumą.

Nors strateginiuose dokumentuose išskiriamas sumanios visuomenės prioritetas, IRT potencialo išnaudojamas, tačiau valstybės audito ataskaitoje (2013) teigiama, kad „asmens duomenų apsaugos būklė Lietuvoje paskutinį kartą išsamiai analizuota rengiant Duomenų apsaugos plėtojimo 2002–2004 m. programą ir ruošiantis narystei ES“. Vėliau buvo nagrinėtos tik atskiros asmens duomenų apsaugos sritys, bet kompleksinio vertinimo nebuvo 10 metų (Valstybės audito ataskaita, 2013).

Apibendrinant galima teigti, kad nacionaliniu lygiu aukščiausią galią turintis teisinis dokumentas, kuris gina žmogaus teisę į privatumą yra Lietuvos Respublikos Konstitucija. Kadangi Lietuva yra Europos Sąjungos valstybė narė, Lietuva privalo reaguoti į ES priimamus sprendimus, nutarimus ar išleidžiamas direktyvas. Asmens duomenų teisinės apsaugos įstatymas (1996) buvo priimtas reaguojant į ES direktyvą „Dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių

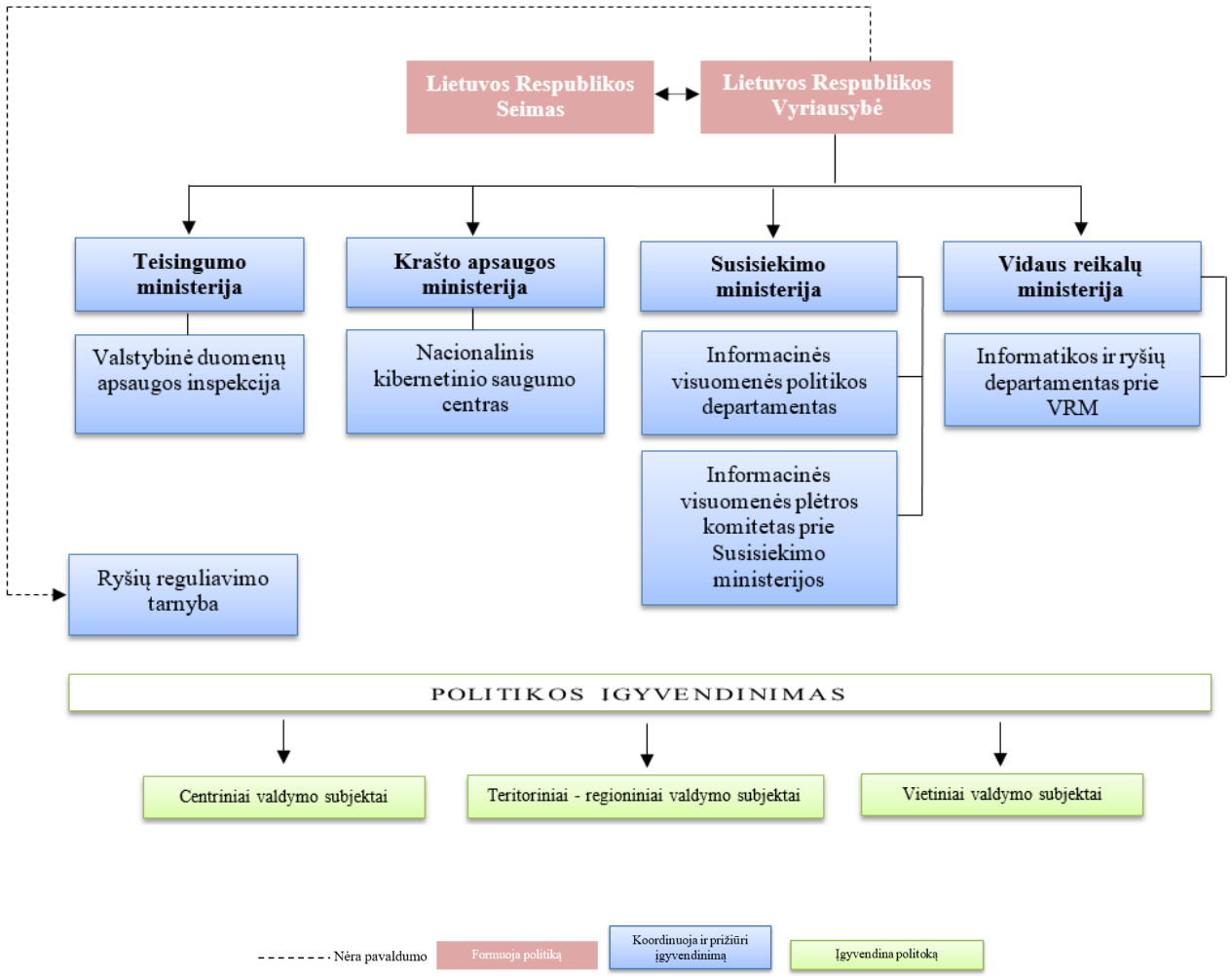
duomenų judėjimo“ (1995). Nors tuo metu, kai buvo priimtas asmens duomenų įstatymas Lietuva dar nepriklausė ES, šioje vietoje galima būtų įžvelgti tam tikrus pasiruošimo stoti į ES ženklus. Pastarasis įstatymas yra pagrindinis asmens duomenų apsaugą reglamentuojantis teisinis dokumentas Lietuvoje. Kadangi asmens duomenų apsauga yra plati sritis, tai bendrai atsispindi Lietuvos Respublikos įstatyminėje bazėje – reklamos, elektroninių ryšių, informacinės visuomenės paslaugų, kibernetinio saugumo įstatymuose. Nacionaliniuose strateginiuose dokumentuose, įvardijami sumanaus valdymo, sumanios visuomenės prioritetai, tai lemia, kad viešoje sektoriaus paslaugos persikelia į elektroninę erdvę. Todėl didėja asmens duomenų apsaugos užtikrinimo poreikis.

2.2. Viešojo valdymo institucijų vaidmuo užtikrinant duomenų apsaugą Lietuvoje

Su fiziniais asmenimis susijusius duomenis tvarko savivaldybės, kredito įstaigos, Valstybinė mokesčių inspekcija, policija, „Sodra“, švietimo bei sveikatos priežiūros įstaigos, ryšių ir telekomunikacijų bendrovės, bibliotekos ir kitos institucijos. Lietuvos Nacionalinis kibernetinio saugumo centras (toliau – *NKSC*) siekdamas įvertinti valstybės informacinių išteklių valdytojų požiūrį į naujai priimtus kibernetinį saugumą reglamentuojančius teisės aktus, vykdė elektroninę valstybinių įstaigų apklausą kibernetinio saugumo tema. Ši apklausa, išryškino rimtą problemą - įstaigos ignoruoja Lietuvos teisės aktų reikalavimus, juos mažai nagrinėja, netaiko veikloje ir net neplanuoja vyriausybės nustatytais terminais įgyvendinti nustatytų kibernetinio saugumo reikalavimų (NKSC metinė ataskaita, 2016).

Pagal Lietuvos Respublikos Konstituciją valstybės valdžią Lietuvoje vykdo Seimas, Respublikos Prezidentas ir Vyriausybė ir Teismas. Pateiktoje schemoje yra pavaizduotos institucijos, kurios yra susijusios su duomenų apsaugos formavimu, kontrole ir vykdymu Lietuvoje. Kaip aukščiausią galią, asmens duomenų apsaugos srityje turinčios institucijos yra pavaizduotas Seimas ir Vyriausybė. Seimas, pavaizduotoje schemoje atlieka įstatymo leidėjo funkciją, taip pat ratifikuoja tarptautines sutartis susijusias su asmens duomenimis. Kaip nurodyta Lietuvos Respublikos Konstitucijoje Vyriausybė tvarko krašto reikalus, saugo Lietuvos Respublikos teritorijos neliečiamybę, garantuoja valstybės saugumą ir viešąją tvarką, taip pat koordinuoja ministerijų ir kitų Vyriausybės įstaigų veiklą. Šiuo atveju Vyriausybė koordinuoja nepriklausomas institucijas, atsakingas už duomenų apsaugą Lietuvoje. Taip pat prižiūri, kaip įstatymų ir Vyriausybės nutarimų laikosi viešojo administravimo subjektai. Schemoje (žr. 7 pav.) išskirti centriniai (vyriausybinės įstaigos, įstaigos prie ministerijų), teritoriniai – regioniniai (centrinių valdžios institucijų teritorinės struktūros, apskričių viršininkų administracijos) ir

vietiniai viešojo administravimo subjektai (savivaldybės), kurie privalo įgyvendinti suformuotą asmens duomenų apsaugos politiką.



7 pav. Viešojo valdymo institucijų vaidmuo asmens duomenų apsaugoje (sudaryta autorės)

Valstybinė duomenų apsaugos inspekcija (toliau – *VDAI*) yra asmens duomenų apsaugos priežiūros institucija, kuri rūpinasi, kad būtų ginama žmogaus teisė į asmens duomenų ir privatumo apsaugą, tvarkant asmens duomenis profesiniais tikslais, kad asmens duomenų apsauga Lietuvoje atitiktų Europos Sąjungos teisinius reikalavimus ir būtų tinkamai užtikrinama informacinės visuomenės aplinkoje. VDAI yra atskaitinga teisingumo ministerijai, kuriai Asmens duomenų teisinės apsaugos įstatyme (1996, 35 str.) numatyta, formuoti valstybės politiką asmens duomenų apsaugos srityje, rengti įstatymų, reglamentuojančių asmens duomenų apsaugą, projektus, atlikti kituose teisės aktuose nustatytas funkcijas asmens duomenų apsaugos srityje. Asmens duomenų teisinės apsaugos įstatymo komentare (2005, p. 242) teigiama, kad VDAI kompetencijai priklauso asmens duomenų tvarkymo priežiūra ne tik valstybinėse institucijose, bet ir privačiose įmonėse. Ši nuostata padeda užtikrinti skaidrumą duomenų subjektams bei duomenų valdytojams, taip pat nekyla klausimų dėl to, į kurią instituciją kreiptis.

Šiuo metu VDAI atlieka šias funkcijas:

- padeda duomenų subjektams apginti teisę į duomenų apsaugą ir privatumą;
- padeda duomenų valdytojams tinkamai valdyti ir tvarkyti asmens duomenis;
- kontroliuoja asmens duomenų tvarkymo teisėtumą;
- rengia ir derina teisės aktus, užtikrinančius asmens duomenų ir privatumo apsaugą;
- vykdo tarptautinius įsipareigojimus asmens duomenų apsaugos srityje;
- didina visuomenės informuotumą asmens duomenų apsaugos klausimais.

Svarbu pažymėti ir tai, kad per 20 metų nuo VDAI įkūrimo, šios institucijos veiklos sritys išsiplėtė. Tam didelę įtaką turėjo Lietuvoje priimti įstatymai bei teisės aktų pakeitimai (pvz. Elektroninių ryšių įstatymo pakeitimas, Kibernetinio saugumo įstatymas), kuriuose buvo numatoma kompetencija VDAI, kurios iki tol nebuvo. VDAI veiklai ir funkcijoms įtakos turėjo ir 1.2. skyrelyje analizuotos ES priimtos direktyvos. Pavyzdžiui, Lietuvoje pradėjus taikyti direktyvą 2006/24/EB „Dėl duomenų, generuojamų arba tvarkomų teikiant viešai prieinamas elektroninių ryšių paslaugas arba viešuosius ryšių tinklus, saugojimo“ VDAI numatyta pareiga kaupti informaciją apie sunkius ir labai sunkius nusikaltimus tyrimo, atskleidimo ir baudžiamojo persekiojimo tikslais teikimą kompetentingoms institucijoms ir kasmet teikti šios informacijos pagrindu sukauptus statistinius duomenis Komisijai.

Lietuvos Respublikos ryšių reguliavimo tarnyba yra elektroninių ryšių, pašto paslaugos teikimo veiklą reguliuojanti, elektroninio parašo priežiūros institucijos funkcijas atliekanti savarankiška ir nepriklausomai veikianti valstybės įstaiga. Ryšių reguliavimo tarnyba bendradarbiauja su kompetentingomis valstybės institucijomis, tarp jų ir su Valstybine duomenų apsaugos inspekcija, kad būtų užtikrinta žmogaus privataus gyvenimo neliečiamumo teisė, kiek tai susiję su asmens duomenų tvarkymu. Taip pat rengia ir tvirtina informacijos, susijusios su Elektroninių ryšių įstatymo, Pašto įstatymo, Elektroninio parašo įstatymo, Nepilnamečių apsaugos nuo neigiamo viešosios informacijos poveikio įstatymo įgyvendinimu, skelbimo tvarką, apimtį ir sąlygas, atsižvelgdama į teisės normas, reglamentuojančias konfidencialios informacijos, įskaitant valstybės, tarnybos, komercinės paslapties ar apie fizinio asmens privatų gyvenimą, apsaugą, skelbia šią informaciją ir įstatymų nustatyta tvarka teikia turimą informaciją kitoms valstybės ir savivaldybių institucijoms jų prašymu (Ryšių reguliavimo tarnybos nuostatai, 2014).

Nacionalinis kibernetinio saugumo centras, pagal kompetenciją įgyvendindamas kibernetinio saugumo politiką ir vykdydamas valstybės informacinių išteklių ir ypatingos svarbos informacinių infrastruktūrų kibernetinių incidentų valdymo padalinio veiklą. NKC atlieka valstybės informacinių išteklių ir ypatingos svarbos informacinės infrastruktūros atitikties kibernetinio saugumo reikalavimams stebėseną, valdo kibernetinio saugumo informacinį tinklą, reaguoja į kibernetinius

incidentus valstybės informaciniuose ištekliuose. NKC turi teisę tvarkyti asmens duomenis, būtinus numatytoms funkcijoms kibernetinio saugumo užtikrinimo srityje atlikti (Kibernetinio saugumo įstatymas, 2014).

Lietuvos Respublikos susisiekimo ministerijos Informacinės visuomenės politikos departamentas dalyvauja formuojant elektroninio parašo naudojimo valstybės politiką, valstybės politiką elektroninių ryšių srityje, taip pat rengia ir teikia siūlymus dėl elektroninio parašo teisinio reglamentavimo, naudojimo plėtros ir priemonių tobulinimo srityse. Informacinės visuomenės plėtros komitetas prie Susisiekimo ministerijos dalyvauja formuojant valstybės informacinių išteklių politiką, atlieka valstybės informacinės visuomenės plėtros ir valstybės informacinių išteklių vertinimo ir kontrolės funkcijas (Informacinės visuomenės politikos departamento nuostatai, 2015).

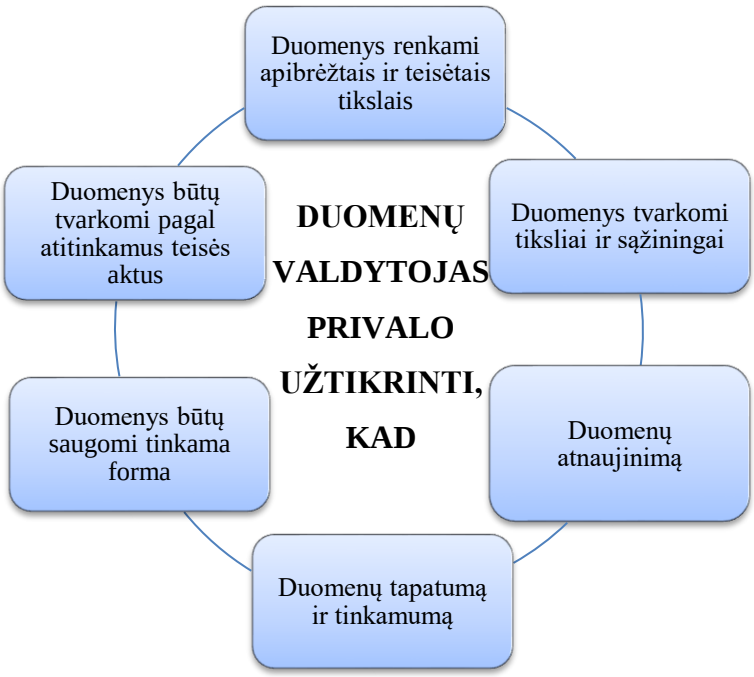
Informatikos ir ryšių departamentas prie Lietuvos Respublikos vidaus reikalų ministerijos (toliau – *Informatikos ir ryšių departamentas*) siekdamas efektyvaus ir patikimo vidaus reikalų srities valstybės informacinių sistemų, registrų bei tinklų veikimo, Informatikos ir ryšių departamentas kuria ir diegia saugias informacines ir ryšių technologijas (toliau – *IRT*) viešajam saugumui ir viešajam valdymui užtikrinti, nuosekliai inicijuoja ir įgyvendina projektus, susijusius su IRT plėtra bei sauga. Informatikos ir ryšių departamentas yra Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos tvarkytojas ir asmens duomenų tvarkytojas, taip pat vykdo valstybės informacinių išteklių atitikties nustatytiems elektroninės informacijos saugos reikalavimams stebėseną (Informatikos ir ryšių departamento nuostatai, 2017).

Kaip matoma iš pateiktos schemos ir institucijų aprašymų, su asmens duomenų apsauga yra susijusios kelios ministerijos – krašto apsaugos, susisiekimo ir vidaus reikalų. Krašto apsaugos ministerijai yra pavaldus NKSC, kurio veiklos sritys apima visą šalies kibernetinę erdvę, tuo pačiu ir elektroninius asmens duomenis. Susisiekimo ministerijai yra pavaldžios dvi institucijos – informacinės visuomenės politikos departamentas ir informacinės visuomenės plėtros komitetas. Analizuojant šių institucijų veiklos sritis, buvo galima įžvelgti nemažai panašumų. Šios institucijos dalyvauja formuojant ir įgyvendinant informacinių ryšių politiką, tiria elektroninio parašo plėtros galimybes. Vidaus reikalų ministerijai yra pavaldus informatikos ir ryšių departamentas prie VRM. Visi kiti centriniai, teritoriniai regioniniai ir vietiniai viešojo administravimo subjektai įgyvendina asmens duomenų apsaugos politiką. Išanalizavus viešojo valdymo institucinę sąrangą, būtina akcentuoti ir tai, kad vienintelė nepriklausoma institucija – tai Ryšių reguliavimo tarnyba, kuri nėra pavaldi jokiai ministerijai. Tiesa, Ryšių reguliavimo tarnyba turi pateikti finansines ataskaitas vyriausybei. Nors, kaip minėta 1.2. skyrelyje analizuojant tarptautinį asmens duomenų apsaugos reguliavimą, nacionalinė institucija, užtikrinanti asmens duomenų apsaugą, turi būti nepriklausoma. Šiuo atveju Teisingumo ministerija daro įtaką VDAI, kurios valdymo sričiai pastaroji yra priskirta.

2.3. Asmens duomenų apsaugos užtikrinimas viešojo administravimo procesuose Lietuvoje

Duomenų tvarkymas yra apibrėžiamas gana plačiai – bet kuris su asmens duomenimis atliekamas veiksmas: rinkimas, užrašymas, kaupimas, saugojimas, klasifikavimas, grupavimas, jungimas, keitimas (papildymas ar taisymas), teikimas, paskelbimas, naudojimas, loginės ir aritmetinės operacijos, paieška, skleidimas, naikinimas ar kitoks veiksmas arba veiksmų rinkinys (Asmens duomenų teisinės apsaugos įstatymas, 1996, 2 str.).

Sukūrus prieigą, kurioje vartotojas gali gauti el. paslaugas, būtina užtikrinti jo duomenų apsaugą, viso paslaugų teikimo proceso metu. Paveikslėlyje yra nurodyti asmens duomenų teisėto tvarkymo kriterijai, apibrėžti Asmens duomenų teisinės apsaugos įstatyme (1996).



8 pav. Asmens duomenų valdytojui keliami reikalavimai susiję su duomenų apsauga (Sudaryta autorės pagal Asmens duomenų teisinės apsaugos įstatymą, 1996).

Pirmiausia, jis turi užtikrinti, kad būtų apibrėžti asmens duomenų tvarkymo tikslai, renkamų ir profiliuojamų duomenų tinkamumą ir naudą, duomenų sunaikinimą per atitinkamą laikotarpį. Taip pat duomenų valdytojas turi užtikrinti, kad duomenų subjektai būtų informuoti ir galėtų pasinaudoti savo teisėmis (prieiga, taisymas, ištrynimas). Reikia įvertinti, ar į šias teises atsižvelgiama organizacijos lygmeniu ir ar šios teisės yra veiksmingos. Tvarkant asmeninius duomenis būtina laikytis paveikslėlyje (žr. 8 pav.) nurodytų kriterijų, tiesa jų laikomasi ne visuomet. Valstybės audito ataskaitoje (2013) nustatyta, kad dauguma (84 proc.) institucijų, kurios tvarko duomenis laikėsi ne visų teisės aktais nustatytų reikalavimų, susijusių su asmens duomenų apsauga. Petraitytės (2011, p. 168) teigimu,

tokios abstrakčios asmens duomenims tvarkyti keliamų reikalavimų formuluotės leidžia apimti platų su asmens duomenų tvarkymu susijusių veiksmų spektrą, neatsižvelgiant į asmens duomenų tvarkymo būdą (automatizuotas ar neautomatizuotas), duomenims tvarkyti naudojamas technologijas.

Rizikos šaltiniai, kurie gali pakenkti duomenų apsaugai: tai gali būti asmenys, priklausantys organizacijoms (kompiuterių specialistai), asmenys už organizacijos ribų (gavėjas, teikėjas, konkurentas, įgaliotoji trečioji šalis), šaltiniai, kurių neįtakoja žmogaus veikla (kompiuterinis virusas, stichinė nelaimė, degios medžiagos). Šie rizikos šaltiniai gali atsitiktinai arba sąmoningai pakenkti įvairiems informacinės sistemos komponentams bei materialiniam turtui. ENISA pateiktuose duomenyse (2016) teigiama, kad rizika gali apimti:

- įrenginius: kompiuteriai, ryšio priemonės, usb diskai, kietieji diskai.
- programinę įrangą: operacinės sistemos, pranešimai, duomenų bazės, kitos informacinės programos.
- tinklus: lokalūs, bevieliai, šviesolaidiniai.
- žmones: vartotojai, administratoriai, vadovai.
- dokumentų perdavimo kanalus: paštas, dokumentų valdymo sistemos, registrai.

Svarbu pabrėžti tai, kad rizikos šaltiniai geba išnaudoti sistemos pažeidžiamumą pasinaudodami savo įgūdžiais, turimu laiku, finansiniais ištekliais, sistemos prieinamumu, motyvacija, nebaudžiamumo jausmu. Administracines paslaugas teikiančios institucijos vadovaujasi „Bendraisiais reikalavimais organizacinėms ir techninėms asmens duomenų saugumo priemonėms“. Jose nurodoma, kad atsižvelgiant į saugotinų asmens duomenų pobūdį ir jų tvarkymo keliamą riziką, yra išskiriami trys automatiniu būdu tvarkomų asmens duomenų saugumo lygiai, nurodyti lentelėje.

4 lentelė. Automatiniu būdu tvarkomų asmens duomenų saugumo lygiai ir būdingos priemonės

I saugumo lygis	**II saugumo lygis**	**III saugumo lygis**
Šiam saugumo lygiui priskirtas organizacines ir technines duomenų saugumo priemones turi užtikrinti visi duomenų valdytojai, tvarkantys viešai skelbiamus asmens duomenis, taip pat duomenų valdytojai, automatiniu būdu tvarkantys asmens duomenis duomenų bazėje, prie kurios nėra prieigos per išorinius duomenų perdavimo tinklus.	šiam saugumo lygiui priskirtas organizacines ir technines duomenų saugumo priemones turi užtikrinti duomenų valdytojai, automatiniu būdu tvarkantys asmens duomenis duomenų bazėje, prie kurios yra prieiga per išorinius duomenų perdavimo tinklus, taip pat duomenų valdytojai, automatiniu būdu tvarkantys ypatingus asmens duomenis duomenų bazėje, prie kurios nėra prieigos per išorinius duomenų perdavimo tinklus.	šiam saugumo lygiui priskirtas organizacines ir technines duomenų saugumo priemones turi užtikrinti duomenų valdytojai, automatiniu būdu tvarkantys ypatingus asmens duomenis duomenų bazėje, prie kurios yra prieiga per išorinius duomenų perdavimo tinklus.
Kokios saugumo priemonės taikomos		
Patvirtintas rašytinės formos dokumentas, kuriame turi būti nurodyta: duomenų valdytojas, duomenų tvarkytojai ir jų	Jeigu yra paskirtas už duomenų apsaugą atsakingas asmuo ar padalinys, jis negali atlikti administratoriaus funkcijų;	Numatyta taikyti I ir II saugumo lygiui numatytus reikalavimus bei papildomas

atliekamos funkcijos, teisės aktai ir standartai, kuriais vadovaujamasi tvarkant asmens duomenis, apibrėžtas ir teisėtas asmens duomenų tvarkymo tikslas ir baigtinis tvarkomų asmens duomenų sąrašas kiekvienu asmens duomenų tvarkymo tikslu bei konkretūs veiksmai ar procedūros, kurie leis įgyvendinti kitus asmens duomenų tvarkymo reikalavimus. Asmens duomenų saugojimo aktyviojoje ir pasyviojoje duomenų bazėje terminas, duomenų subjekto teisių įgyvendinimo tvarka; asmens duomenų gavėjai ir asmens duomenų teikimo tvarka; asmenų, kuriems suteikta teisė tvarkyti asmens duomenis, funkcijų paskirstymas; prieigos teisių ir įgaliojimų tvarkyti asmens duomenis suteikimo, naikinimo ir keitimo tvarka; asmenų, kuriems suteikta teisė tvarkyti asmens duomenis, informavimas ir apmokymų organizavimo tvarka; asmens duomenų tvarkymo keliamos rizikos vertinimo atlikimo tvarka; saugumo pažeidimų valdymas ir reagavimo į šiuos pažeidimus veiksmai; duomenų atkūrimo jų avarinio praradimo atvejais tvarka; periodiškas Bendrųjų reikalavimų ir juose reglamentuotų nuostatų vykdymo kontrolė; numatyta duomenų atsarginių kopijų darymo ir saugojimo tvarka; reglamentuotos kitos užtikrinamos organizacinės ir techninės duomenų saugumo priemonės; užtikrintas prieigos prie duomenų valdymas ir kontrolė: prieiga prie asmens duomenų gali būti suteikta tik tam asmeniui, kuriam asmens duomenys yra reikalingi jo funkcijoms vykdyti; su asmens duomenimis galima atlikti tik tuos veiksmus, kuriems atlikti yra suteiktos teisės; užtikrintas slaptažodžių konfidencialumas juos suteikiant, pateikiant, reguliariai keičiant bei saugant, jeigu tapatybės patvirtinimas vykdomas naudojant slaptažodžius; turi būti užtikrintos organizacinės ir techninės duomenų saugumo priemonės, skirtos apsaugoti duomenų bazes nuo neteisėto prisijungimo elektroninių ryšių priemonėmis; užtikrintas patalpų, kuriose saugomi asmens duomenys, saugumas užtikrinta kompiuterinės įrangos apsauga nuo žalingų programų.	kontroliuojama prieiga prie asmens duomenų tokiomis organizacinėmis ir techninėmis duomenų saugumo priemonėmis, kurios fiksuoja ir kontroliuoja registravimosi bei teisių gavimo pastangas; nustatytas leistinų nevykusių bandymų prisijungti prie duomenų bazės skaičius; fiksuojami šie asmenų, kuriems suteikta teisė tvarkyti asmens duomenis, prisijungimų prie duomenų bazės įrašai: prisijungimo identifikatorius, data, laikas, trukmė, jungimosi rezultatas, bylos, prie kurių buvo jungtasi, atlikti veiksmai su asmens duomenimis. Šie įrašai turi būti saugomi ne trumpiau kaip 1 metus. Nesant galimybės užtikrinti šiame punkte numatytų priemonių techninėmis priemonėmis, jos turi būti užtikrintos organizacinėmis priemonėmis; užtikrintas patalpų, kuriose saugomi asmens duomenys, saugumas. Teikiamų asmens duomenų paieškos užklausoje turi būti suformuluotas duomenų paieškos tikslas; užtikrinamas saugių protokolų ir slaptažodžių naudojimas, teikiant asmens duomenis išoriniais duomenų perdavimo tinklais; užtikrintas išorinių duomenų laikmenų, kuriose saugomi gaunami ir teikiami asmens duomenys, registravimas, kontrolė ir asmens duomenų ištrynimas po jų panaudojimo perkeliant į duomenų bazes ir pan.; registruojami avarinio asmens duomenų atkūrimo veiksmai. Užtikrinta, kad informacinių sistemų testavimas nebūtų vykdomas su realiais asmens duomenimis, išskyrus būtinus atvejus, kurių metu būtų naudojamos organizacinės ir techninės duomenų saugumo priemonės, užtikrinančios realių asmens duomenų saugumą. Nešiojamuosiuose kompiuteriuose, jeigu jie naudojami ne duomenų valdytojo vidiniame duomenų perdavimo tinkle, esantys asmens duomenys turi būti šifruojami tokiomis priemonėmis, kurios atitiktų duomenų tvarkymo keliamą riziką.	priemones: šifruojami išorinėje duomenų laikmenoje teikiami asmens duomenys arba naudojamos saugos priemonės, užtikrinančios, kad asmens duomenys bus perduodami saugiai ir nebus galimybės tretiesiems asmenims jais pasinaudoti; ne rečiau kaip vieną kartą per mėnesį peržiūrimas naudotojų prisijungimų prie duomenų bazės elektroninis žurnalas ir duomenų valdytojui teikiamos peržiūros ataskaitos.

Duomenų valdytojas turi užtikrinti tvarkomų duomenų saugumą. Todėl prieš nustatant tinkamas duomenų apsaugos saugumo užtikrinimo priemones, būtina nustatyti rizikas, susijusias su duomenų apsaugos tvarkymu. Taip pat duomenų valdytojas turi atitikti specialius reikalavimus, taikomus duomenų apdorojimui ir tvarkomiems duomenims, jei asmens duomenys perduodami už ES ribų. Pagrindiniai asmens duomenų tvarkymo institucijose trūkumai, nurodomi valstybės audito ataskaitoje (2013) yra susiję su duomenų tvarkymo dokumentais. Nėra rengiamos duomenų valdytojo ir duomenų tvarkytojo sutartys, parengtieji jau neaktualūs, pasikeitę asmens duomenų tvarkymo tikslai ir apimtys, taip pat nepakankamai valdoma prieiga prie informacinių sistemų, kai kurios įstaigos, tvarkančios ypatingus asmens duomenis, neįgyvendina net minimalių organizacinių ir techninių duomenų saugos priemonių. 2016 m. gauta 443 skundai, iš jų 291 skundas dėl privataus sektoriaus veiksmų, 57 dėl valstybės institucijų, 82 dėl kitų institucijų, 13 atvejų skundžiamasis asmuo nenurodytas (VDAI metinė ataskaita, 2016, p. 10). Valstybės audito ataskaitoje (2013, p. 21) nurodoma, kad daugiausia dėmesio asmens duomenų apsaugai VDAI turėtų kreipti ten, kur duomenų valdytojai/ tvarkytojai užsiima finansinių paslaugų veikla (18 proc.), teisėsaugos ir teisėtvarkos veikla (17 proc.) ir sveikatos priežiūros veikla (17 proc.). Duomenų kodavimas, šifravimas yra viena iš pagrindinių asmens duomenų apsaugos priemonių. Tai rodo, kad saugumas vertinamas bendrame privatumo kontekste ir gali apimti, pavyzdžiui, asmens tapatybės apsaugą naudojant slapyvardžius arba naudojant šifravimo mechanizmus, leidžiančius saugų duomenų ištrynimą pasibaigus nustatytam saugojimo laikotarpiui.

Pagal žmogaus teisių stebėjimo instituto pateikiamus duomenis apie 2018 m. pradedamą ES duomenų apsaugos reformą, kuri detaliau buvo analizuota 1.2. skyrelyje, bei įsigaliosiančias taisykles tikina žiną tik 5 proc. Lietuvos gyventojų. Dauguma norėtų gauti daugiau informacijos iš žiniasklaidos arba interneto. Tačiau, Lietuvoje nėra sistemiškų ir plačių kampanijų, skirtų paaiškinti gyventojams kompleksinius procesus, vykstančius tvarkant jų duomenis bei įgalinti juos geriau šiuos procesus kontroliuoti (Privatumo paradoksas, 2016, p. 27). Teikiant administracines paslaugas būtina užtikrinti, kad būtų išvengta neteisėtos prieigos prie asmens duomenų, neįvyktų asmens duomenų praradimas, taip pat užtikrinti, kad duomenų apdorojimas vyksta pagal teisės aktuose nurodytus kriterijus (nevyksta nesąžiningas duomenų rinkimas, nukrypimas nuo pradinio tikslo). Tokių situacijų atsiradimas turi įtakos duomenų subjektų privatumui, žmogaus tapatumui, žmogaus teisėms ar pilietinėms laisvėms.

Apibendrinant galima teigti, kad saugumo rizikos vertinimas ir valdymas yra labai svarbus asmens duomenų saugumui. Tinkamai identifikavus grėsmes, galima pasirinkti tinkamas priemones asmens duomenų saugumui užtikrinti. Administracines paslaugas teikiančios institucijos vadovaujasi „Bendraisiais reikalavimais organizacinėms ir techninėms asmens duomenų saugumo priemonėms“. Pagal saugotinų asmens duomenų pobūdį ir keliamą riziką yra išskiriami trys automatiniu būdu tvarkomų asmens duomenų saugumo lygiai.

2.4. Administracinių paslaugų teikimas Lietuvoje

Viešasis sektorius teikia viešąsias gėrybes, dėl kurių nėra konkuruojama, kurios prieinamos kiekvienam individui (Valackienė ir Trofimovas, 2015, p. 123). Pagal Lietuvos Respublikos viešojo administravimo įstatymą (1999, 15 str. 1 d.) administracinės paslaugos yra:

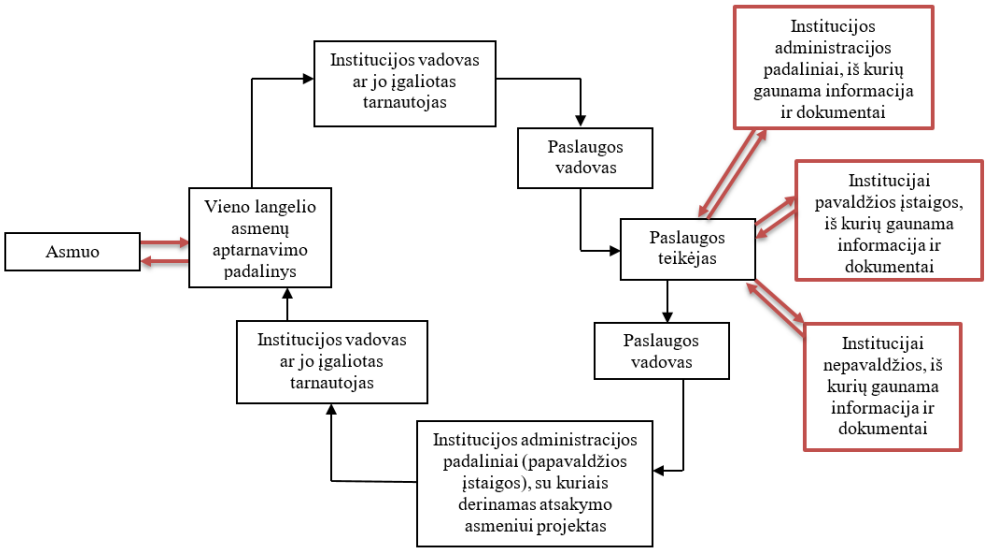
1. leidimų, licencijų išdavimas;
2. dokumentų, kuriais patvirtinamas tam tikras juridinis faktas, išdavimas;
3. deklaracijų priėmimas ir tvarkymas;
4. asmenų konsultavimas viešojo administravimo subjekto kompetencijos klausimais;
5. įstatymų nustatytos viešojo administravimo subjekto informacijos teikimas asmenims;
6. administracinės procedūros vykdymas.

Kaip teigia Raipa ir Laurišonienė (2017, p. 54) „pagrindinis vietos savivaldų teikiant viešąsias paslaugas tikslas yra: viešųjų paslaugų teikimo efektyvumas ir vietos gyventojų, t. y. tų paslaugų vartotojų visuotinis poreikių patenkinimas“. Vietos savivaldybės privalo užtikrinti viešųjų paslaugų teikimą kiekvienam piliečiui. Informacinių ir ryšio technologijų dėka viešosios švietimo, kultūros, civilinės metrikacijos, socialinės pagalbos, viešojo transporto ir kt. paslaugos yra perkeliamos į elektroninę erdvę. Anot Milės ir Junevičiaus (2013, p. 458) „be IT plėtros nebūtų galima kalbėti tiek apie e. valdžios, tiek apie pačių e. paslaugų atsiradimą“. Savo el. tinklapiuose vietos valdžia sukuria prieigą, kurioje piliečiai gali rasti visą su viešosiomis paslaugomis susijusią informaciją, dokumentų formas ir kt.

2012 m. VRM pradėjo projektą „Centralizuotos viešųjų ir administracinių paslaugų sistemos kūrimas ir diegimas įgyvendinant vieno langelio principą“, kurio metu institucijos turėjo užtikrinti, kad administracinė paslauga gyventojui nuo prašymo pateikimo iki paslaugos suteikimo būtų suteikta vienoje darbo vietoje. Administracinių paslaugų teikimo vieno langelio principu būklės viešojo valdymo institucijose analizėje (2012) yra nurodoma, kad „institucijos pačios, nedalyvaujant asmeniui, iš savo administracijos padalinių, pavaldžių įstaigų ir kitų institucijų gautų prašymui išnagrinėti ir administracinei paslaugai suteikti reikalingą informaciją ir dokumentus“. Vadovaujantis vidaus reikalų ministro 2009 m. gruodžio 1 d. patvirtintomis Administracinių paslaugų teikimo aprašymų rengimo rekomendacijomis savivaldybės turėjo parengti administracinių paslaugų teikimo aprašymus ir juos viešai paskelbti. Tai turėjo sudaryti sąlygas vartotojams gauti susistemintą informaciją apie institucijos teikiamas administracines paslaugas. Tačiau minėtas dokumentas buvo tik rekomendacinio pobūdžio. VRM nurodė, kad 2014 m. sausio 20 d., kai fiksuotas šios projekto veiklos įgyvendinimas, buvo užpildyta apie 60 proc. planuotų paslaugų aprašų, 22 institucijos ir įstaigos nepateikė administracinių paslaugų aprašymų. Atlikę teisės aktų analizę ir bendraudami su VRM atstovais nustatėme, kad nėra

reglamentuotas įpareigojimas institucijoms ir įstaigoms teikti bei atnaujinti paslaugų aprašus, reikalingus paslaugų katalogui sudaryti (Valstybės audito ataskaita, 2014, p. 16-17).

Pagal „Viešųjų ir administracinių paslaugų teikimo aprašymų rengimo tvarkos aprašą“ galima išskirti elektroninėmis ir neelektroninėmis priemonėmis teikiamas administracines paslaugas. Abiem priemonėms yra sudaryta veiksmų seka, kuria turėtų būti vadovaujamasi suteikiant administracinę paslaugą. Žemiau pateiktame paveikslėlyje (žr. 8 pav.) yra pateikiama veiksmų seka, kurie yra būtini teikiant administracinę paslaugą neelektroniniu būdu.

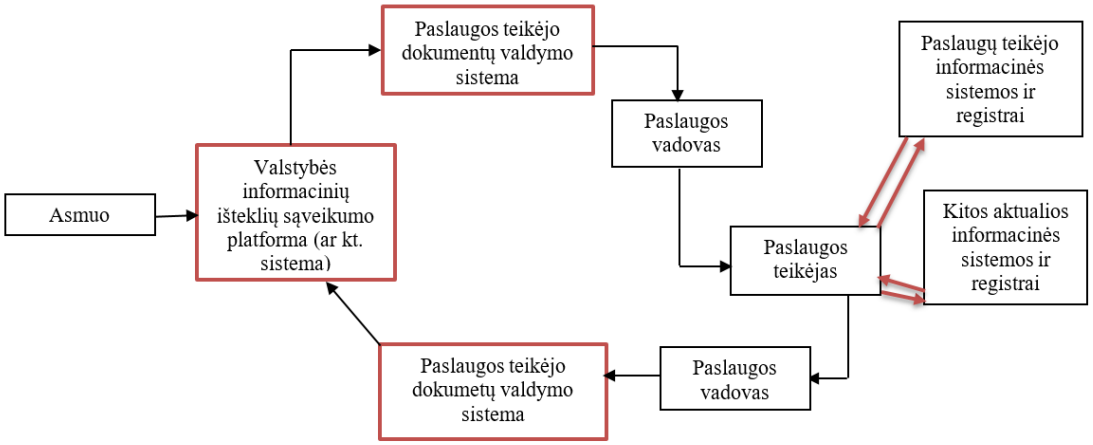


9 pav. Rekomenduojama būtinų veiksmų, atliekamų teikiant paslaugas neelektroninėmis priemonėmis, sekos schema

Kaip matoma, dažniausiai rizika, susijusi su asmens duomenų apsaugos užtikrinimu, kyla kai į administracinės paslaugos teikimą įsijungia paslaugos teikėjas, kuris gauna informaciją ir reikiamus dokumentus iš kitų institucijos administracijos padalinių, institucijai pavaldžių ar nepavaldžių įstaigų. Lietuvos Respublikos dokumentų ir archyvo įstatyme yra nurodyta, kad valstybės ar savivaldybės institucijos, privalo nustatyti institucijos veiklos dokumentų registrus, kitus apskaitos dokumentus taip pat paskirti už veiklos dokumentų registravimą, tvarkymą, apskaitą, saugojimą ir naikinimą atsakingus asmenis ir nustatyti jų įgaliojimus. Valstybės ir savivaldybių institucijos taip pat privalo teisės aktų nustatyta tvarka išduoti juridinius faktus patvirtinančius dokumentus, susijusius su asmens teisių įgyvendinimu. Atsižvelgiant į Lietuvos vyriausiojo archyvaro patvirtintas dokumentų saugojimo taisyklės, bendrieji saugyklų įrengimo reikalavimai taikomi visoms dokumentų saugojimo patalpoms bei patalpoms, kuriose saugomi elektroniniai dokumentai. Pagrindiniai reikalavimai, kad saugyklos būtų įrengiamos specialiai archyvui arba dokumentams saugoti pritaikytose patalpose, apsaugotuose nuo kenksmingo aplinkos poveikio, neįrengiant langų, patalpų aukštis būtų ne mažesnis kaip 250 cm. Saugyklose neturi būti dujotiekio, vandentiekio, lietaus kanalizacijos vamzdynų, elektros tranzitinių kabelių, kurie galėtų pakenkti saugomiems dokumentams.

Spartūs technologiniai pokyčiai lėmė tai, kad administracinių paslaugų teikimas sparčiai keliasi į elektroninę erdvę. Teikiant administracines paslaugas yra kuriami metaduomenys. Anot Prokopčik (2008) „metaduomenys yra struktūriškai apibrėžta informacija, kuri apibūdina, paaiškina dokumentą ar informacinį išteklių, nurodo jo buvimo vietą arba kitokiu būdu palengvina jo suradimą, naudojimą arba valdymą“. Administraciniuose procesuose metaduomenys siejami su atliekamais procesų valdymais ir gaunama informacija apie bet kokio tipo ar rūšies informacijos išteklių. Administravimo metaduomenys apima įvairius technologinius procesus: komplektavimas, skaitmeninimas, autorių teisių apsauga, dokumentų priežiūros veiksmai – konservavimas, restauravimas, skaitmeninimas (Prokopčik, 2008).

Informacinės visuomenės plėtros komiteto pateiktais duomenimis, nurodoma, kad siekiant sudaryti sąlygas valstybės informacinėms sistemoms ir registrams standartizuotu būdu keistis duomenimis bei elektronines paslaugas kurti ir jas teikti centralizuotai, 2008 m. buvo sukurta ir įdiegta Viešojo administravimo institucijų informacinių sistemų interoperabilumo sistema, vėliau ji buvo pervadinta į Valstybės informacinių išteklių sąveikumo platforma (VIISP) susidedanti iš dviejų pagrindinių dalių: duomenų mainų platformos ir centrinio elektroninių paslaugų portalo „Elektroniniai valdžios vartai“. Būtini veiksmai, kuriuos reikia atlikti teikiant administracines paslaugas elektroniniu būdu yra pateikiama paveikslėlyje (žr. 10 pav.).



10 pav. Rekomenduojama būtinų veiksmų, atliekamų teikiant paslaugas elektroninėmis priemonėmis, sekos schema

Vyriausybė nurodė nuo 2010 m. valstybės institucijoms, administruojančios viešąsias ir teikiančioms administracines paslaugas, el. erdvėje užtikrinti paslaugų pasiekiamumą el. valdžios vartų svetainę (Valstybinio audito ataskaita, 2013).

VIISP užtikrina galimybę asmenims vieno langelio principu gauti institucijų teikiamas viešąsias ir administracines elektronines paslaugas. VIISP nuostatose nurodoma, kad VIISP duomenų bazėje tvarkomi šie duomenys:

- juridinio asmens kodas, pavadinimas, buveinės adresas, kontaktiniai duomenys (el. pašto adresas, tel. nr.);
- fizinio asmens kodas, vardas ir pavardė, kontaktiniai duomenys (el. pašto adresas, tel. nr.)
- valstybės tarnautojo ar darbuotojo kodas Valstybės tarnautojų registre, pareigybės patvirtinimas, duomenys apie valstybės ar savivaldybių instituciją ar įstaigą, kurioje pareigybė registruota, kontaktiniai duomenys;
- VIISP paslaugų gavėjo sistemą identifikuojantys techniniai duomenys;
- elektroninės paslaugos duomenys (elektroninės paslaugos pavadinimas; trumpas elektroninės paslaugos aprašymas; kam paslauga skirta; paslaugos kategorija; tapatybės nustatymo būdai; elektroninės paslaugos brandos lygis; duomenys apie suteiktą konsultaciją);
- elektroninių paslaugų gavėjo tapatybės patvirtinimo data, laikas ir kt. parametrai;
- VIISP paslaugų gavėjų dokumentai (raštai);

Nors viešojo administravimo įstatyme yra aiškiai apibūdintos administracinės paslaugos, Lietuvoje vis dar sunku įvertinti kiek tiksliai valstybinės institucijos ir savivaldybės teikia paslaugų. Atsakingos institucijos nežino kiek ir kokių paslaugų yra teikiama asmenims. Iki šiol Lietuvoje nevykdoma nuosekli visų viešųjų ir administracinių paslaugų stebėsena (Valstybės audito ataskaita, 2014, p. 17). Vartotojams sunku rasti reikiamą informaciją apie paslaugas, kadangi Lietuvoje veikia keletas paslaugų katalogų ir nė vienas ne tik neapima visų paslaugų:

- „Verslo vartai“ – koordinuoja VŠĮ „Versli Lietuva“;
- „Elektroniniai valdžios vartai“ – koordinuoja IVPK;
- „Prisijungusi Lietuva“ – IVPK inicijuotas informacinis projektas;
- „Lietuvos paslaugų katalogas“ – Lietuvos Respublikos vidaus reikalų ministerija.

Iš sukurtų katalogų galima susidaryti nuomonę, kad administracinių paslaugų teikime elektroninėje erdvėje trūksta vientisumo ir bendros politikos. Administracinės paslaugos yra išskiriamos viešojo administravimo įstatyme. Administracinės paslaugos gali būti teikiamos elektroninėmis ir neelektroninėmis priemonėmis, jų teikimui būtinų veiksmų seka yra nurodyta „Viešųjų ir administracinių paslaugų teikimo aprašymų rengimo tvarkos apraše“. Spartūs technologiniai pokyčiai lėmė tai, kad administracinių paslaugų teikimas sparčiai keliasi į elektroninę erdvę. Tačiau Vidaus reikalų ministerijos inicijuotas centralizuotas administracinių paslaugų perkėlimo į elektroninę erdvę projektas turėjo trūkumų, kurie sukėlė nepatogumus vartotojo atžvilgiu.

Apibendrinant galima teigti, kad asmens duomenų teisinės apsaugos įstatymas (1996) yra pagrindinis asmens duomenų apsaugą reglamentuojantis teisinis dokumentas Lietuvoje, vis dėl to asmens duomenų apsauga yra plati sritis. Tai bendrai atsispindi Lietuvos Respublikos įstatyminėje bazėje – reklamos, elektroninių ryšių, informacinės visuomenės paslaugų, kibernetinio saugumo

įstatymuose, kuriuose yra numatytas asmens duomenų užtikrinimas. Nors Lietuvoje teisinė bazė yra pakankama, kad užtikrintų asmens duomenų apsaugą, institucijų atžvilgiu dubliuojasi veiklos sritys, kaupiami pertekliniai duomenys, kurie vėliau nėra panaudojami. Su asmens duomenų apsauga dirba krašto apsaugos, susisiekimo ir vidaus reikalų ministerijos. VDAI yra ta institucija, kuri prižiūri, kaip duomenų valdytojai laikosi nustatytų reikalavimų. Administracinių paslaugų teikimo metu gyventojai pateikia asmeninius duomenis, kurių apsaugą būtina užtikrinti. Viešųjų ir administracinių paslaugų teikimo aprašymų rengimo tvarkos apraše“ yra išskirti elektroniniu ir neelektroniniu būdu teikiamos administracinės paslaugos. Administracines paslaugas teikiant neelektroniniu būdu yra vadovaujamasi dokumentų ir archyvų įstatymu taip pat dokumentų saugojimo taisyklėmis. Informacinių technologijų pokyčiai lėmė, kad administracinės paslaugos buvo vis plačiau perkeliamos į elektroninę erdvę. Siekiant sudaryti sąlygas valstybės informacinėms sistemoms ir registrams standartizuotu būdu keistis duomenimis bei elektronines paslaugas kurti ir jas teikti centralizuotai, buvo sukurta Valstybės informacinių išteklių sąveikumo platforma.

3. ASMENS DUOMENŲ APSAUGOS UŽTIKRINIMO TEIKIANT ADMINISTRACINES PASLAUGAS SAVIVALDYBĖSE TYRIMAS

Šiame skyriuje pateikiama empirinio tyrimo metu surinktų duomenų analizė. Analizuojami asmens duomenų apsaugos užtikrinimo pokyčiai Lietuvoje, priėmus svarbiausius ES teisinius dokumentus – duomenų apsaugos direktyvą (1995) ir Bendrąjį duomenų apsaugos reglamentą. Tiriamos asmens duomenų apsaugos užtikrinimo priemonės teikiant administracines paslaugas Lietuvos savivaldybėse.

3.1. Tyrimo metodika

Tyrimo tikslas – nustatyti kaip Lietuvos savivaldybės taiko asmens duomenų apsaugos užtikrinimui nustatytas priemones, teikdamos administracines paslaugas. Šiam tikslui įgyvendinti buvo iškelti tokie uždaviniai:

1. Išanalizuoti, kaip kito asmens duomenų apsaugos užtikrinimas Lietuvoje;
2. Ištirti, kokios asmens duomenų apsaugos priemonės yra taikomos Lietuvos savivaldybės teikiant administracines paslaugas.
3. Nustatyti, kaip vyksta pasiruošimas Bendrojo duomenų apsaugos reglamento taikymui ir kiek pasiruošusios yra Lietuvos savivaldybės.

Asmens duomenų apsauga yra specifinė sritis, todėl tyrimui atlikti buvo pasirinktas kokybinio tyrimo metodas. Anot Tidikio (2003, p. 359), kokybinių metodų naudojimas yra prioritetinis, jeigu tyrėjo dėmesio centre yra atskiro socialinio objekto savitumas, viso įvykio vaizdo arba atvejo, objektyvių ir subjektyvių jo faktorių vienovės ir sąveikos tyrimas.

Tyrimui atlikti pasirinktas pusiau struktūruoto interviu metodas: iš anksto sudaromi klausimai, tačiau tyrimo metu gali būti pateikiami ir plane neįrašyti klausimai, kuriuos tyrėjas gali užduoti papildomai. Taip sukuriama laisvesnė bendravimo aplinka (Bitinas, Rupšienė, Žydžiūnaitė, 2008). Kaip teigia Tidikis (2003, p. 467), ši rūšis patogi tuo, kad griežtai neformalizuojamas pašnekesys ir tarp klausėjo su respondentu būna laisvesnė atmosfera.

Mokslinėje literatūroje detaliau aprašomas interviu tyrimo planavimas. Steinaras Kvale mini tokius interviu tyrimo planavimo etapus, kurių laikantis buvo atliekamas tyrimas:

- temos formulavimas
- tyrimo planas
- interviu ėmimas
- interviu duomenų aprašymas, transkribavimas

- duomenų analizė ir jos pateikimas (Kardelis, 2016, p. 262)

Pusiau struktūruotas interviu atliekamas dviem etapais. Pirmiausia buvo sudarytas klausimynas, skirtas VDAI darbuotojams apklausti (1 priedas). Darbuotojai pateikė ekspertinę nuomonę apie asmens duomenų apsaugos reikalavimus, taikomus viešajame sektoriuje. Iš viso buvo apklausti 2 darbuotojai, interviu vyko telefonu iš anksto suderintu laiku. Informantų atsakymai buvo užkoduoti (kodas A1, A2).

Antrasis etapas – savivaldybių tyrimas, siekiant ištirti nustatytų priemonių laikymąsi teikiant administracines paslaugas. Klausimynas pateikiamas prieduose (žr. 2 priedas). Iš viso buvo apklaustos 8 savivaldybės: Tauragės, Raseinių, Jurbarko, Trakų, Šilalės, Pagėgių, Prienų rajonų bei Kauno miesto savivaldybės. Savivaldybės buvo parinktos patogiosios atrankos būdu.

5 lentelė. Informacija apie informantus

Savivaldybė	Interviu pobūdis	Informanto specialybė	Kodas
Tauragės rajono	Susitikimas	Informatikos skyriaus vedėjas	S1
Trakų rajono	Raštu	Bendrųjų reikalų ir informacinių technologijų skyriaus vedėjas	S2
Raseinių rajono	Telefonu	Dokumentų ir viešųjų ryšių skyriaus vyriausioji (informatikos) specialistė	S3
Kauno miesto	Raštu	E. paslaugų ir informacinių technologijų skyriaus vyriausioji specialistė	S4
Šilalės rajono	Raštu	Dokumentų valdymo skyriaus vedėja	S5
Jurbarko rajono	Raštu	Teisės ir personalo skyriaus vedėja	S6
Prienų rajono	Raštu	Personalo ir ūkio skyriaus vedėja	S7
Pagėgių rajono	Telefonu	Bendrojo ir juridinio skyriaus vedėja	S8

Dėl apklausiamųjų laiko stokos interviu teko derinti net kelias savaites, dėl tos pačios priežasties respondentai skubindavosi ir stengdavosi kuo greičiau užbaigti interviu. Tačiau visais atvejais pavyko gauti atsakymus į visus klausimus arba bent jau pakankamai informacijos, kuri leistų gauti duomenis apie esamą situaciją, identifikuoti problemas ir nustatyti ateities planus analizuojamoje srityje.

Klausimynai buvo išsiųsti 60 savivaldybių administracijų, bet atsakas sulauktas tik iš 16, iš jų dar 8 neturėjo galimybės atsakyti, nes už duomenų apsaugą atsakingi darbuotojai tuo metu atostogavo arba buvo komandiruotėje. Dažniausiai už duomenų apsaugos užtikrinimą savivaldybėse atsakingi yra IT specialistai, tačiau yra ir išimčių kai tai daro bendrojo skyriaus specialistai. Čia išryškėjo problema, kad institucijose apskritai sunku rasti asmenį, kuris būtų kompetentingas atsakyti į sudarytą klausimyną. Pavyzdžiui, Pagėgių rajono savivaldybės atveju vyko didelė darbuotojų kaita. Neseniai

Pagėgių rajono savivaldybės bendrojo ir juridinio skyriaus vedėjos ir IT specialisto pareigas pradėjo eiti nauji darbuotojai, todėl atsakyti į užduotus klausimus galėjo labai siaurai. Prienų rajono savivaldybė nurodė, kad šiuo metu tik pradeda dirbti duomenų apsaugos srityje, lyginant su apklaustomis savivaldybėmis Prienų rajonas yra mažiausiai pažengęs asmens duomenų apsaugos srityje.

3.2. Asmens duomenų apsaugos užtikrinimo raida Lietuvoje

Asmens duomenų apsaugos užtikrinimą Lietuvoje lėmė ES lygiu priimti teisiniai dokumentai. *„Duomenų apsauga Lietuvoje kito tiek, kiek kito ES reglamentavimas“ (A1).* Nuo pat 1990 m. Yra išskiriami trys etapai, lėmę esminius pokyčius asmens duomenų apsaugos srityje. Pirmasis – kuomet buvo pripažintas asmens duomenų apsaugos teisinio reguliavimo reikalingumas. *„Pirmas kardinalus įvykis –tai duomenų apsaugos reglamentavimo pradžia, ne tik informacijos saugumo prasme, bet ir kaip žmogaus teisė į duomenų apsaugą (ne vien privatumą)“ (A1).* Pirmasis teisinis dokumentas, kuris lėmė tolesnį asmens duomenų apsaugos reglamentavimą ES šalyse narėse yra direktyva „Dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo“ (1995). Šis dokumentas, turėjo užtikrinanti lygiavertę asmens duomenų apsaugą ES ribose. Pradėjus taikyti direktyvą atsirado suvokimas, kad asmens duomenys yra svarbus visuomenės saugumo klausimas: „*Antras virsmas yra ir kiekybinis ir kokybinis, tai pripažinimas, kad asmens duomenų apsauga yra labai svarbus dalykas ne tik žmogaus teisių gynimo prasme, tačiau ir visuomenės saugumo prasme“ (A1).* Asmens duomenų apsauga yra viena iš žmogaus teisių gynimo sričių, todėl kaip ir kitas pagrindines laisves ir teises, taip ir asmens duomenų apsaugą valstybė turi užtikrinti. Iki duomenų apsaugos direktyvos (1995) taikymo pradžios, asmens duomenų apsaugą Lietuvoje tam tikrais pažeidimų atvejais reguliavo civilinis kodeksas. *„Bet tai ne ta duomenų apsauga, kaip mes ją dabar suprantame pagal europinius dokumentus“ (A2).* 1996 m. Įsigaliojo asmens duomenų apsaugos įstatymas bei įkurta asmens duomenų priežiūros institucija. VDAI atliekamos funkcijos ir galios plėtėsi: *„Manau reikšminis pokytis – tai, kad inspekcijos galios pasidarė tokios pačios kaip ir kitų ES priežiūros institucijų“ (A2).* VDAI darbuotojų skaičius išsiplėtė nuo 8 darbuotojų iki šiuo metu esamų 30. Tokį darbuotojų skaičiaus pokytį lėmė išplėstos funkcijos: *„8 žmonės prižiūrėjo tik valstybės informacinius išteklius – registrus. Šiuo metu 30 žmonių prižiūri visą juridinių asmenų registrą. Nesvarbu, kad kai kurie juridiniai asmenys neturi pareigos registruotis, kaip duomenų valdytojai, tačiau jų veikla vis vien yra prižiūrima“ (A1).* Nors šiuo metu VDAI turi tokią pat galią kaip ir kitų ES šalių institucijos, atsakingos už asmens duomenų apsaugą, yra ir tam tikrų skirtumų: *„tai kad inspekcija prisideda ir prie kibernetinio saugumo politikos vykdymo“(A2).* Šie įgaliojimai VDAI atsirado visai ne seniai 2014 m., kuomet buvo priimtas kibernetinio saugumo įstatymas. Kitus pokyčius asmens duomenų apsaugos

srityje taip pat būtų galima susieti su kintančia teisine baze Lietuvoje. Pirmiausia tai su elektroninių ryšių įstatymu:

> *„jis buvo priimtas įgyvendinant direktyvą, kas liečia duomenų tvarkymą – elektroninė rinkodara, ryšių priemonės ir t.t. <...> Inspekcija pradėjo prižiūrėti juridinius asmenis. Ką tai reiškia? Jei siunčiu rinkodarą abonentu, abonentas gali būti ir juridinis asmuo. Tai toks išskirtinis visiškai atvejis, kada inspekcija gina ne tik fizinio asmens teises, bet ir juridinio asmens teises“ (A2).*

Valstybės informacinių išteklių įstatyme numatyta, kad VDAI atsako už asmens duomenų apsaugos reikalavimų įgyvendinimą ir jų laikymosi priežiūrą: *„kompetencija numatyta ir valstybės informacinių išteklių valdymo įstatyme, ko ankščiau nebuvo, tą lėmė tik paskutiniai įstatymo pakeitimai“ (A2).*

Trečiasis etapas – tai duomenų apsaugos reforma ir jos įgyvendinimas. Nuo 2018 m. Gegužės 25 d. Bus pradėtas taikyti Bendrasis duomenų apsaugos reglamentas, kuris palies tiek viešąjį tiek privatų sektorius:

> *„Pokyčiai laukia visų duomenų valdytojų ir tvarkytojų. Jie taps atsakingi už visus savo veiksmus ar neveikimą, tvarkant asmens duomenis. Jie bus atsakingi, kad duomenys bus surinkti turint teisinį pagrindą, kad duomenys būtų tvarkomi pagal teisės aktų reikalavimus, kad duomenys nebūtų atskleisti ar surinkti neturint tam pagrindo“ (A1).*

Nepaisant teisinės aplinkos pokyčių, VDAI galių išsiplėtimo, visuomenėje vis dar trūksta supratimo, kad asmens duomenų apsaugos užtikrinimas yra viena iš žmogaus teisių ginimo sričių, kurią būtina užtikrinti. Kibernetinio saugumo apžvalgoje (2016, p. 46) teigiama, kad „incidentai globaliame elektroninių ryšių tinkle sukelia realias grėsmes individų teisėms ir laisvėms“. Viešasis sektorius taip pat nėra apsaugotas nuo incidentų, priešingai, pastaraisiais metais vis daugiau viešojo sektoriaus institucijų tapo kibernetinių atakų taikiniu. Pasikartojantys incidentai verčia vartotojus abejoti viešojo sektoriaus teikiamomis paslaugomis: *„vartotojas 100 proc. galbūt ir negali būti garantuotas duomenų saugumu“ (S1).* Tačiau pranešimų apie duomenų apsaugos pažeidimus viešajame sektoriuje, lyginant su privačiu sektoriumi skaičius nėra toks didelis: *„su elektroninių paslaugų teikimu, kad būtų užfiksuota pranešimų, inspekcija nėra daug užfiksavusi“ (A2).* Mažas incidentų skaičius viešajame sektoriuje yra siejamas su tuo, kad viešajame sektoriuje nėra vykdoma tiesioginė rinkodara, kur ir yra užfiksuojamas didžiausias incidentų skaičius: *„<...> patys pažeidimai yra panašūs ir viešajame ir privačiame sektoriuose. Gal tiesiog skiriasi pažeidimų skaičius, kadangi viešajame sektoriuje nėra vykdoma tiesioginė rinkodara“ (A1).* Nors ir vienetiniai incidentai viešajame sektoriuje kelią didžiulį susirūpinimą duomenų saugumu: *„<...> kiekvienas atvejis yra kitoks. 2003 m.*

vykusi duomenų vagystė iš SODROS, sakyčiau vienetinis atvejis“ (A1). Duomenų vagystę iš Sodros tyrė kriminalinė policija. Inspekcija atliko patikrinimą – kokios saugumo priemonės naudojamos tvarkant asmens duomenis. Buvo pateiktas nurodymas, kurį Sodra įvykdė. *„<...> gerai žinomas atvejis, su vyriausia rinkimų komisija.. atvejis, kai dėl techninių kliūčių buvo momentas, kai buvo galima susipažinti su trečiųjų asmenų duomenimis“ (A2).* Vyriausioji rinkimų komisija pranešimą apie pažeidimą pateikė 2016 m. spalio mėn. Pažeidimo esmė buvo ta, kad prisijungimo prie www.rinkejopuslapis.lt galėjo būti matomi 97 asmenų duomenys: vardas, pavardė, gimimo metai ir adresas. Inspekcija atliko patikrinimą, pateikė nurodymą. „<...>*Buvo atvejis su INFOSTATYBA taip pat“ (A2).* Valstybinė teritorijų planavimo ir statybos inspekcija prie Aplinkos ministerijos apie pažeidimą pranešė 2017 m. sausio mėn. Per portalą be jokių papildomų pastangų buvo galima pamatyti apie 200 asmens duomenų. Nustatyta, kad programų diegėjai padarė klaidą. Klaida buvo ištaisyta iš karto kai tapo žinoma. Ją pastebėjęs asmuo paskambino į VDAI, kuri iš karto susisiekė su įstaiga. VDAI atliko patikrinimą, pateikė nurodymą.

3.3. Lietuvos savivaldybių administracinių paslaugų teikimo metu taikomos asmens duomenų apsaugos užtikrinimo priemonės

Visi tyrime dalyvavę informantai nurodė, kad teikdami administracines paslaugas gyventojams vadovaujasi asmens duomenų teisinės apsaugos įstatymu. *„Asmens duomenų apsaugos reikalavimai yra vienodi tiek viešajam, tiek privačiam sektoriui. Įstatymas yra vienodai taikomas visiems“ (A1).* Detaliau analizuojant taikomas priemones asmens duomenų saugumo užtikrinimui, dalis informantų nurodė, kad vadovaudamiesi „Bendrųjų elektroninės informacijos saugos reikalavimų aprašu“, savivaldybėse yra sukurti ir patvirtinti įgyvendinamieji teisės aktai, kuriuose numarytos priemonės asmens duomenų užtikrinimui. *„Asmens duomenų apsaugos įstatymas numato bazę, kaip tokią, jei žiūrėti siauriau yra minėti bendrieji reikalavimai organizacinėms ir techninėms saugumo priemonėms, kurias yra patvirtinęs inspekcijos direktorius“ (A2).* Lentelėje nurodoma, kokiais metais atitinkama savivaldybė priėmė dokumentus susijusius su asmens duomenų apsauga.

6 lentelė. Savivaldybėse priimti asmens duomenų saugumą užtikrinantys dokumentai

Savivaldybė	Data	Dokumentas
Tauragės rajono	2016 m. gruodžio 9 d.	Įsakymas „Dėl asmens duomenų tvarkymo Tauragės rajono savivaldybės administracijoje taisyklių patvirtinimo“.
	2016 m. kovo 31 d.	Įsakymas „Dėl Tauragės rajono savivaldybės administracijos informacinės sistemos duomenų saugos nuostatų patvirtinimo“.
	2017 m. vasario 27 d.	Įsakymas „Dėl Tauragės rajono savivaldybės administracijos elektroninės informacijos saugos dokumentų patvirtinimo“.

Kauno miesto	2011 m. lapkričio 17 d.	Įsakymas „Dėl asmens duomenų tvarkymo“. Kiti dokumentai viešai neprieinami.
Raseinių rajono	2016 m.	Dokumentas viešai neprieinamas.
Jurbarko rajono	2017 m. kovo 30 d.	Įsakymas „Dėl Jurbarko rajono savivaldybės administracijos informacinės sistemos naudotojų administravimo taisyklių, Jurbarko rajono savivaldybės administracijos informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklių ir Jurbarko rajono savivaldybės administracijos informacinės sistemos veiklos tęstinumo valdymo plano patvirtinimo“.
	2016 m. gruodžio 8 d.	Įsakymas „Dėl asmens duomenų tvarkymo Jurbarko rajono savivaldybės administracijoje taisyklių patvirtinimo“.
	2016 m. balandžio 13 d.	Įsakymas „Dėl Jurbarko rajono savivaldybės administracijos informacinės sistemos duomenų saugos nuostatų patvirtinimo, saugos įgaliotinio, administratoriaus skyrimo ir saugos politiką įgyvendinančių dokumentų rengimo“.
Šilalės rajono	2015 m. vasario 3 d.	„Dėl Asmens duomenų tvarkymo Šilalės rajono savivaldybės administracijoje taisyklių patvirtinimo“.
	2008 m. gegužės 30 d.	„Dėl Šilalės rajono savivaldybės administracijos informacinių sistemų duomenų saugos nuostatų patvirtinimo“.

Asmens duomenų apsaugos įstatyme yra nurodyta, kad tvarkant asmens duomenis būtina užtikrinti jų saugumą, kaip tai bus daroma turi pasirinkti pati institucija: *„mes sakome, kad turite užtikrinti saugumą, prieigą riboti ir t.t. bet kokiu būdu tai darys pasirenka pačios institucijos“ (A2).* Iš pateiktų duomenų matoma, kad didžioji dalis savivaldybių saugos nuostatus patvirtino 2016 – 2017 metais: *„viešasis sektorius labai daug padarė per pastaruosius metus, kadangi jau kelerius metus yra stebimi valstybės informaciniai ištekliai, tikrinami įvairūs duomenų apsaugos aspektai <...>“ (A1).* Galima išskirti tik Kauno miesto savivaldybę, kuri asmens duomenų tvarkymą reguliuoti pradėjo 2011 m. Be to Kauno miesto savivaldybė yra nurodžiusi, kad patvirtintos priemonės yra taikomos ne tik darbuotojams, kurie tvarko asmens duomenis, bet ir kitoms įstaigoms tvarkančioms asmens duomenis: *<...> „įsakymas yra taikomas visiems asmens duomenims, kuriuos tvarko KMSA darbuotojai – ir tiems, kurių valdytoja yra KMSA, ir tiems, kurių valdytojai yra kitos įstaigos“ (S4).*

Tačiau duomenys rodo ir tai, kad daugelis tyrime dalyvavusių savivaldybių vis dar neturi pasitvirtinusios jokių saugos nuostatų. Pavyzdžiui, Prienų rajono savivaldybė dirbti šioje srityje pradėjo tik šiuo metu: *„kol kas nieko negalime padėti, nes su duomenų apsauga pradedame dirbti tik dabar“ (S7).* Iš tyrime dalyvavusių savivaldybių jokių duomenų saugos nuostatų neturi ir Pagėgių ir Trakų rajono savivaldybės *<...> „tokia netvarka kol kas yra daugelyje savivaldybių“ (S1).* Čia galima įžvelgti tam tikrus prieštaravimus, kadangi VDAI tvirtinimu, viešajame sektoriuje sisteminių problemų, susijusių su asmens duomenų apsauga nėra: *„Na viešajame sektoriuje tokių problemų kaip ir nėra <...> nėra sisteminių problemų“(A1).* Tačiau asmens duomenų apsaugos sistema Lietuvoje vis dar nėra iki galo išgryninta, viešajame sektoriuje trūksta tarpusavio veiksmų suderinamumo:

„informaciją apie asmens duomenų automatizuotą tvarkymą ir apsaugą viešajame sektoriuje skirtingais tikslais ir priemonėmis kaupė įvairios įstaigos (pvz.: Vidaus reikalų ir Susisiekimo ministerijos) ir priežiūros institucijos (pvz.: Ryšių reguliavimo tarnyba), tačiau nei viena jų tarpusavyje nesuderino stebėjimo procesų ir įrankių, o VDAI neturėjo galimybių automatiniu būdu gauti kaupiamus duomenis“ (Valstybės audito ataskaita 2013, p. 21 – 22).

Kaip matoma trūksta tarp institucinio bendradarbiavimo. Duomenys yra masiškai renkami, tik tolesnis jų panaudojimas yra ribotas. VDAI tvirtina, kad valstybės audito metu nustatyti trūkumai yra vis dar šalinami: *„Valstybės kontrolė, atlikdama informacinių išteklių tyrimą, tiesiog rado trūkumus, kuriuos reikėtų šalinti ir jie yra šalinami“.* 2016 m. vykusios kibernetinio saugumo pratybos rodo, kad pažanga šioje srityje padaryta. NKC duomenimis pratybos „Kibernetinis skydas 2016“ parodė, kad priimti saugumą reglamentuojantys teisės aktai leidžia identifikuoti ir valdyti kibernetinius incidentus, tačiau vis dar išlieka trūkumai susiję su gebėjimu vadovautis ir mokėjimu interpretuoti skirtingus teisės aktus (NKC metinė ataskaita, 2016, p.46).

Be ankščiau įvardintų asmens duomenų apsaugai užtikrinti naudojamų priemonių – teisės aktų ir vidaus tvarkos taisyklių, informantai teigė, kad teikiant administracines paslaugas yra naudojamos ir bendrosios priemonės: *„slaptažodžiai, antivirusinės programos“ (S1, S5, S7, S8), papildomos programinės įrangos apsaugos priemonės (S2, S4), prieigų prie informacijos ribojimas, slaptažodžių, elektroninių autentifikavimo priemonių naudojimas (S3).* Kaip viena iš pagrindinių apsaugos užtikrinimo priemonių buvo įvardytas saugaus valstybinio duomenų perdavimo tinklas: *„viena iš pagrindinių priemonių tai saugaus duomenų perdavimo tinklas, savivaldybė nenaudoja viešo interneto. Tai gana brangi paslauga. Taigi, duomenys juda tik tame saugiame tinkle“ (S1).* Viešasis sektorius turi ribotą biudžetą, todėl ne kiekviena savivaldybė gali leisti įdiegti šį tinklą. Valstybinės įmonės „Infostruktūra“ duomenimis šiuo metu saugiu valstybinio duomenų perdavimo tinklu naudojasi apie 60 proc. visų viešojo sektoriaus institucijų. Iš visų tyrime dalyvavusių savivaldybių, tik Kauno miesto savivaldybė išskyrė, kad asmens duomenys yra tvarkomi teisėtais tikslais, kurie yra skelbiami asmens duomenų valdytojų valstybiniame registre:

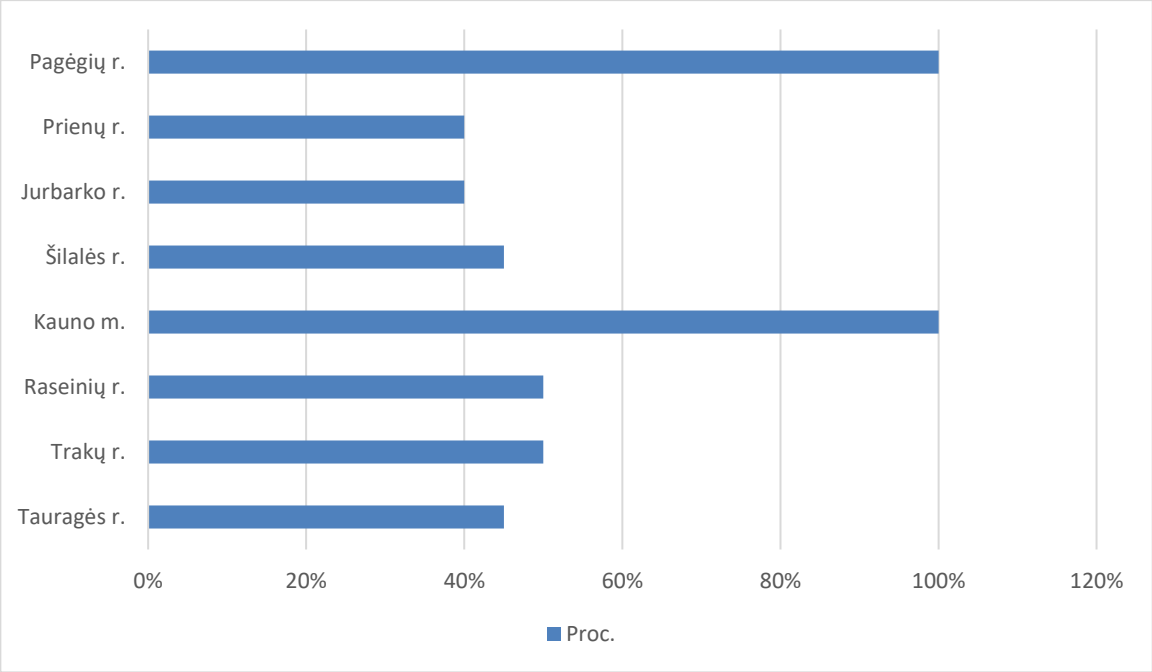
> *„asmens duomenų tvarkymas vykdomas vadovaujantis teisės aktais, Asmens duomenų teisinės apsaugos įstatyme (toliau – ADTAĮ) yra nustatyta, kad asmens duomenys gali būti tvarkomi tik teisėtais tikslais, todėl kalbėdami apie asmens duomenų tvarkymą reikėtų kalbėti apie konkretų duomenų tvarkymo tikslą. Vadovaujantis ADTAĮ, Kauno miesto savivaldybės administracijos (toliau – KMSA) asmens duomenų tvarkymo tikslai skelbiami Asmens duomenų valdytojų valstybiniame registre https://www.ada.lt/go.php/lit/img/11“ (S4).*

Tyrimo metu buvo tikrinamas minėtas asmens duomenų valdytojų valstybinis registras, kuriame buvo skelbiami visų tyrime dalyvavusių savivaldybių asmens duomenų tvarkymo tikslai, tiesa skyrėsi

tik jų skaičius bei registravimo datos. Kauno miesto savivaldybė įvardijo 16, Šilalės rajono savivaldybė 10, Jurbarko rajono – 8, Trakų ir Raseinių rajono savivaldybės – 4 asmens duomenų tvarkymo tikslus, Pagėgių, Tauragės rajono savivaldybės nurodė, kad asmens duomenys yra tvarkomi švietimo tikslais, Prienų rajono savivaldybė – pažymos apie gyvenamąją vietą išdavimo tikslu. Detalūs savivaldybių asmens duomenų tvarkymo tikslai yra pateikiame prieduose (žr. 3 priedas). Iš surinktų duomenų galima teigti, kad didelė dalis savivaldybių vangiai atnaujina prieš daugiau ne dešimtmetį įregistruotus asmens duomenų tvarkymo tikslus.

Savivaldybės asmens duomenų saugumo užtikrinimu teikiant administracine paslaugas yra kontroliuojamos, teikia ataskaitas: *„Savivaldybė yra kontroliuojama, taip pat nuolat teikia ataskaitas, kartą per metus pateikia duomenis NKSC, VRM“ (S1), „Apie elektroniniu būdu ir kitais būdais suteiktas paslaugas kas ketvirtis yra teikiamos Paslaugų stebėsenos rodiklių ataskaitos Vidaus reikalų ministerijai <...>“ (S5).*

Analizuojant savivaldybių administracinių paslaugų teikimo metu taikomas asmens duomenų apsaugos užtikrinimo priemonės būtina pabrėžti, kad daugumoje tirtų savivaldybių tik apie pusę teikiamų administracinių paslaugų yra perkeltos į elektroninę erdvę. Iš tyrime dalyvavusių savivaldybių tik Kauno miesto ir Pagėgių rajono savivaldybėse visos administracinės paslaugos yra teikiamos internetu. Čia, vėl gi, galima išskirti Kauno miesto savivaldybę, padariusią didžiausią pažangą, kadangi didžioji dalis perkeltų administracinių paslaugų yra 3 – 4 brandos lygio.



11 pav. Administracinių paslaugų perkėlimo į elektroninę erdvę pasiskirstymas pagal savivaldybes

Savivaldybėms teikiant administracines paslaugas ne elektroniniu būdu atsiranda kiti asmens duomenų apsaugos reikalavimai. Kadangi paslaugos teikimo metu atsiranda popieriniai dokumentai, kuriuos būtina saugoti pagal atitinkamas taisykles:

„Kitas aspektas – užtikrinamas duomenų kaupimas ir archyvavimas, kad duomenys nebūtų prarasti <...> Archyvams yra taikomi papildomi specialūs reikalavimai“ (S1).

„Byloms, kuriose saugomi asmenų duomenys, taikoma griežta apskaita; jos saugomos papildomas fizines apsaugos priemones turinčiose patalpose (ne pirmame aukšte; turinčiose patikimesnes užraktų sistemas ir pan.). Bylos, kuriose kaupiami asmenų duomenys, naikinamos laikantis nustatytų tvarkų dokumentų naikikliais (jokiu būdu nepriduodamos makulatūros surinkėjams)“ (S2).

<..> „popieriniai dokumentai, kuriuose yra asmens duomenų saugojami seifuose bei užrakinamose metalinėse spintose, o pasibaigus jų saugojimo terminams yra perduodami saugoti į valstybės archyvus teisės aktų nustatyta tvarka“ (S5).

„Kiekvienas registras, kuriame yra saugomi dokumentai turi tam tikras taisykles, kuriose nurodytas saugojimo laikas, kokiomis priemonėmis užtikrinamas duomenų saugumas, kai dokumentai turi būti sunaikinami“ (S6).

Dokumentų saugojimo ir saugyklų įrengimo taisyklės nustato valstybės ir savivaldybių institucijų dokumentų saugojimo ir saugyklų įrengimo reikalavimus. Dokumentų ir archyvų įstatyme yra numatyta, kad valstybės ir savivaldybių institucijos privalo saugoti dokumentus patikimoje ir saugioje aplinkoje, įvertindami galimus rizikos veiksnius. Už numatytų reikalavimų laikymąsi yra atsakingas institucijos vadovas.

Savivaldybės, teikdamos administracines paslaugas neelektroniniu būdu vis vien naudojasi tam tikromis sistemomis: MASIS, SPIS, INFOSTATYBA, MEPIS, GIS ir kt. *„Administracinės paslaugos yra teikiamos su tam tikra sistema, kuri kaupia duomenis, vėliau yra sukuriamos duomenų bazės, kur duomenys yra archyvuojami ir šifruojami“ (S1).* Dažniausiai skirtingomis sistemomis naudojasi atitinkamų skyrių specialistai – jie ir yra atsakingi, kad teikiant gyventojui administracinę paslaugą būtų užtikrinta asmens duomenų apsauga ir neįvyktų incidentai. Vėliau minėtomis sistemomis surinkti duomenys yra sisteminami ir archyvuojami serveriuose:

„Informacinėse sistemose saugomų duomenų apsaugai taip pat taikomos sustiprintos fizinės apsaugos priemonės – kompiuterinės darbo vietos įrengiamos papildomai apsaugotose patalpose, kurios saugomos apsaugos signalizacijos; taikomos papildomos programinės įrangos apsaugos priemonės“ (S2).

<...> „tai prieigų prie informacijos ribojimas, slaptažodžių, elektroninių autentifikavimo priemonių naudojimas prisijungimui prie informacinių sistemų, kuriose naudojami asmens duomenys“ (S3).

Serveriams taip pat yra taikomi saugumo reikalavimai, tačiau mažai tikėtina, kad visos Lietuvos savivaldybės turi galimybę užtikrinti visus keliamus saugumo reikalavimus:

„Dėl pačių dokumentų kopijų saugojimo, yra specialūs reikalavimai serveriams. Pati VPK politika yra ta, kad savivaldybės nebeturėtų tokių serverinių, nebekauptų pas save duomenų, nes apsaugojimas nėra pas mus maksimalus, koks tūrėtų būti. O viską perkelti į vadinamus debesis“ (S1).

Technologinė pažanga turėjo didelės įtakos duomenų generavimui, kaupimui ir tolesniam naudojimui: *„Duomenys jau seniai nebetvarkomi popierinėse laikmenose, tai yra galingos, tarpusavyje integruotos ir realiame laike besikeičiančios duomenimis informacinės sistemos“ (A1).* Žvelgiant iš perspektyvų, tai ilgainiui kuriamos technologijos turėtų būti prieinamos vis plačiau. Taigi, viešojo administravimo institucijos, tame tarpe ir savivaldybės, turės galimybę atsisakyti perteklinio duomenų kaupimo, perkeliant juos į minėtus debesis.

Didžioji dalis informantų teigė, kad administracinėms paslaugoms teikiamoms tiek elektroniniu būdu, tiek neelektroniniu būdu yra taikomos tos pačios ar panašios saugumo priemonės. To priežastis, kad teikiant administracinę paslaugą ir neelektroniniu būdu, duomenys patenka į ankščiau minėtą dokumentų valdymo sistemą:

„Laikoma, kad visos naudojamos sistemos yra Tauragės rajono savivaldybės vienos informacinės sistemos posistemės, kurioms taikomi tie patys saugumo principai (pagal patvirtintus duomenų saugos nuostatus). Taigi, duomenys tvarkomi, lyg tai būtų viena bendra sistema“ (S1).

„Asmens duomenų apsauga vykdoma tais pačiais būdais, kuriuos išvardinau pirmame punkte“ (S2).

„Apsaugos priemonės tos pačios naudojamos tiek paslaugom teikiamoms įprastai, tiek el. būdu, kadangi įprastai teikiamos paslaugos vis tiek patenka į vidines informacines sistemas, tokias kaip Dokumentų valdymo sistema“ (S3).

„Šilalės rajono savivaldybės administracijos gauti ir parengti dokumentai yra rengiami ir apskaitomi dokumentų valdymo sistemoje „Kontora“ (S5).

„ <...> asmens duomenims, kurie tvarkomi teikiant paslaugas automatiniu būdu, taikoma ta pati apsauga, kaip ir visiems asmens duomenims, kurių valdytoja yra KMSA“ (S4).

Pagrindinės priemonės, susijusios su asmens duomenų apsauga yra: *„elektroniniams dokumentams taikomos saugos priemonės yra informacinių sistemų saugumą užtikrinančios priemonės, sakykim protokolai, ugniasienės ir kita programinė įranga“ (A1).* Tačiau kiekviena institucija turi visišką diskrecijos laisvę, pasirinkti techninius įrankius, kuriais bus užtikrinama asmens duomenų apsauga. Nepaisant suteikiamos laisvės, priemonės turi atitikti bendruosius reikalavimus techninėms ir organizacinėms priemonėms:

„Patį techninį įrankį renkasi duomenų valdytojas, pagal savo galimybes. Tai kas turi daugiau lėšų renkasi geresnį įrankį, kas neturi, aišku prastesnį. Tai yra visiška diskrecijos laisvė, kaip duomenų valdytojas tai daro. Išskyrus bendruosius reikalavimus organizacinėms ir techninėms priemonėms, kur aiškiai pasakyta, ką privalu užtikrinti“ (A2).

Kaip matoma, finansiniai ištekliai turi didžiausią įtaką saugumo priemonių pasirinkimui. Tačiau finansiniai ištekliai viešojo administravimo įstaigose yra riboti: *„viešajam sektoriui didesnė problema – lėšų stygius“ (A1).*

> *„<...> visada reikalaujama užtikrinti kaip įmanoma didesnes saugumo priemones. Bet mes suprantame, kad viešojo administravimo institucijos turi ribotą biudžetą ir paprastai tokiam dalykui, kaip kibernetinis saugumas, kaip atskirai sričiai nėra skiriama lėšų. <...> tai yra didelė problema“ (A2).*

Analizuojant asmens duomenų apsaugos priemones taikomas elektroniniu būdu teikiamoms administracinėms paslaugoms svarbu apžvelgti patį paslaugų perkėlimo procesą. Dalis Lietuvos savivaldybių administracines paslaugas į elektroninę erdvę jau buvo perkėlusios prieš 2012 m. VRM pradėtą vykdyti projektą „Centralizuotos viešųjų ir administracinių paslaugų sistemos kūrimas ir diegimas įgyvendinant vieno langelio principą“. Todėl administracinės paslaugos yra matomos paslaugų kataloge, bet yra teikiamos individualiai per savivaldybių sukurtas platformas:

> *„Taigi, mes teikiame e.paslaugas per savo savivaldybės platformą, kuri yra susieta ir su dokumentų valdymo sistema. Per sistemoje www.lietuva.gov.lt ir elektroninius valdžios vartus taip pat galima rasti Jurbarko savivaldybės teikiamas administracines paslaugas, tačiau šioje vietoje matomi it paslaugų aprašymai, pasirinkus jas yra nukreipiama į savivaldybės svetainę. Jurbarkas, Klaipėda, Kaunas ir Vilnius, šių miestų savivaldybės teikia administracines paslaugas individualiai“ (S6).*

Iš pateiktų duomenų matyti, kad dar prieš įvykstant centralizuotam projektui Jurbarko rajono, Klaipėdos, Kauno ir Vilniaus miestų savivaldybės jau buvo sukūrusios atitinkamas platformas savivaldybių internetinėse svetainėse, kuriose gyventojai turėjo galimybę gauti administracines paslaugas. Nors bendrai pati projekto idėja nėra vertinama blogai:

„Pačio projekto idėja buvo tokia, kad savivaldybė turi DVS (dokumentų valdymo sistema) ir prie šio modelio atsiranda PVS (paslaugų valdymo sistema). Tai reiškia, kad valdomi tiek dokumentai, tiek paslaugos, kurios tinkamai aprašytos. Iš PVS duomenys toliau keliauja į paslaugų katalogą (www.lietuva.gov.lt), jeigu ten viskas gerai ir savivaldybė nedirba su savo PVS – jungiasi tiesiai, tai tiesiai kataloge suveda paslaugas ir jeigu viskas gerai jos automatiškai yra publikuojamos“ (S1).

Tačiau strigo pats projekto įgyvendinimas, nebuvo atsižvelgiama į jau pažengusias šioje srityje savivaldybes:

„Čia įvyko didelis nesusikalbėjimas. <...> Galvojome, kad bus per e.valdžios vartus bus sukurtos tam tikros nuorodos į mūsų teikiamas paslaugas, bet viso šito nebuvo padaryta ir likome nuošalyje. E.valdžios vartuose parašyta, kad savivaldybė paslaugas teikia, bet tai daro tik per savo svetainę. Na gavosi kaip gavosi“ (S6).

Ir tai ne pagrindinė problema. Valstybės audito ataskaitos duomenimis (2014, p. 16-17) tuo metu, kai buvo fiksuotas šio projekto įgyvendinimas buvo užpildyta apie 60 proc. planuotų paslaugų aprašų, 22 institucijos ir įstaigos nepateikė administracinių paslaugų aprašymų. To priežastis – nebuvo reglamentuotas įpareigojimas institucijoms teikti ir atnaujinti paslaugų aprašus, reikalingus paslaugų katalogui sudaryti.

„Ištiktųjų tokia situacija, kai vienos paslaugos yra vienur, kitos – kitus, tik kelia žmonėms sumaištį. Bet mes savo sukurto paslaugų teikimo modelio neatsisakysime, nes sistemos yra sujungtos, yra įdėtas įdirbis, be to nematome ir reikalo tai daryti“ (S6).

Šiuo metu Lietuvoje veikia 4 paslaugų katalogai: „Verslo vartai“, „Elektroniniai valdžios vartai“, „Prisijungusi Lietuva“ ir „Lietuvos paslaugų katalogas“. Katalogus koordinuoja skirtingos institucijos ar ministerijos. Viso proceso pasėkoje – nukenčia paslaugos gavėjas, kadangi sunku suprasti kokia savivaldybė, kokias paslaugas teikia. Aptinkama ir sisteminių klaidų. Lietuvos paslaugų kataloge (www.lietuva.gov.lt) yra publikuojamos savivaldybių teikiamos administracinės paslaugos, tačiau jos yra suvedamos automatiškai (pagal šablonus) todėl paslaugų aprašymuose aptinkama klaidų:

„Tačiau automatinis publikavimas neveikia, yra sudėtingas administravimas, kažkur fiziškai nespėjama, kažkur sistema sutrinka. Galutiniame variante paslaugų kataloge išpublikuotose administracinių paslaugų aprašymuose yra klaidų, prie e.paslaugų nesimato pilnų aprašymų, nors pati e.paslauga veikia tinkamai“ (S1).

Informantai įžvelgia ir tai, kad tuo laikotarpiu, kai vyko centralizuotas paslaugų perkėlimas buvo koncentruojamasi į būdus kaip tai padaryti ir kiti aspektai, kaip saugumas, suderinamumas, patogumas vartotojui buvo paliekami kiek nuošalyje.

„Ankščiau, galbūt, labiau buvo kreipiamas dėmesys į pačios paslaugos perkėlimą į elektroninę erdvę, bet saugumo pusė buvo paliekama e.paslaugos teikėjui ar institucijai, kuri naudosis e.paslauga. Bet ar jie užtikrins numatytus saugumo reikalavimus niekas negalėjo garantuoti“ (S1).

Didžioji dalis informantų teigė, kad už asmens duomenų saugumo užtikrinimą administracinių paslaugų teikimo metu yra atsakingi paslaugos teikėjai: *„Kai duomenys patenka į informacinės visuomenės plėtros komiteto sistemą ar VRM tai jie vadovaujasi savo patvirtintais duomenų saugumo nuostatais“ (S1), „<...> už saugumą atsakingi paslaugų tiekėjai“ (S7), „El. paslaugų saugumą užtikrina paslaugų teikėjai“ (S8).*

Vis dėl to informantai teigia, kad teikiant administracines paslaugas elektroniniu būdu, dažniausiai grėsmės yra susijusios su asmens identifikavimo pažeidimais:

„Teikiant administracines paslaugas el. erdvėje dažniausiai susiduriama su asmens identifikavimo pažeidimais. <...> Svarbiausia užtikrinti, kad neįvyktų duomenų vagystė, kad aplinka, kurioje yra suteikiama paslauga būtų draugiška ir kad žmogus galėtų prisijungti tada, kada jam reikia „(A1).

„Realiai, kas liečia saugumą, tai visas asmens identifikavimas vyksta per el. bankininkystę bei el. parašu, pastarosios yra pakankamai saugios priemonės. Identifikavus asmenį, toliau pateikiami papildomi duomenys kaip gyvenamoji vieta, el. paštas ir kt. Tai, šiuo atveju, kad paslaugą užsisakys kitas asmuo yra labai mažai tikėtina“ (S6).

„Šiuo atveju vartotojus per e.paslaugų teikimo procesą, nuo neteisėto duomenų pasisavinimo apsaugo vartotojo identifikavimas“ (S1).

Tačiau lyginant administracinę paslaugą teikiant elektroniniu ir neelektroniniu būdais ekspertai prioritetą saugumo prasme teikia elektroninei paslaugai: *„Valstybė žmogui teigdama paslaugas ją teikia arba elektroniniu arba popieriniu būdu. El. paslauga, mano manymu, yra saugesnė“ (A1).* Svarbus aspektas ir tai, kad savivaldybės skiria dėmesį ne tik techninėms apsaugos priemonėms, bet ir informuoja darbuotojus apie galimas grėsmes naudodami: *prevencinės priemonės skirtas darbuotojams (S1).* Būtina nuolat šviesti darbuotojus, laiku perspėti apie kibernetinėje erdvėje esančius pavojus ir grėsmių tendencijas, gerinti darbuotojų kibernetinio saugumo žinias, kadangi didelė dalis vis dar nesugeba įvertinti galimų veiksmų pasekmių. (NKC metinė ataskaita, 2016, p. 47). Prevencinių priemonių naudojimas, darbuotojų nuolatinis informavimas apie kintančią išorinę aplinką, galimas grėsmes gali stipriai sumažinti žmogiškosios klaidos galimybė, kuri visada išlieka:

„Kas priklauso nuo savivaldybės tai mes esame viską padarę, todėl bendrai asmens duomenų apsaugos situaciją vertinčiau gerai. Bet žmogiškasis faktorius visada lieka ir liks. <...>

žmogus ar institucijos darbuotojas turi būti supažindintas, kokios pasekmės dėl galimų jo veiksmų laukia“ (S6).

„Visada yra tikimybė, kad įvyks žmogiškoji klaida, pvz. kad netinkamai duomenys bus perduoti tarp institucijų, policininkas pasižiūrėjo informacinėje sistemoje ne tik įtariamojo duomenis, bet ir tarkim kaimyno“ (A1).

Vartotojai yra indikatorius. Tik jų elgesys parodo, yra pasitikėjimas elektroninėmis paslaugomis, arba jo nėra (Kibernetinio saugumo apžvalga, 2016, p. 46). Galima daryti prielaidą, kad sisteminės klaidos, didelis paslaugų katalogų skaičius mažina vartotojų pasitikėjimą e.paslaugomis. Apskritai mažesnėse arba regionuose esančiose savivaldybėse yra gana mažas e.paslaugų naudojimo procentas:

„Elektroniniu būdu teikiamos paslaugos nėra labai populiarios, dažniausiai rajono gyventojai dėl paslaugų teikimo kreipiasi asmeniškai, atvykdami į savivaldybės administraciją ar seniūniją, arba atsiųsdami prašymus įprastu paštu. 2017 m. gruodžio 19 d. elektroniniu būdu kreipėsi tik 44 asmenys“ (S5).

„galime akcentuoti, kad gyventojai mažai naudojasi el. Paslaugomis, dažniausiai tiesiogiai atvyksta į savivaldybę“ (S8).

Tačiau mažam administracinių paslaugų naudojimuisi galima daryti ir kitas prielaidas, tokias kaip visuomenės senėjimas: *„Kaip žinia, esame senstanti tauta, tai didelė dalis asmenų tiesiog nenori paslaugos gauti el. būdu, todėl esame priversti paslaugas teikti paslaugas popieriniu būdu. Bet šiuo atveju neįžvelgčiau esminio kokybės skirtumo“ (A1).* Taip pat nemokėjimas ar nesugebėjimas naudotis esamomis informacinėmis technologijomis: *„tiesiog technologijos taip greitai sensta, o mes lėtai mokomės jomis naudotis, mūsų klientai taip pat“ (A1).*

3.4. Savivaldybių pasiruošimas taikyti Bendrąjį duomenų apsaugos reglamentą

Nuo 2018 m. gegužės 25 d. bus pradėtas taikyti Bendrasis duomenų apsaugos reglamentas. Ekspertai nurodo, kad duomenų apsaugos srityje reikės dėti didelį įdirbį visiems duomenų valdytojams: *„šioje srityje mums visiems reiks pasitemti ir pasimokyti vieniems iš kitų ir iš kitų šalių praktikos“ (A1).* Nors iki šiol buvo reikalaujama, kad kiekvienas incidentas susijęs su asmens duomenų apsaugos pažeidimais turi būti fiksuojamas ir pranešamas VDAI, šis aspektas bus vertinamas labai griežtai: *„<...> kiekvieną incidentą susijusį su asmens duomenimis reikės fiksuoti ir pranešti VDAI (S1), „viską, kas yra daroma su asmens duomenimis turės būti fiksuojama ir pateikiama duomenų priežiūros institucijai pareikalavus. Šie reikalavimai bus taikomi absoliučiai visiems*

duomenų valdytojams ir tvarkytojams“ (A1). Didžioji dalis informantų nurodė, kad po Bendrojo duomenų apsaugos reglamento įsigaliojimo bus griežčiau vertinamas asmens duomenų apsaugos užtikrinimas: *„naujojo reglamento taikymas skatins institucijas dar atidžiau dirbti asmens duomenų apsaugos srityje, tai palies ne tik e.paslaugas ar informacines sistemas, bet ir el.paštą, popierinius dokumentus (S6).*

VDAI savo ruoštu deda visus turimus resursus, kad pokyčių valdymas viešojo administravimo institucijose vyktų kuo sklandžiau. Tam yra parengtos įvairios priemonės: *„kalbant apie pasiruošimą, inspekcija parengė metodinę medžiagą, kad institucijoms ir įstaigoms būtų lengviau pasiruošti naujovėms. Organizuojame daug renginių ir seminarų, tame tarpe ir savivaldybėms, kadangi sulaukiame daug klausimų.* Informantai nurodė, kad pagrindinės savivaldybėse naudojamos pasiruošimo priemonės – įgyvendinamųjų teisės aktų atnaujinimas, papildomas finansavimas duomenų apsaugos sričiai bei bendradarbiavimas su VDAI – vadovaujamasi parengta metodika, dalyvavimas organizuojamose seminaruose ir mokymuose.

7 lentelė. Savivaldybių pasiruošimas Bendrojo duomenų apsaugos reglamento taikymui

Kategorija	Subkategorija	Citata
Lietuvos savivaldybių pasiruošimas asmens duomenų apsaugos reformai	Įgyvendinamųjų teisės aktų bazės atnaujinimas	*<...> „keisis ir nacionaliniai teisės aktai, todėl, atsižvelgiant į Bendrojo duomenų apsaugos reglamento ir nacionalinių teisės aktų bei VDAI pateiktus išaiškinimus ir nurodymus, KMSA turės būti įgyvendintos naujos nuostatos, susijusios su duomenų tvarkymu ir asmens teisių įgyvendinimu bei pakeisti teisės aktai, užtikrinantys teisėtą asmens duomenų tvarkymą“ (S4).* *<...> „Savivaldybės administracijoje pirmiausiai bus peržiūrėtos visos tvarkos reglamentuojančios duomenų apsaugą, tvarkos ir taisyklės ir parengtos naujos atitinkančios galiojančius teisės aktus“ (S5).*
	Skiriamas papildomas finansavimas asmens duomenų apsaugos sričiai	*<...> „savivaldybėje didėja išlaidos IT sričiai ir saugumui bendrai“ (S1).* *<...> „Savivaldybė tam nusimatė 2018 m. lėšų papildomos apsaugos priemonėms įsidiegti, tačiau kokios konkrečiai jos bus, dabar negalime atsakyti“ (S2).*
	Naudojama VDAI parengta metodinė medžiaga	*<...> „šiais metais vykome į VDAI organizuotus mokymus, naudojamės metodine priemone, kai prireikia komunikuojame tiesiogiai“ (S1).* *<...> „sekame VDAI parengtas metodines priemones ir rekomendacijas. Atsižvelgiant į jas stengiamės atlikti būtinus veiksmus“ (S5).*

Kaip viena iš svarbiausių problemų, trukdančių pasiruošimui įvardijami vis dar nepatvirtinti VDAI parengti teisės aktų projektai:

<...> „Šiam reglamentui ruošiamės jau seniai. Pradžia yra padaryta, duomenų saugos taisyklės atnaujintos, įdirbis yra. Kitas dalykas, kol kas negalime iki galo pasiruošti, nes VDAI

yra paruošusi įstatymo pakeitimo projektą. Taigi dar nemažai teisės aktų guli vyriausybės stalčiuose. Tai mus kol kas ir stabdo“ (S6).

Vienas pagrindinių pokyčių – tai institucijose turės atsirasti duomenų apsaugos pareigūnas. Informantai šį pokyti vertina dvejopai. Dalis informantų šį pokyti vertina teigiamai, kadangi institucijose atsiras konkretus žmogus, kurio veiklos sritis bus asmens duomenų apsauga:

„ <...> tai tas žmogus, kurio dabar nėra, IT specialistai rūpinasi, kad vartotojai dirbtų tvarkingai, būtų apsaugota kompiuterinė darbo vieta ir pan. VPK rūpinasi, kad e.paslaugos būtų tinkamai teikiamos, paslaugos teikėjai, darbuotojai rūpinasi, kad paslauga būtų kuo greičiau suteikta. Bet visi būdai kaip tai daroma, niekas iki šiol netikrino.

Kiti – išreiškia susirūpinimą, dėl duomenų apsaugos pareigūno įsiliejimo į organizacijos veiklą: *„kol kas dar neaišku ir koks bus asmens duomenų apsaugos pareigūno statusas ir kaip jis įsilies į instituciją <...>“ (S6).* Tačiau dažnu atveju informantai duomenų apsaugos pareigūno statusą supranta klaidingai, jis turėtų būti patariamasis balsas institucijose:

„*Pareigūnas, nesupraskite klaidingai, tai turėtų būti labiau patarėjas, kuris turėtų išmanyti organizacijos funkcijas. Tai tokia tarpinė tarp vadovybės, žmogaus, inspekcijos ir darbuotojų. Tai turėtų būti universalus žmogus, turėti pakankamai ekspertinių žinių. Tai nereiškia, kad tai būtinai turėtų būti teisininkas, na tiesiog... žmogus, išmanantis organizacijos veiklą <...> (A2).*

Kaip labiausiai komplikuota asmens duomenų apsaugos pareigūno savybė išskiriama – nepriklausomumas: *„nepriklausomumas – sunkiausiai užtikrinama dalis, nes nėra visiškai nepriklausomo darbuotojo dirbančio įstaigoje. Galbūt organizacijos samdymas būtų patikimesnis būdas, tačiau gerokai brangesnis (A1).*

Reglamente taip pat nurodomas naujas aspektas – duomenų šifravimas, kuris stipriai padidins duomenų apsaugos užtikrinimą, kadangi: *„vienas dalykas, kai duomenys yra prarandami, kitas – kai duomenys yra prarandami, bet jais negali pasinaudoti“*. Įgyvendinus šią nuostatą, bus padarytas pagrindinis įdirbis Bendrojo duomenų apsaugos reglamento taikymui.

Apibendrinant tyrimą galima teigti, kad asmens duomenų užtikrinimą Lietuvoje lėmė ES priimti teisės aktai. Didžiausią įtaką tolesnei asmens duomenų apsaugos užtikrinimo raidai Lietuvoje turėjo direktyva „Dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo“ (1995). Jau sekančiais metais buvo priimtas Asmens duomenų teisinės apsaugos įstatymas – pagrindinis teisinis dokumentas, užtikrinantis asmens duomenų apsaugą Lietuvoje, vėliau įkurta ir VDAI. Tyrimas parodė, kad VDAI funkcijos ilgainiui išsiplėtė, institucijos kompetencijos numatytos kibernetinio saugumo įstatyme, informacinių išteklių įstatyme. Nepaisant teisinės aplinkos pokyčių, VDAI funkcijų ir galios išplėtimo, asmens duomenų apsaugos užtikrinimo sistemoje aptinkama klaidų.

Lietuvos savivaldybės teikdamos administracines paslaugas vadovaujasi asmens duomenų užtikrinimą reglamentuojančiais teisės aktais ir patvirtintais vidaus dokumentais, taip pat bendrosiomis priemonėmis, tokiomis kaip slaptažodžiai, antivirusinės programos, papildoma programinė įranga, saugaus valstybinio duomenų perdavimo tinklas. Šiuo atveju būtina pabrėžti tai, kad institucijos vadovaujasi „Bendraisiais reikalavimais organizacinėms ir techninėms asmens duomenų saugumo priemonėms“, tačiau įrankius saugumui užtikrinti renkasi pačios, atsižvelgdamos į turimus finansinius išteklius. Administracinės paslaugos Lietuvos savivaldybėse yra teikiamos tiek elektroniniu, tiek neelektroniniu būdu. Teikiant administracines paslaugas neelektroniniu būdu yra vadovaujamasi dokumentų ir archyvo įstatyme įvardijamomis dokumentų saugojimo nuostatomis. Tačiau teikiant paslaugą neelektroniniu būdu vis vien yra naudojamasi įvairiomis sistemomis, kaip SPIS, MEPIS, GIS ir kt. o visi gauti ir parengti dokumentai yra rengiami ir apskaitomi savivaldybių dokumentų valdymo sistemose. Dėl šių priežasčių, asmens duomenų apsaugai užtikrinti taikomos priemonės yra panašios tiek administracinę paslaugą teikiant elektroniniu, tiek neelektroniniu būdu. Teikiant administracinę paslaugą elektroniniu būdu yra naudojamasi valstybės informacinių išteklių sąveikumo platforma. Tyrimas parodė, kad centralizuotas paslaugų perkėlimas į elektroninę erdvę buvo komplikuotas, projekto metu nebuvo atsižvelgta į šioje srityje pažengusias savivaldybes, sukurti paslaugų katalogai yra nepatogūs vartotojui. Nors administracinės paslaugos yra teikiamos tinkamai, tačiau aptinkama klaidų paslaugų aprašymuose, tai dar labiau klaidina vartotoją. Todėl elektroniniu būdu teikiamos administracinės paslaugos yra nepopuliarios didžiojoje dalyje tirtų savivaldybių.

Pasiruošimas Bendrojo duomenų apsaugos reglamento taikymui Lietuvos savivaldybėse vyksta skirtingai. Dalis savivaldybių apskritai tik šiuo metu pradėjo dirbti asmens duomenų apsaugos užtikrinimo srityje. Tačiau didžioji dalis yra padariusi viską, kas reikalinga prieš įsigaliojant Bendrojo duomenų apsaugos reglamento taikymui, tačiau imtis tolesnių veiksmų jas stabdo Vyriausybėje įstrigę teisės aktų projektai. Iš esmės savivaldybėms šiuo metu neturi pakankamai žinių, kaip reikės taikyti naujai įsigaliosiančias reglamento nuostatas. Daugiausiai klausimų kyla dėl duomenų apsaugos pareigūno, kuris privalės būti kiekvienoje institucijoje. Tačiau šis pasikeitimas didžiojoje dalyje savivaldybių vertinamas teigiamai, kadangi buvo įžvelgiamas tokio asmens trūkumas, kadangi asmens duomenų apsauga dažniausiai buvo „primesta“ kuriam nors iš darbuotojų (dažniausiai IT specialistams). Žinių trūkumą savivaldybės bando kompensuoti dalyvaudamos VDAI organizuojamuose seminaruose ir mokymuose, taip pat naudojasi VDAI sukurta metodika, kuri skirta palengvinti Bendrojo duomenų apsaugos taikymo pasiruošimo procesui.

IŠVADOS

1. Asmens duomenų apsauga yra specifinė sritis, kuri yra stipriai veikiama išorinės aplinkos pokyčių, susijusių su globalizacija, konvergencija ir multimedija. Sparti technologinė pažanga lėmė, kad elektroninių platformų naudojimas tampa įprastu reiškiniu, asmeninių duomenų „bankai“ tampa vis išsamesni ir sudėtingesni, o sukuriamų skaitmeninių duomenų mąstai smarkiai išaugo. To pasėkoje asmeniniai duomenys įgavo dar didesnę reikšmę, todėl būtina užtikrinti vieną iš pamatinių žmogaus teisių – asmens duomenų apsaugą.
2. Ilgą laiką asmens duomenų apsauga neturėjo teisinio reguliavimo nei vienoje šalyje. Asmens teisę į privatumą konstatavo Europos žmogaus teisių ir pagrindinių laisvių konvencija. Tik nuo 1980 metų imtos taikyti tarptautinės priemonės. Vienas pagrindinių teisinių dokumentų reglamentuojančių asmens duomenų apsaugą Europos Sąjungos lygmeniu yra 1995 m. duomenų apsaugos direktyva, kurioje numatytos pagrindinės asmens duomenų apsaugą užtikrinančios taisyklės ir principai. Duomenų apsaugos direktyvoje numatyti reikalavimai užtikrinti asmens duomenų apsaugą perduodant duomenis į trečiąsias šalis, sukėlė daug nesusipratimų dėl „tinkamumo“ standarto. Labiausiai tai palietė ES ir JAV santykius, kadangi šis reikalavimas daugybei organizacijų nešė finansinius nuostolius. 2018 m. gegužės 25 d. bus pradėtas taikyti Bendrasis duomenų apsaugos reglamentas turės įtakos visiems ES duomenų valdytojams ir tvarkytojams, o asmens duomenų apsaugos užtikrinimo reikalavimai bus harmonizuoti ES lygmeniu.
3. Šiuo metu itin pabrėžiama atvirųjų duomenų svarba, pakartotinis viešojo sektoriaus informacijos naudojimas, viešojo administravimo institucijų integralumas. Kadangi viešasis sektorius tarnauja visuomenei, todėl su asmenimis susijusių duomenų generavimo mastai yra didesni nei kituose sektoriuose sektoriuje. Saugumo rizikos vertinimas ir valdymas viešajame sektoriuje yra labai svarbus asmens duomenų saugumui. Tinkamai identifikavus grėsmes, galima pasirinkti tinkamas priemones asmens duomenų saugumui užtikrinti. Duomenų valdytojas turi atitikti specialius reikalavimus, taikomus duomenų apdorojimui ir tvarkomiems duomenims, pabrėžiamas duomenų tvarkymas teisėtais tikslais.
4. Nacionaliniu lygiu aukščiausią galią turintis teisinis dokumentas, kuris gina žmogaus teisę į privatumą yra Lietuvos Respublikos Konstitucija. Asmens duomenų apsaugos teisinė sistema Lietuvoje funkcionuoja remiantis asmens duomenų teisinės apsaugos įstatymu. Tai pagrindinis įstatymas, kuriuo vadovaujantis yra užtikrinama asmens duomenų apsauga. Asmens duomenų apsauga apima didelę dalį gyvenimo sričių, tai bendrai atsispindi Lietuvos Respublikos

įstatyminėje bazėje – reklamos, elektroninių ryšių, informacinės visuomenės paslaugų, kibernetinio saugumo įstatymuose, kuriuose yra numatyta asmens duomenų apsauga.

5. Asmens duomenų teisinės apsaugos įstatyme yra numatyti būdai, kuriais privaloma užtikrinti asmens duomenų apsauga. Įstatymas nenumato priemonių, todėl savivaldybės priemones renkasi atsižvelgdamos į finansinius išteklius, kurie šioje institucijoje yra riboti. Lietuvos savivaldybės teikdamos administracines paslaugas vadovaujasi asmens duomenų užtikrinimą reglamentuojančiais teisės aktais ir patvirtintais vidaus dokumentais, taip pat bendrosiomis priemonėmis, tokiomis kaip slaptažodžiai, antivirusinės programos, papildoma programinė įranga bei saugaus valstybinio duomenų perdavimo tinklais.
6. Įstatyminė bazė Lietuvoje pakankamai reglamentuoja asmens duomenų apsaugą, tačiau dalis savivaldybių tiesiog nedirbo šioje srityje, kurios vis dar neturi patvirtintų vidaus dokumentų, saugos nuostatų ir kt. Šie trūkumai išryškėjo priėmus Bendrąjį duomenų apsaugos reglamentą, kuriam įsigaliojus asmens duomenų apsauga bus dar griežčiau reguliuojama.

REKOMENDACIJOS

Atsižvelgiant į surinktus duomenis ir atliktą tyrimą suformuotos rekomendacijos valstybinei duomenų apsaugos inspekcijai, Lietuvos savivaldybėms ir Informacinės visuomenės plėtros komitetui.

1. Valstybinei duomenų apsaugos inspekcijai siūloma gerinti institucinį bendradarbiavimą ir komunikaciją tarp viešojo valdymo sektorių. Šiuo metu asmens duomenų apsaugos srityje dirba krašto apsaugos, susisiekimo ir vidaus reikalų ministerijos. Todėl veiklos sritys tarp ministerijų persipina, skirtingais tikslais ir priemonėmis institucijos renka duomenis apie asmens duomenų tvarkymą ir apsaugą Lietuvoje, tačiau nesuderindamos tarpusavio veiksmų, neužtikrina renkamų duomenų tolesnio panaudojimo.
2. Lietuvos savivaldybėms siūloma administracinių paslaugų teikimo metu atsižvelgti į paslaugos teikimo pobūdį (elektroninis/neelektroninis), pagal tai parinkti atitinkamas asmens duomenų saugumą užtikrinančias priemones. Teikiant administracines paslaugas elektroniniu būdu nusimatyti saugiklius, kurie užtikrintų tokiu būdu teikiamos paslaugos saugumą, o ne palikti asmens duomenų apsaugos užtikrinimą tik paslaugos tiekėjo atsakomybėje. Taip pat didinti elektroniniu būdu teikiamų administracinių paslaugų teikimą, kadangi tokiu būdu teikiama paslauga laikoma saugesne ir kyla mažesnė žmogiškosios klaidos grėsmė.
3. Informacinės visuomenės plėtros komitetui siūloma pašalinti valstybės informacinių išteklių sąveikumo platformoje (VIISP) tyrimo metu identifikuotas klaidas susijusias su administracinių paslaugų aprašymais. Taip pat susieti tų savivaldybių elektroninių administracinių paslaugų teikimo platformas, kurios dar prieš centralizuotai vykūsį administracinių paslaugų perkėlimą buvo pažengusios šioje srityje. Taip vartotojai galės visas savivaldybių administracines paslaugas rasti viename kataloge, o paslaugų teikimo metu nebus nukreipiami į papildomas savivaldybių sistemas. Sistemos patobulinimai leis vartotojams lengviau rasti norimas administracines paslaugas, patogiau naudotis paslaugų katalogu. Tikėtina, kad patogus vartotojui paslaugų katalogas, ilgainiui padidins elektroninėmis administracinėmis paslaugomis teikiamų paslaugų skaičių.
4. Visiems duomenų valdytojams ir tvarkytojams prieš įsigaliojant Bendrajam duomenų apsaugos reglamentui siūloma atnaujinti vidaus tvarką reguliuojančius dokumentus. Taip pat siūloma perskirstyti biudžeto lėšas, numatant papildomą finansavimą asmens duomenų apsaugai, kadangi papildomų sąnaudų reikalaus duomenų apsaugos pareigūnas. Duomenų valdytojams ir tvarkytojams rekomenduojama atnaujinti programinę įrangą, kuri leistų šifruoti saugomus duomenis, taip užtikrinant, kad įvykus incidentui prarasti asmens duomenys nebus panaudojami neteisėtiems tikslams.

LITERATŪRA

1. Abdulrauf, L. A., Fombad,Ch. M. (2016). The African Union's data protection Convention 2014: a possible cause for celebration of human rights in Africa?Journal of Media Law
2. Administracinių paslaugų teikimo vieno langelio principu būklės viešojo valdymo institucijose analizė. [žiūrėta: 2017-12-07]. Prieiga internetu: file:///C:/Users/proje/Downloads/Aptarnavimo_bukles_analize_9.pdf .
3. Agarwal, A. K. (2005). Legal aspects of data protection. *Paradigm*, 9, 1: p. 98-101
4. Asmens duomenų teisinės apsaugos įstatymo komentaras. [žiūrėta: 2017-10-07]. Prieiga internetu: http://www.ada.lt/images/cms/File/komentaras%20adtai.pdf
5. Barcevičius, E. (2008). Viešasis valdymas ir informacinės technologijos. Naujo institucinio modelio link. Politologija, 1(49), 85-120.
6. Chen, H., Chiang, R. H., Storey, V. C. (2012). Business intelligence and analytics: From big data to big impact. MIS quarterly, 36(4).
7. Civilka, M. (2001). *Asmens duomenų apsauga tarptautinėje ir EB teisėje.* Vilnius: Vilniaus universitetas.
8. Civilka, M., Šlapimaitė, L. (2015). Asmens duomenų samprata elektroninėje erdvėje. *Teisė*, *96*(96), 126-148. [žiūrėta: 2017-10-13]. Prieiga internetu: http://www.zurnalai.vu.lt/teise/article/view/8761
9. Dawes, S. S., Cresswell, A. M., & Pardo, T. A. (2009). From "need to know" to "need to share": Tangled problems, information boundaries, and the building of public sector knowledge networks. *Public Administration Review*, *69*(3), 392-402.
10. Domarkas, V., Masionytė, R. (2015). Viešojo administravimo modernizavimo galimybės globalizacijos sąlygomis. [žiūrėta: 2017-10-07]. Prieiga internetu: https://repository.mruni.eu/pdfpreview/bitstream/handle/007/13667/2421-5166-1-SM.pdf?sequence=1
11. ENISA. Guidelines for SMEs on the security of personal data processing. [žiūrėta: 2017-12-07]. Prieiga internetu: https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing
12. Europos duomenų apsaugos teisinis vadovas. (2014). [žiūrėta: 2017-10-11]. Prieiga internetu: https://www.coe.int/en/web/data-protection/home
13. Gantz, J., Reinsel, D. (2012). The digital universe in 2020: Big Data, Bigger Digital Shadows, and Biggest Growth in the Far East. [žiūrėta: 2017-10-29]. Prieiga internetu: http://www.emc2.my/collateral/analyst-reports/idc-the-digital-universe-in-2020.pdf
14. Gaulė, E. (2014). Sumanus viešasis valdymas: samprata ir dimensijos. [žiūrėta: 2017-10-23]. Prieiga internetu: https://www.ceeol.com/search/article-detail?id=222320
15. Greenleaf, G. (2015). Global data privacy laws 2015: Data Privacy Authorities and Their Organisations. žiūrėta: 2017-10-23]. Prieiga internetu: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2641772
16. Informacinės visuomenės plėtros komitetas prie Susisiekimo ministerijos. [žiūrėta: 2017-11-17]. Prieiga internetu: https://ivpk.lrv.lt/lt/veiklos-sritys-1/viisp

17. Informacinės visuomenės plėtros 2014–2020 metų programa „Lietuvos Respublikos skaitmeninė darbotvarkė“. [žiūrėta: 2017-10-07]. Prieiga internetu: https://www.e-tar.lt/portal/lt/legalAct/dbd546f0b04011e39a619f61bf81ad0a
18. Informatikos ir ryšių departamento nuostatai. [žiūrėta: 2017-12-07]. https://www.e-tar.lt/portal/lt/legalAct/TAR.49172C46C223/EkbBUtigyX
19. Interneto vartotojai pasaulyje (gyvoji statistika). [žiūrėta: 2017-11-07]. Prieiga internetu: http://www.internetlivestats.com/internet-users/
20. Jastiuginas, S. (2011). Informacijos saugumo valdymas Lietuvos viešajame sektoriuje. [žiūrėta: 2017-10-15]. Prieiga internetu: http://www.zurnalai.vu.lt/informacijos-mokslai/article/view/3137
21. Klijn, E. H. (2002). Governing Networks in the Hollow State: Contacting-out, Process Management or a Combination of the Two. *Public Management Review*, 2(2), 66–149.
22. Kibernetinio saugumo apžvalga. [žiūrėta: 2018-01-03]. Prieiga internetu: http://apzvalga.eu/images/kibernetinis_saugumas.pdf
23. Kiškis, M., Petrauskas, R., Rotomskis, I., Štitilis, D. (2006). Teisės informatika ir informatikos teisė. *Vilnius: Mykolo Romerio universitetas*, p. 152-154.
24. Kiurienė, V. (2014). Viešojo valdymo pokyčiai ir jų įtaka vietos savivaldai. *Studies in Modern Society*, 167.
25. Lankauskas, M. (2007). Balansavimas tarp teisės į privatumą ir saviraiškos laisvės Europos žmogaus teisių teismo jurisprudencijoje. *Teisės problemos*, 2, 56.
26. Limba, T. (2009). Elektroninės valdžios paslaugų pakopų modeliai: jų lyginamoji analizė. [žiūrėta: 2017-10-03]. Prieiga internetu: http://www.zurnalai.vu.lt/files/journals/163/articles/3309/public/30-39.pdf
27. Lynskey, O. (2014) Deconstructing data protection: the 'added-value' of a right to data protection in the EU legal order. *International and Comparative Law Quarterly*, 63 (3). p. 569-597.
28. Long, W. J., Quek, M. P. (2011). Personal data privacy protection in an age of globalization: the US-EU safe harbor compromise. [žiūrėta: 2017-10-23]. Prieiga internetu: http://www.tandfonline.com/doi/abs/10.1080/13501760210138778
29. Malinauskaitė, I. (2015). Privatumas virtualiuose socialiniuose tinkluose kaip įstatymo saugoma vertybė. *Social Transformations in Contemporary Society*, 3, [žiūrėta: 2017-10-14]. Prieiga internetu: http://stics.mruni.eu/wp-content/uploads/2015/07/STICS_2015_3_115-127.pdf
30. Markauskas, L. (2015). Asmens duomenų apsaugos teisiniai aspektai ir problemos. Vilnius: UAB „Mokesčių srautas“.
31. McAfee, A., Brynjolfsson, E., Davenport, T. H. (2012). Big data: the management revolution. *Harvard business review*, 90(10), p. 60-68.
32. McDermott, Y. (2017). Conceptualising the right to data protection in an era of Big Data. *Big Data & Society*, vol. 4, 1.
33. Milė, R., Junevičius, A. (2013). Elektroninių viešųjų paslaugų teikimo ypatumai Šakių rajono savivaldybėje. *Viešoji politika ir administravimas*, 12(3).

34. Oficialioji statistika apie nusikalstamumą LR savivaldybėse (2017). [žiūrėta: 2017-11-17]. Prieiga internetu:https://www.ird.lt/lt/paslaugos/nusikalstamu-veiku-zinybinio-registro-nvzr-paslaugos/ataskaitos-1/nusikalstamumo-ir-ikiteisminiu-tyrimu-statistika-1/view_item_datasource?id=6455&datasource=16987
35. Pardo, T. A., Cresswell, A. M., Thompson, F., & Zhang, J. (2006). Knowledge sharing in cross-boundary information system development in the public sector. *Information Technology and Management*, *7*(4), 293-313.
36. Petraitytė, I. (2011). Asmens duomenų apsauga ir teisė į privatų gyvenimą. *Teisė, 80.*
37. Petrauskas, R. ir Selskaite, N. (2009). Viešojo sektoriaus informacijos pakartotinis panaudojimas: situacija Lietuvoje. Public administration.
38. Pearce, H. (2017). Big data and the reform of the European data protection framework: an overview of potential concerns associated with proposals for risk management-based approaches to the concept of personal data. p. 312-335.
39. Privacy and Human Rights Report (2006). [žiūrėta: 2017-11-13]. Prieiga internetu: http://www.worldlii.org/int/journals/EPICPrivHR/2006/PHR2006-The-2.html#fn38
40. Purtova N. (2015). The illusion of personal data as no one's property. *Law, Innovation and Technology*. No. 7. p.83-111.
41. Raipa, A. (2015). Viešoji politika ir viešasis administravimas: raida, struktūra ir sąveika. [žiūrėta: 2017-10-17]. Prieiga internetu: https://repository.mruni.eu/pdfpreview/bitstream/handle/007/13347/2543-5410-1-SM.pdf?sequence=1
42. Raipa, A., Laurišonienė, I. (2017). Kompleksinis naujojo viešojo valdymo pobūdis: klaipėdos miesto savivaldybės paslaugų teikimas. *Public administration.* p. 54-63.
43. Salamon, L., M. (2002). The New Governance and the Tools of Public Action: an Introduction. In *The Tools of Government: A Guide to the New Governance* (1–47). New York: Oxford University Press.
44. Sveklaitė, L., Stasiukynas, A. (2015). Sumanios visuomenės bruožai viešojo valdymo modernizavimo kontekste. *Jaunųjų mokslininkų darbai*, 2 (44).
45. Štitilis D., Pakutinskas P., Laurinaitis M., Dauparaitė I. (2011). Tapatybės vagystė elektroninėje erdvėje: socialiniai, elektroninio verslo ir teisinio reguliavimo aspektai. Vilniaus: Mykolo Riomerio universitetas.
46. Tidikis, R. (2003) *Socialinių mokslų tyrimų metodologija.* Vilnius: Lietuvos teisės universitetas.
47. Točickienė, N. (2003). Asmens duomenų apsaugos reglamentavimas Europos Sąjungos ir Lietuvos Respublikos teisėje. *Jurisprudencija*, *44*(36), p. 114-123.
48. Uddin, M. F., Gupta, N. (2014, April). Seven V's of Big Data understanding Big Data to extract value. [žiūrėta: 2017-10-29]. Prieiga internetu: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6820689
49. Valackienė, A., Trofimovas, V. (2015). Pokyčių komunikacija viešajame sektoriuje: tyrimo metodologinis konstruktas. *Organizacijų vadyba: sisteminiai tyrimai, 2015, nr. 73, p. 121-141*.
50. Valstybinė duomenų apsaugos inspekcija. [žiūrėta: 2017-10-25]. Prieiga internetu: https://www.ada.lt/go.php/lit/Veikla

51. Valstybinės duomenų inspekcijos metinė ataskaita. (2016) [žiūrėta: 2017-12-03]. Prieiga internetu: file:///C:/Users/Agn%C4%97/Downloads/VDAI2016m.veiklosataskaita20170323.pdf
52. Zaleskis, J. (2017). ES Bendrasis duomenų apsaugos reglamentas: reikšmė duomenų apsaugos teisei. Teisė, 103(103), 45-54.
53. Zins, C. (2007). Conceptual approaches for defining data, information, and knowledge. *Journal of the Association for Information Science and Technology*, *58*(4), 479-493.
54. Žiobienė, E. (2015). Aktualios konstitucinės teisės į privatų gyvenimą apsaugos problemos. [žiūrėta: 2017-10-14]. Prieiga internetu: https://repository.mruni.eu/pdfpreview/bitstream/handle/007/13311/3135-6596-1-SM.pdf?sequence=1

TEISĖS AKTAI

55. African Union Convention on Cyber Security and Personal Data Protection. [žiūrėta: 2017-10-25]. Prieiga internetu: https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection
56. Dokumentų saugojimo taisyklės. [žiūrėta: 2017-12-29]. Prieiga internetu: https://www.e-tar.lt/portal/lt/legalAct/TAR.2EBA39845DEE/BcenDbAWLS
57. Europos Sąjungos pagrindinių teisių chartija. [žiūrėta 2017-10-09]. Prieiga per internetą: http://europa.eu/legislation_summaries/justice_freedom_security/combating_discrimination/l33501_lt.htm
58. Europos sąveikumo sistema. Įgyvendinimo strategija. [žiūrėta: 2017-10-10]. Prieiga internetu: https://ec.europa.eu/transparency/regdoc/rep/1/2017/LT/COM-2017-134-F1-LT-MAIN-PART-1.PDF
59. Europos žmogaus teisių deklaracija 1948m. [žiūrėta: 2017-10-09]. Prieiga internetu :
60. https://www.e-tar.lt/portal/legalAct.html?documentId=TAR.181EDAC3A371
61. Informacinės visuomenės plėtros 2014–2020 metų programa „Lietuvos Respublikos skaitmeninė darbotvarkė“. [žiūrėta: 2017-11-10]. Prieiga internetu: https://www.e-tar.lt/portal/lt/legalAct/dbd546f0b04011e39a619f61bf81ad0a
62. Informacinės visuomenės politikos departamento nuostatai. [žiūrėta: 2017-12-10]. Prieiga internetu:http://sumin.lrv.lt/lt/struktura-ir-kontaktai/informacines-visuomenes-politikos-departamentas-1
63. Jungtinių Tautų generalinė asamblėja. Tarptautinis Pilietinių ir Politinių Teisių Paktas. [žiūrėta: 2017-10-09]. Prieiga internetu: https://www.e-tar.lt/portal/lt/legalAct/TAR.261D576EDC40
64. Komisijos komunikatas Europos Parlamentui ir Tarybai dėl „saugaus uosto“ nuostatų veikimo ES piliečių ir ES įsisteigusių bendrovių požiūriu (2013) Briuselis, 2013 11 27 COM(2013) 847
65. Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu. [žiūrėta: 2017-10-09]. Prieiga internetu: https://www.e-tar.lt/portal/lt/legalAct/TAR.A28CF120BC09
66. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas Nr. I-1374. TAR, 1996, Nr. 63-1479.
67. Lietuvos Respublikos asmens duomenų, tvarkomų vykdant policijos ir teisminį bendradarbiavimą bylose, teisinės apsaugos įstatymas Nr. XI-1336. TAR, 2011, Nr. 52-2511
68. Lietuvos Respublikos civilinis kodeksas, Žin., 2000 m., Nr. 74-2262
69. Lietuvos Respublikos dokumentų ir archyvo įstatymas Nr. IX-2084. TAR, 2004, Nr.57-1982.
70. Lietuvos Respublikos elektroninių ryšių įstatymas Nr. IX-2135. TAR, 2004, Nr. 69-2382.
71. Lietuvos Respublikos informacinės visuomenės paslaugų įstatymas Nr. X-614. TAR, 2006, Nr. 65-2380.
72. Lietuvos Respublikos kibernetinio saugumo įstatymas Nr. XII-1428, TAR, 2014, Nr. 20553
73. Lietuvos Respublikos Konstitucija. Žin., 1992, Nr. 33-1014

74. Lietuvos Respublikos pacientų teisių ir žalos sveikatai atlyginimo įstatymas Nr. I-1562. TAR, 1996, Nr. 115-4284
75. Lietuvos Respublikos reklamos įstatymas Nr. VIII-1871. TAR, 2000, Nr. 64-1937.
76. Lietuvos Respublikos viešojo administravimo įstatymas. Nr. X-736. Žin., 2006, Nr. 77-2975.
77. Pasiūlymas dėl Europos Parlamento rezoliucijos [žiūrėta: 2017-11-22]. Prieiga internetu: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2017-0178+0+DOC+XML+V0//LT#title1
78. Ryšių reguliavimo tarnybos nuostatai. [žiūrėta: 2017-12-22]. Prieiga internetu: http://www.rrt.lt/lt/administracine_23/nuostatai.html
79. Septynioliktosios Lietuvos Respublikos Vyriausybės programa [žiūrėta: 2017-11-09]. Prieiga internetu: https://www.e-tar.lt/portal/lt/legalAct/ed6be240c12511e6bcd2d69186780352
80. Valstybės informacinių išteklių sąveikumo platformos nuostatai. [žiūrėta: 2017-11-19]. Prieiga internetu: https://www.e-tar.lt/portal/lt/legalAct/1eafc1f04a6711e5a38cd6cdb94b0c51
81. Valstybinės duomenų apsaugos inspekcijos direktoriaus 2008 m. lapkričio 12 d. įsakymas Nr. 1T-71(1.12) „Dėl Bendrųjų reikalavimų organizacinėms ir techninėms duomenų saugumo priemonėms patvirtinimo“.
82. Valstybinio audito 2013 m. gruodžio 11 d. automatiniu būdu tvarkomų asmens duomenų apsauga ataskaita. TAR, 2013, Nr.VA-P-90-3-21.
83. 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, 1995, L 254
84. 1997 m. gruodžio 15 d. Europos Parlamento ir Tarybos direktyva 97/66/EB dėl asmens duomenų apdorojimo ir privatumo apsaugos telekomunikacijų sektoriuje. OL, 1997, L 344
85. 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje OL, 2002, L 184
86. 2006 m. kovo 15 d. Europos Parlamento ir Tarybos direktyva 2006/24/EB dėl duomenų, generuojamų arba tvarkomų teikiant viešai prieinamas elektroninių ryšių paslaugas arba viešuosius ryšių tinklus, saugojimo iš dalies keičiantis Direktyvą 2002/58/EB. OL, 2006, L 075
87. 2009 m. lapkričio 25 d. Europos Parlamento ir Tarybos direktyva 2009/136/EB iš dalies keičianti direktyvą dėl universaliųjų paslaugų ir paslaugų gavėjų teisių, susijusių su elektroninių ryšių tinklais ir paslaugomis, direktyvą 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje ir reglamentą Nr. 2006/2004 dėl nacionalinių institucijų, atsakingų už vartotojų apsaugos teisės aktų vykdymą, bendradarbiavimo. OL, 2009, L 322
88. 2016 m. liepos 12 d. Komisijos įgyvendinimo sprendimas (ES) 2016/1250 dėl ES ir JAV „privatumo skydo“ užtikrinamos apsaugos tinkamumo pagal Europos Parlamento ir Tarybos direktyvą 95/46/EB (pranešta dokumentu Nr. C(2016) 4176)
89. 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 arba Reglamentas (ES) 2016/679)

90. 2014–2020 metų nacionalinės pažangos programa. [žiūrėta: 2017-10-27]. Prieiga internetu: https://www.e-tar.lt/portal/lt/legalAct/TAR.31A566B1512D/OKkwPNbfzS
91. 2016 metų nacionalinio kibernetinio saugumo būklės ataskaita. [žiūrėta: 2017-11-03]. Prieiga internetu: https://kam.lt/download/57062/nksc_metine_ataskaita_uz_2016.pdf

PRIEDAI

1 PRIEDAS

Klausimynas (VDAI)

Esu Kauno technologijos universiteto socialinių, humanitarinių mokslų ir menų fakulteto magistrantūros studijų studentė. Atlieku tyrimą, kurio tikslas – nustatyti asmens duomenų apsaugos užtikrinimui taikomas priemones administracinių paslaugų teikime Lietuvos savivaldybėse. Tyrimas anoniminis ir atliekamas vadovaujantis konfidiancialumo principu, todėl savo nuomonę pateiktais klausimais galite drąsiai išsakyti, užtruksite apie 30 min. Jūsų pateikti atsakymai bus naudojami tik šiame darbe ir daugiau publikuojami nebus. Kiekviena jūsų išsakyta mintis yra svarbi.

1. Kaip keitėsi asmens duomenų apsaugos užtikrinimas Lietuvoje nuo 1990-ųjų metų? Prašome, įvardinkite svarbiausius pokyčius. Kas juos lėmė?
2. Kaip (kokiomis priemonėmis) užtikrinama asmens duomenų apsauga viešojo administravimo institucijose?
3. Kokios asmens duomenų apsaugos grėsmės/iššūkiai kyla viešojo administravimo institucijose? Kiek gaunate pranešimų, susijusių su asmens duomenų apsaugos pažeidimais viešojo administravimo institucijose? Kokio pobūdžio pažeidimai dažniausiai užfiksuojami?
4. Viešajame sektoriuje administracinių paslaugų teikimas vis plačiau teikiamas elektroninėje erdvėje. Kokie pažeidimai, susiję su administracinių paslaugų teikimu elektroninėje erdvėje dažniausiai užfiksuojami? Kaip dažnai?
5. Nuo 2018 m. gegužės 25 d. bus pradėtas taikyti Bendrasis duomenų apsaugos reglamentas, kokie esminiai pokyčiai laukia viešojo administravimo institucijų? Kaip vertinate pasiruošimą Bendrojo duomenų apsaugos reglamento taikymui?

2 PRIEDAS

Klausimynas (Savivaldybėms)

Esu Kauno technologijos universiteto socialinių, humanitarinių mokslų ir menų fakulteto magistrantūros studijų studentė. Atlieku tyrimą, kurio tikslas – nustatyti asmens duomenų apsaugos užtikrinimui taikomas priemones administracinių paslaugų teikime Lietuvos savivaldybėse. . Tyrimas anoniminis ir atliekamas vadovaujantis konfidiancialumo principu, todėl savo nuomonę pateiktais klausimais galite drąsiai išsakyti, užtruksite apie 20 min. Jūsų pateikti atsakymai bus naudojami tik šiame darbe ir daugiau publikuojami nebus. Kiekviena jūsų išsakyta mintis yra svarbi.

1. Kokias asmens duomenų apsaugos užtikrinimo priemones taikote institucijoje (tame tarpe administracinių paslaugų teikime)?
2. Kokia dalis institucijos administracinių paslaugų yra perkelta į elektroninę erdvę? Kaip užtikrinama asmens duomenų apsauga teikiant el. administracines paslaugas?
3. Nuo 2018 m. gegužės 25 d. bus pradėtas taikyti Bendrasis duomenų apsaugos reglamentas. Kokią įtaka tai turės asmens duomenų apsaugos užtikrinimui Jūsų institucijoje?

3 PRIEDAS

8 lentelė. Savivaldybių asmens duomenų tvarkymo tikslai (sudaryta autorės)

Savivaldybė	Registravimo data	Tikslas
Tauragės rajono	2002-06-06	Švietimas
Trakų rajono	2005-04-18	Valstybinės žemės nuomos mokesčio administravimas Moksleivių ir studentų duomenų banko tvarkymas Tiesioginių išmokų žemės ūkio subjektams skaičiavimas, prašymų įregistruoti žemės ūkio ir kaimo valdą priėmimas, pasėlių deklaracijų priėmimas Viešosios tvarkos užtikrinimas Trakų rajono savivaldybės Trakų, Lentvario ir Rūdiškių miestuose (vaizdo stebėjimas)
Raseinių rajono	2002-08-27	Socialinių paslaugų ir kitos socialinės paramos teikimas Asmenų, pageidaujančių gauti valstybės paramą, aprūpinant gyvenamosiomis patalpomis, registravimas Civilinės būklės aktų registravimas, papildymo, pakeitimo įrašų sudarymas, visų rūšių aktų apskaitymas, kartotinių liudijimų išdavimas Mokinio krepšelio paskaičiavimas, mokinių ir nelankančių mokyklos vaikų apskaita
Kauno miesto	1998-12-18	Leidimų prekiauti viešose miesto vietose išdavimas Leidimų įvažiuoti mechaninėmis priemonėmis į valstybės saugomas teritorijas išdavimas Valstybės garantijų, numatytų Lietuvos Respublikos piliečių nuosavybės teisių į išlikusį nekilnojamąjį turtą atkūrimo įstatyme, vykdymas Lietuvos gyventojų genocido ir rezistencijos tyrimo centro išduodamo Nukentėjusiųjų nuo 1939-1990 m. okupacijų teisinio statuso dokumento gavimas Valstybinės žemės nuomos mokesčio administravimas bei žemės nuomos mokesčio lengvatų teikimas Teisės į valstybės paramą įsigyti būstą patvirtinimas bei papildomų lengvatų teikimas asmenims, gavusiems lengvatinius ar valstybės remiamus būsto kreditus Savivaldybės gyvenamųjų patalpų ir jų priklausinių privatizavimas (pardavimas) lengvatinėmis ir rinkos kainomis Savivaldybės teritorijos planavimo dokumentų tvarkymas Savivaldybės socialinio būsto nuoma Piliečių nuosavybės teisių į išlikusį nekilnojamąjį turtą (gyvenamuosius namus, jų dalis, butus, ūkinės-komercinės paskirties pastatus su priklausiniais) atkūrimas Savivaldybės teritorijoje gyvenančių ikišauktinio amžiaus jaunuolių ir šauktinių apskaita Pažymų išdavimas seniūnijų gyventojams Pašalpų ir šalpos (socialinių) pensijų skyrimas ir mokėjimas Valstybinės vaiko teisių apsaugos funkcijos vykdymas Administracinių teisės pažeidimų išaiškinimas bei administracinių teisės pažeidimų bylų nagrinėjimas ir nuobaudų skyrimas (administracinių bylų teisenos vykdymas)

		Santuokos sudarymas
Šilalės rajono	2004-09-03	Teisė į valstybės paramą įsigyti būstą bei papildomų Lengvatų teikimas asmenims, gavusiems lengvatinius ar valstybės remiamus būsto kreditus Rinkėjų duomenų bazės sudarymas ir koregavimas Žemės nuomos mokesčio administravimas Pašalpų, kompensacijų, šalpos išmokų ir išmokų vaikams skyrimas ir mokėjimas Patvirtintų detaliųjų planų registracija, Nuolatinės statybos komisijos suderintų statybos objektų projektų registracija Civilinės būklės aktų registravimas Savivaldybės geoinformacinė sistema, adresų suteikimas ir keitimas, savivaldybei nuosavybės teise priklausančios žemės ir kitų teritoijų planavimo dokumentų tvarkymas Karo prievolės administravimas savivaldybės teritorijoje Vaikų teisių apsauga, laikinosios ir nuolatinės globos nustatymas, patraukimas administracinėn atsakomybėn, tėvų valdžios apribojimas Švietimas
Jurbarko rajono	2004-07-14	Sąlygų teritorijų planavimo dokumentų rengimui gavimas ir išdavimas, leidimų statyti ir griauti išdavimas Alkoholio, tabako, naftos produktų licencijų išdavimas Jurbarko rajono savivaldybės administracijos elektroninių paslaugų teikmas Žemės ūkio paskirties žemės naudotojų apskaita Švietimas Civilinės būklės aktų registravimas Socialinė parama įvairioms gyventojų grupėms Valstybės paramos teikimas, įsigyjant gyvenamąjį būstą
Prienų rajono	2015-09-01	Išduoti pažymas gyvenamosios patalpos savininkui (-ams) apie jo patalpose gyvenamąją vietą deklaravusius asmenis
Pagėgių rajono	2001-11-27	Švietimas

INTERVIU TRANSKRIPCIJA

Tauragės rajono savivaldybė (S1 respondentas)

1. Kokias asmens duomenų apsaugos užtikrinimo priemones taikote institucijoje (tame tarpe administracinių paslaugų teikime)?

Kadangi didžiąją dalį administracinių paslaugų, teikiamų Tauragės rajono savivaldybėje, suteikia tam tirkrų sričių specialistai, kurie naudojasi kompiuterine darbo vieta t. y. paslaugai suteikti naudojasi tam tikra sistema, tai pagrindinės asmens duomenų apsaugai užtikrinti priemonės yra teisės aktai ir kitos patvirtintos vidaus tvarkos. 2016 metais buvo patvirtintos asmens duomenų tvarkymo Tauragės rajono savivaldybės administracijoje taisyklės bei Tauragės rajono savivaldybės administracijos informacinės sistemos duomenų saugos nuostatai. 2017 metais – Tauragės rajono savivaldybės administracijos saugaus elektroninės informacijos tvarkymo taisyklės. Vadovaujantis šiais dokumentais visi vartotojai yra administruojami centralizuotai, jiem priskirti slaptažodžiai su atitinkamais reikalavimais, praėjus tam tikram laikui slaptažodžiai yra keičiami. Kitas aspektas – užtikrinamas duomenų kaupimas ir archyvavimas, kad duomenys nebūtų prarasti. Administracinės paslaugos yra teikiamos su tam tikra sistema, kuri kaupia duomenis, vėliau yra sukuriamos duomenų bazės, kur duomenys yra archyvuojami ir šifruojami. Archyvams yra taikomi papildomi specialūs reikalavimai. Taigi, apibendrintai galima sakyti, kad savivladybėje yra taikomos bendrosios priemonės – slaptažodžiai, antivirusinės programos, prevencinės priemonės skirtos darbuotojams. Viena iš pagrindinių priemonių tai saugaus duomenų perdavimo tinklas, savivaldybė nenaudoja viešo interneto. Tai gana brangi paslauga. Taigi, duomenys juda tik tame saugiame tinkle. Dėl pačių dokumentų kopijų saugojimo, yra specialūs reikalavimai serveriams. Pati VPK politika yra ta, kad savivaldybės nebeturėtų tokių serverinių, nebekauptų pas save duomenų, nes apsaugojimas nėra pas mus maksimalus, koks tūrėtų būti. O viską perkelti į vadinamus debesis.

Žiūrint bendrai, tai savivaldybėje didėja išlaidos IT sričiai ir saugumui bendrai. Įsidiegėme atitinkamą programinę įrangą automatizuotom kopijų darymui.

2. Kokia dalis institucijos administracinių paslaugų yra perkelta į elektroninę erdvę? Kaip užtikrinama asmens duomenų apsauga teikiant el. administracines paslaugas?

Sunku vienareikšmiškai atsakyti. Norėčiau pradėti nuo pačio administracinių paslaugų perkėlimo proceso. 2015 metais vidaus reikalų ministerijos sprendimu administracinės paslaugos centralizuotai buvo perkeltos į elektroninę erdvę. Tuo metu buvo perkeltos 65 administracinės paslaugos, tačiau šios paslaugos buvo dar iškaidomos (pvz. licendzijos išdavismas, jos dublikato išdavimas, licendzijos

panaikinimas) ir nurodomos kaip atskira paslauga. Pagal šį modelį, šiuo metu Tauragės rajono savivaldybė administruoja apie 150 administracinių paslaugų.

Gal galite įvardyti elektroninėje erdvėje teikiamas administracines paslaugas procentaliai?

Žvelgiant į visą Tauragės rajono savivaldybėje teikiamų administracinių paslaugų sąrašą elektroninėje erdvėje teikiamos administracinės paslaugos sudaro apie 45 proc. Esmė tokia, kad kiekvienas specialistas žino, kokias administracines paslaugas, su kokia tam skirta sistema jis turi teikti, tai yra nurodyta ir pareigybinėse nuostatose, tačiau bendros tokios politikos, kuri leistų visas administracines paslaugas prižiūrėti bendrai, nėra. Bardakas. Bet tokia netvarka kol kas yra daugelyje savivaldybių. Mūsų savivaldybės atveju, dedame pastangas, kad administracinė aplinka būtų tvarkinga, tačiau viešojoje erdvėje jos vis dar nėra tinkamai išpublikuotos, pats paslaugų katalogas yra problematiškas.

Ar administracines paslaugas teikiate per elektroninius valdžios vartus?

Pačio projekto idėja buvo tokia, kad savivaldybė turi DVS (dokumentų valdymo sistema) ir prie šio modelio atsiranda PVS (paslaugų valdymo sistema). Tai reiškia, kad valdomi tiek dokumentai, tiek paslaugos, kurios tinkamai aprašytos. Iš PVS duomenys toliau keliauja į paslaugų katalogą (lietuva.gov.lt), jeigu ten viskas gerai ir savivaldybė nedirba su savo PVS – jungiasi tiesiai, tai tiesiai kataloge suveda paslaugas ir jeigu viskas gerai jos automatiškai yra publikuojamos. Tačiau automatinis publikavimas neveikia, yra sudėtingas administravimas, kažkur fiziškai nespėjama, kažkur sistema sutrinka. Galutiniame variante paslaugų kataloge išpublikuotose administracinių paslaugų aprašymuose yra klaidų, prie e.paslaugų nesimato pilnų aprašymų, nors pati e.paslauga veikia tinkamai. Kai duomenys patenka į informacinės visuomenės plėtros komiteto sistemą ar VRM tai jie vaduovaujasi savo patvirtintais duomenų saugumo nuostatais. Šiuo atveju vartotojus per e.paslaugų teikimo procesą, nuo neteisėto duomenų pasisavinimo apsaugo vartotojo identifikavimas.

Savivaldybė turi patvirtintus vidinius nuostatus, kurios yra pagrindas saugiam duomenų tvarkymui. Savivaldybės skyriaus darbuotojai dirba su tokiomis sitemomis kaip licencijų alkoholiui, tabakui ir naftos produktams išdavimo programa, gyvenamosios vietos deklaravimo sistema, statybos leidimų duomenų tvarkymo informacinė sistema ir kt. Laikoma, kad visos naudojamos sistemos yra Tauragės rajono savivaldybės vienos informacinės sistemos posistemės, kurioms taikomi tie patys saugumo principai (pagal patvirtintus duomenų saugos nuostatus). Taigi, duomenys tvarkomi, lyg tai būtų viena bendra sistema.

Ar vartotojas visais atvejais gali tikėtis, kad jo duomenys administracinės paslaugos teikimo metu bus saugūs?

Problema yra tame, kad administracinių paslaugų teikime veikia daug posistemių ir kiekvienoje iš jų gali atsirasti spragų. Ir per šias spragas, sistemos netobulumą yra galimybė duomenis prarasti. Iki šiol gal nebūdavo pakankamai skirama dėmesio. Gal savivaldybėje kaupiami duomenys nėra tokie jautrūs, lyginant su kitais (paminimas „Grožio hirurgijos“ atvejis). Vartotojas 100 proc. galbūt ir negali būti garantuotas duomenų saugumu.

3. Nuo 2018 m. gegužės 25 d. bus pradėtas taikyti Bendrasis duomenų apsaugos reglamentas. Kokią įtaka tai turės asmens duomenų apsaugos užtikrinimui Jūsų institucijoje?

Nuo gegužės mėn. Vartotojas turės teisę reikalauti, kad būtų supažindinta, kaip yra tvarkomi jo duomenys. Tada galbūt pasirodys tam tikros spragos pačioje įstaigoje. Gal mes negalime matyti, kur vėliau sistemoje yra panaudojami duomenys (nežinome ar gavus paslaugą duomenys yra sunaikinami).

Ankščiau galbūt labiau buvo kreipiamas dėmesys į pačios paslaugos perkėlimą į elektroninę erdvę, bet saugumo pusė buvo paliekama e.paslaugos teikėjui ar institucijai, kuri naudosis e.paslauga. Bet ar jie užtikrins numatytus saugumo reikalavimus niekas negalėjo garantuoti. Dar neįsigaliojus reglamentui jau dabar kyla neaiškumų, kaip užtikrinti naudojamų posistemių apsaugą. Ar reiks sutartyse numatyti papildomus reikalavimus teikėjams? Ar teikėjai sutiks prisiimti tokią atsakomybę? Ar tai reikalaus papildomų išlaidų? Kas esant incidentui bus baudžiamas?

Atsiras duomenų saugos pareigūnas – tai tas žmogus, kurio dabar nėra, IT specialistai rūpinasi, kad vartotojai dirbtų tvarkingai, būtų apsaugota kompiuterinė darbo vieta ir pan. VPK rūpinasi, kad e.paslaugos būtų tinkamai teikiamos, paslaugos teikėjai, darbuotojai rūpinasi, kad paslauga būtų kuo greičiau suteikta. Bet visi būdai kaip tai daroma, niekas iki šiol netikrino. Gal tos informacijos yra prikaupta nemažai. Bet manau bus sunku rasti žmogų šiai pozicijai, nes reikalingi ir vadybiniai sugebėjimai, informacinių technologijų žinios bei prisideda juridiniai aspektai. Aš manau, kad situacija Tauragės rajono savivaldybėje yra išties nebloga, duomenys ir pakankamai gerai tvarkomi. Kiekviena paslauga yra aprašyta kiekvienas paslaugos teikėjas gali prašyti tik tokių duomenų, kurie yra būtini paslaugai suteikti. Lyginant su privačiu verslu (el. paruotuvės), kas ten daroma – neaišku. Savivaldybė yra kontroliuojama, taip pat nuolat teikia ataskaitas, kartą per metus pateikia duomenis NKSC, VRM.

Kalbant apie patį pasiruošimą naujajam reglamentui, tai šiais metais vykome į VDAI organizuotus mokymus, naudojamės metodine priemone, kai prireikia komunikuojame tiesiogiai. Reglamente paminėtas naujas aspektas – duomenų šifravimas. Vienas dalykas, kai duomenys yra prarandami, kitas – kai duomenys yra prarandami, bet jais negali pasinaudoti. Manau įgyvendinus šią nuostatą, bus padaryta didelė dalis darbo, kad atitikti naujajam reglamentui. Dar vienas dalykas, kad kiekvieną incidentą susijusį su asmens duomenimis reikės fiksuoti ir pranešti VDAI.

I. Trakų rajono savivaldybė (S2 respondentas)

Laba diena,

Administracijos direktoriaus pavedimu atsakau į jūsų pateiktus klausimus:

1. Kokias asmens duomenų apsaugos užtikrinimo priemones taikote institucijoje (tame tarpe administracinių paslaugų teikime)?

Pagrindinė priemonė – reikalavimas visiems administracijos darbuotojams tiksliai vykdyti asmens duomenų teisinės apsaugos ir kitų įstatymų nuostatas. Todėl labai svarbu nerinkti ir nereikalauti pateikti perteklinių duomenų. Asmens duomenys saugomi tiek popieriniame variante, tiek informacinėse sistemose ar laikmenose. Byloms, kuriose saugomi asmenų duomenys, taikoma griežta apskaita; jos saugomos papildomas fizines apsaugos priemones turinčiose patalpose (ne pirmame aukšte; turinčiose patikimesnes užraktų sistemas ir pan.). Bylos, kuriose kaupiami asmenų duomenys, naikinamos laikantis nustatytų tvarkų dokumentų naikikliais (jokiu būdu nepriduodamos makulatūros surinkėjams). Informacinėse sistemose saugomų duomenų apsaugai taip pat taikomos sustiprintos fizinės apsaugos priemonės – kompiuterinės darbo vietos įrengiamos papildomai apsaugotose patalpose, kurios saugomos apsaugos signalizacijos; taikomos papildomos programinės įrangos apsaugos priemonės.

2. Kokia dalis institucijos administracinių paslaugų yra perkelta į elektroninę erdvę? Kaip užtikrinama asmens duomenų apsauga teikiant el. administracines paslaugas?

Į elektroninę erdvę perkelta apie pusė savivaldybės teikiamų paslaugų, deja, jomis labai mažai naudojamasi. Asmens duomenų apsauga vykdoma tais pačiais būdais, kuriuos išvardinau pirmame punkte.

3. Kokia dalis institucijos administracinių paslaugų yra perkelta į elektroninę erdvę? Kaip užtikrinama asmens duomenų apsauga teikiant el. administracines paslaugas

Kol kas sunku atsakyti, nors neabejoju, kad dėmesys asmens duomenų apsaugai didės. Savivaldybė tam nusimatė 2018 m. lėšų papildomos apsaugos priemonėms įsidiegti, tačiau kokios konkrečiai jos bus, dabar negalime atsakyti.

Raseinių rajono savivaldybė (S3 respondentas)

1. Kokias asmens duomenų apsaugos užtikrinimo priemones taikote institucijoje (tame tarpe administracinių paslaugų teikime)?

Pirmiausia taikome teisines priemones, administracijos direktoriaus įsakymu yra patvirtintos tvarkos, pagal kurias darbuotojai yra įpareigojami saugoti asmens duomenis, pasirašyti konfidencialumo pasižadėjimus. Toliau naudojamos įprastos informacinių technologijų saugos priemonės asmens duomenims apsaugoti – tai prieigų prie informacijos ribojimas, slaptažodžių, elektroninių autentifikavimo priemonių naudojimas prisijungimui prie informacinių sistemų, kuriose naudojami asmens duomenys.

2. Kokia dalis institucijos administracinių paslaugų yra perkelta į elektroninę erdvę? Kaip užtikrinama asmens duomenų apsauga teikiant el. administracines paslaugas?

Į elektroninę erdvę yra perkelta apie 50 proc. administracinių paslaugų. Teikiant šias paslaugas asmens duomenų apsauga įgyvendinama Elektroninių valdžios vartų autentifikavimo priemonėmis, kadangi visas paslaugas būtent teikiame per ten. Apsaugos priemonės tos pačios naudojamos tiek paslaugom teikiamom įprastai, tiek el.būdu, kadangi įprastai teikiamos paslaugos vis tiek patenka į vidines informacines sistemas, tokias kaip Dokumentų valdymo sistema.

3. Nuo 2018 m. gegužės 25 d. bus pradėtas taikyti Bendrasis duomenų apsaugos reglamentas. Kokią įtaka tai turės asmens duomenų apsaugos užtikrinimui Jūsų institucijoje?

Pakolkas dar tik ruošiamės darbui pagal šį reglamentą, tačiau bet kokiu atveju asmens duomenų apsauga bus griežtesnė ir labiau reglamentuota. Bus įdomu stebėti, kaip institucijos, tame tarpe ir mūsų savivaldybė, išspęs duomenų apsaugos pareigūno klausimą, nes tai visiškai naujas dalykas šioje srityje.

Kauno miesto savivaldybė (S4 respondentas)

Teikiu Jums atsakymus savo kompetencijos ribose ir apie automatiniu būdų tvarkomus asmens duomenis.

Norėčiau atkreipti dėmesį, kad asmens duomenų tvarkymas vykdomas vadovaujantis teisės aktais, Asmens duomenų teisinės apsaugos įstatyme (toliau – ADTAĮ) yra nustatyta, kad asmens duomenys gali būti tvarkomi tik teisėtais tikslais, todėl kalbėdami apie asmens duomenų tvarkymą reikėtų kalbėti

apie konkretų duomenų tvarkymo tikslą. Vadovaujantis ADTAĮ, Kauno miesto savivaldybės administracijos (toliau – KMSA) asmens duomenų tvarkymo tikslai skelbiami Asmens duomenų valdytojų valstybiniame registre https://www.ada.lt/go.php/lit/img/11.

1. Kokias asmens duomenų apsaugos užtikrinimo priemones taikote institucijoje (tame tarpe administracinių paslaugų teikime)?

KMSA informacinės sistemos (toliau—IS) duomenų sugumo politiką nustato KMSA direktoriaus įsakymais patvirtinti dokumentai: KMSA IS duomenų saugumo nuostatai, Saugaus elektroninės informacijos tvarkymo KMSA IS taisyklės; KMSAIS naudotojų administravimo taisyklės; KMSA IS veiklos tęstinumo valdymo planas. Duomenų saugumo politika taikoma ir asmens duomenims. Be to, kaip nustato ADTAĮ, KMSA direktoriaus įsakymu patvirtintose Asmens duomenų tvarkymo taisyklėse yra nustatytos organizacinės ir techninės duomenų saugumo priemonės. Šis įsakymas yra taikomas visiems asmens duomenims, kuriuos tvarko KMSA darbuotojai – ir tiems, kurių valdytoja yra KMSA, ir tiems, kurių valdytojai yra kitos įstaigos.

Aukščiau paminėti teisės aktai yra taikomi užtikrinti KMSA tvarkomų asmens duomenų apsaugą, tame tarpe ir tų, kurie tvarkomi teikiant paslaugas automatiniu būdu.

2. Kokia dalis institucijos administracinių paslaugų yra perkelta į elektroninę erdvę? Kaip užtikrinama asmens duomenų apsauga teikiant el. administracines paslaugas?

Į antrą brandos lygį esame perkėlę visas teikiamas savo paslaugas. 3-4 brandos lygio paslauga galite rasti http://ep.kaunas.lt/index.php/4/?evID=&env=3&e=1 Kadangi antrasis klausimas – tai pirmojo klausimo pakartojimas, galiu atsakyti, kad asmens duomenims, kurie tvarkomi teikiant paslaugas automatiniu būdu, taikoma ta pati apsauga, kaip ir visiems asmens duomenims, kurių valdytoja yra KMSA.

3. Nuo 2018 m. gegužės 25 d. bus pradėtas taikyti Bendrasis duomenų apsaugos reglamentas. Kokią įtaka tai turės asmens duomenų apsaugos užtikrinimui Jūsų institucijoje?

Šiuo metu KMSA asmens duomenų tvarkymo teisėtumas ir saugumas yra užtikrinami vadovaujantis galiojančiais teisės aktais. Pradėjus taikyti duomenų apsaugos reglamentą, kuris yra tiesioginio taikymo, keisis ir nacionaliniai teisės aktai, todėl, atsižvelgiant į Bendrojo duomenų apsaugos reglamento ir nacionalinių teisės aktų bei VDAI pateiktus išaiškinimus ir nurodymus, KMSA turės būti įgyvendintos naujos nuostatos, susijusios su duomenų tvarkymu ir asmens teisių įgyvendinimu bei pakeisti teisės aktai, užtikrinantys teisėtą asmens duomenų tvarkymą.

II. Interviu su Šilalės r. sav. (S5 respondentas)

1. Kokias asmens duomenų apsaugos užtikrinimo priemones taikote institucijoje (tame tarpe administracinių paslaugų teikime)?

Asmens duomenų saugumui užtikrinti vadovaujamasi asmens duomenų teisinės apsaugos įstatymu, Šilalės rajono savivaldybės administracijos direktoriaus 2015 m. vasario 3 d. įsakymu Nr. DĮV-130 „Dėl Asmens duomenų tvarkymo Šilalės rajono savivaldybės administracijoje taisyklių patvirtinimo“ yra parvirtintos Asmens duomenų tvarkymo Šilalės rajono savivaldybės administracijoje taisyklės“ bei Šilalės rajono savivaldybės administracijos direktoriaus 2008 m. gegužės 30 d. įsakymu Nr. DĮV-684 „Dėl Šilalės rajono savivaldybės administracijos informacinių sistemų duomenų saugos nuostatų patvirtinimo“ patvirtinti Šilalės rajono savivaldybės administracijos informacinių sistemų duomenų saugos nuostatai“.

Šilalės rajono savivaldybės administracijos gauti ir parengti dokumentai yra rengiami ir apskaitomi dokumentų valdymo sistemoje „Kontora“. Prisijungimai prie informacinių sistemų yra apsaugoti slaptažodžiais, popieriniai dokumentai, kuriuose yra asmens duomenų saugojami seifuose bei užrakinamose metalinėse spintose, o pasibaigus jų saugojimo terminams yra perduodami saugoti į valstybės archyvus teisės aktų nustatyta tvarka.

2. Kokia dalis institucijos administracinių paslaugų yra perkelta į elektroninę erdvę? Kaip užtikrinama asmens duomenų apsauga teikiant el. administracines paslaugas?

Šilalės rajono savivaldybėje teikiama 151 viena administracinė paslauga, iš kurių 65 paslaugos teikiamos ir elektroniniu būdu. Kiekvienai paslaugai yra parengti paslaugos aprašymai, kurie yra skelbiami Šilalės rajono savivaldybės interneto svetainėje www.silale.lt ir Lietuvos paslaugų katalogo informacinėje sistemoje www.lietuva.gov.lt. Kiekvienai paslaugai yra priskirti paslaugos teikėjai, kurie yra nurodyti paslaugos aprašymuose, taip pat nurodomi jų kontaktiniai duomenys.

Elektroniniu būdu teikiamos paslaugos nėra labai populiarios, dažniausiai rajono gyventojai dėl paslaugų teikimo kreipiasi asmeniškai, atvykdami į savivaldybės administraciją ar seniūniją, arba atsiųsdami prašymus įprastu paštu. 2017 m. gruodžio 19 d. elektroniniu būdu kreipėsi tik 44 asmenys.

Apie elektroniniu būdu ir kitais būdais suteiktas paslaugas kas ketvirtis yra teikiamos Paslaugų stebėsenos rodiklių ataskaitos Vidaus reikalų ministerijai, o ministerija kas mėnesį savivaldybėms teikia informaciją kiek kurioje savivaldybėje gauta prašymų elektroniniu būdu ir kiek tuo pačiu būdu pateikta atsakymų.

3. Nuo 2018 m. gegužės 25 d. bus pradėtas taikyti Bendrasis duomenų apsaugos reglamentas. Kokią įtaka tai turės asmens duomenų apsaugos užtikrinimui Jūsų institucijoje?

Įsigaliojus Bendrajam duomenų apsaugos reglamentui, Savivaldybės administracijoje pirmiausiai bus peržiūrėtos visos tvarkos reglamentuojančios duomenų apsaugą, tvarkos ir taisyklės ir parengtos naujos atitinkančios galiojančius teisės aktus. Ruošdamiesi reglamento taikymui sekame VDAI parengtas metodines priemones ir rekomendacijas. Atsižvelgiant į jas stengiamės atlikti būtinus veiksmus iki gegužės 25 d., būtent tada bus pradėta jį taikyti.

III. Jurbarko rajono savivaldybė (S6 respondentas)

1. Kokias asmens duomenų apsaugos užtikrinimo priemones taikote institucijoje (tame tarpe administracinių paslaugų teikime)?

Pirmiausia tai yra vadovaujamasi asmens duomenų įstatymu. Jurbarko rajono savivaldybė yra pasitvirtinusi bendrąsias duomenų saugos taisykles. Šios taisyklės yra taikomos apskritai viskas, tiek elektroniniams dokumentams, tiek ne elektroniams dokumentams, DVS ir kt. naudojamoms sistemoms. Kiekvienas registras, kuriame yra saugomi dokumentai turi tam tikras taisykles, kuriose nurodytas saugojimo laikas, kokiomis priemonėmis užtikrinamas duomenų saugumas, kai dokumentai turi būti sunaikinami. Viskas reglamentuota, tik reikia laikytis taisyklių. Kas priklauso nuo savivaldybės tai mes esame viską padarę, todėl bendrai asmens duomenų apsaugos situaciją vertinčiau gerai. Bet žmogiškasis faktorius visada lieka ir liks. Bet žmogus ar institucijos darbuotojas turi būti supažindintas, kokios pasekmės dėl galimų jo veiksmų laukia.

2. Kokia dalis institucijos administracinių paslaugų yra perkelta į elektroninę erdvę? Kaip užtikrinama asmens duomenų apsauga teikiant el. administracines paslaugas?

Reiktų saičiuoti.. na kaip čia pažiūrėsi į tą elektroninę erdvę... Viskas yra sudėta Jurbarko rajono savivaldybės tinklapyje. Savivaldybės specialistai teikdami elektronines paslaugas naudojasi atitinkamomis sistemomis (SPIS, IFOSTATYBA, MEPIS ir kt.). Pagal paskutinį centralizuotą projektą į el. erdvę buvo perkeltos 62 paslaugos. Jei išsireikšti procentaliai, tai galima sakyti, kad apie 40 proc. visų administracinių paslaugų yra perkelta į el. erdvę. Taigi, mes teikiame e.paslaugas per savo savivaldybės platformą, kuri yra susieta ir su dokumentų valdymo sistema. Per sistemoje www.lietuva.gov.lt ir elektroninius valdžios vartus taip pat galima rasti Jurbarko savivaldybės teikiamas administracines paslaugas, tačiau šioje vietoje matomi it paslaugų aprašymai, pasirinkus jas yra nukreipiama į savivaldybės svetainę. Jurbarkas, Klaipėda, Kaunas ir Vilnius, šių miestų savivaldybės teikia administracines paslaugas individualiai. Čia įvyko didelis nesusikalbėjimas.

Minėtos savivaldybės buvo šiek tiek labiau pažengusios elektroninių paslaugų teikime dar prieš pradedant vykdyti cetralizuotą projektą, jau turėjo įsidiegusios atitinkamas platformas. Galvojome, kad bus per e.valdžios vartus bus sukurtos tam tikros nuorodos į mūsų teikiamas paslaugas, bet viso šito nebuvo padaryta ir likome nuošalyje. E.valdžios vartuose parašyta, kad savivaldybė paslaugas teikia, bet tai daro tik per savo svetainę. Na gavosi kaip gavosi. Ištikrųjų tokia situacija, kai vienos paslaugos yra vienur, kitos – kitus, tik kelia žmoniems sumaištį. Bet mes savo sukurto paslaugų teikimo modelio neatsisakysime, nes sistemos yra sujungtos, yra įdėtas įdirbis, be to nematome ir reikalo tai daryti. Nebent tam būtų skirtas papildomas finansavimas iš kitų fodų, tačiau savo lėšomis tikrai nežadame papildomai perkelti paslaugų į e.valdžios vartus. Realiai, kas liečia saugumą, tai visas asmens identifikavimas vyksta per el.bankininkystę bei el. parašu, pastarosios yra pakankamai saugios priemonės. Identifikavus asmenį, toliau pateikiami papildomi duomenys kaip gyvenamoji vieta, el. paštas ir kt. Tai, šiuo atveju, kad paslaugą užsisakys kitas asmuo yra labai mažai tikėtina.

3. Nuo 2018 m. gegužės 25 d. bus pradėtas taikyti Bendrasis duomenų apsaugos reglamentas. Kokią įtaka tai turės asmens duomenų apsaugos užtikrinimui Jūsų institucijoje?

Šiam reglamentui ruošiamės jau seniai. Pradžia yra padaryta, duomenų saugos taisyklės atnaujintos, įdirbis yra. Kitas dalykas, kol kas negalime iki galo pasiruošti, nes VDAI yra paruošusi įstatymo pakeitimo projektą. Taigi dar nemažai teisės aktų guli vyriausybės stalčiuose. Tai mus kol kas ir stabdo. Kol kas dar neaišku ir koks bus asmens duomenų apsaugos pareigūno statusas ir kaip jis įsilies į instituciją. Yra daug niuansų.. Naujojo reklamento taikymas skatins institucijas dar atidžiau dirbti asmens duomenų apsaugos srityje, tai palies ne tik e.paslaugas ar informacines sistemas, bet ir el.paštą, popierinius dokumentus.

Prienų rajono savivaldybė (S7 respondentas)

Atsižvelgiant į Jūsų prašymą, deja, kol kas nieko negalime padėti, nes su duomenų apsauga pradedame dirbti tik dabar, todėl jokios informacijos pateikti neturime galimybės. Teikdami administracines paslaugas naudojame slaptažodžius, ugniasienes. Į el. erdvę yra perkelta apie 40 proc. administracinių paslaugų, už saugumą atsakingi paslaugų tiekėjai.

Pagėgių rajono savivaldybė (S8 respondentas)

1. Kokias asmens duomenų apsaugos užtikrinimo priemones taikote institucijoje (tame tarpe administracinių paslaugų teikime)?

Kiekvienas skyrius dirba su atitinkama sistema ir privalo užtikrinti duomenų saugumą, nereikalauti daugiau informacijos nei yra numatyta. Visais atvejais yra vadovaujamasi asmens duomenų apsaugos įstatymu, savivaldybė ruošiasi patsivirtinti duomenų saugos nuostatus, kurie galios ir asmens duomenims. O pagrindinės saugumo priemonės tai slaptažodžiai, ugniasienės.

2. Kokia dalis institucijos administracinių paslaugų yra perkelta į elektroninę erdvę? Kaip užtikrinama Kaip užtikrinama asmens duomenų apsauga teikiant el. administracines paslaugas?

Visos adm. paslaugos yra perkeltos į elektroninę erdvę (www.epaslaugos.lt, www.lietuvagov.lt). El. paslaugų saugumą užtikrina paslaugų teikėjai. Bet galime akcentuoti, kad gyventojai mažai naudojasi el. Paslaugomis, dažniausiai tiesiogiai atvyksta į savivaldybę.

3. Nuo 2018 m. gegužės 25 d. bus pradėtas taikyti Bendrasis duomenų apsaugos reglamentas. Kokią įtaka tai turės asmens duomenų apsaugos užtikrinimui Jūsų institucijoje?

Dar apie tai negalima nieko pasakyti, nes tai bus tik nuo 2018-05-25.

Interviu su VDAI direktorės pavaduotoja (A1)

1. Kaip keitėsi asmens duomenų apsaugos užtikrinimas Lietuvoje nuo 1990-ųjų metų? Prašome, įvardinkite svarbiausius pokyčius. Kas juos lėmė?

Duomenų apsauga Lietuvoje kito tiek, kiek kito ES reglamentavimas. 1995 m. Direktyva galiojo iki 2016 m. Pirmas kardinalus įvykis –tai duomenų apsaugos reglamentavimo pradžia, ne tik informacijos saugumo prasme, bet ir kaip žmogaus teisė į duomenų apsaugą (ne vien privatumą). Antras virsmas yra ir kiekybinis ir kokybinis, tai pripažinimas, kad asmens duomenų apsauga yra labai svarbus dalykas ne tik žmogaus teisių gynimo prasme, tačiau ir visuomenės saugumo prasme. Trečias aspektas – tai 2016 metų asmens duomenų apsaugos reforma ir Bendrojo duomenų apsaugos reglamento taikymas.

Lietuvoje asmens duomenų įstatymas priimtas 1996 m., VDAI įstaiga pradėjo veikti 1997 m. Svarbi data – įstojimas į ES. Palaipsniui VDAI darbuotojų skaičius nuo 8 išaugo iki 30. Kas lėmė tokį darbuotojų skaičiaus didėjimą? 8 žmonės prižiūrėjo tik valstybės informacinius išteklius – registrus. Šiuo metu 30 žmonių prižiūri visą juridinių asmenų registrą. Nesvarbu, kad kai kurie juridiniai asmenys neturi pareigos registruotis, kaip duomenų valdytojai, tačiau jų veikla visvien yra prižiūrima.

2. Kaip (kokiomis priemonėmis) užtikrinama asmens duomenų apsauga viešojo administravimo institucijose?

Pagrindinė priemonė – įstatymas. Jei įstaiga atitinka duomenų apsaugos įstatyme numatytus reikalavimus, reiškias duomenų apsauga yra sutvarkyta tinkamai. Asmens duomenų apsaugos reikalavimai yra vienodi tiek viešajam, tiek privačiam sektoriui. Įstatymas yra vienodai taikomas visiems.

3. Kokios asmens duomenų apsaugos grėsmės/iššūkiai kyla viešojo administravimo institucijose? Kiek gaunate pranešimų, susijusių su asmens duomenų apsaugos pažeidimais viešojo administravimo institucijose? Kokio pobūdžio pažeidimai dažniausiai užfiksuojami?

Viešajam sektoriui didžiausios grėsmės kyla su elektronine ir kibernetine sauga. Viešojo sektoriaus institucijos dažniausiai tvarko asmens duomenis taip, kad jie atitiktų įstatyme numatytus reikalavimus. Įvairių incidentų ar neteisėtų duomenų atskleidimų, žmogiškojo faktoriaus klaidų tikimybė yra visur – tiek viešam tiek privačiam sektoriuje. Viešajam sektoriui didesnė problema – lėšų stygius. Kibernetinių incidentų metu yra didelė tikimybė, kad valstybės informaciniai ištekliai galės būti pažeisti. Dėl šios priežasties, šiuo metu tiek LR Seimas, tiek LR Vyriausybė skiria daug dėmesio šiam

klausimui. Yra rengiama kibernetinio saugumo strategija, per pastaruosius metus patvirtinti būtiniausi įstatymai šioje srityje. Dvejus metus iš eilės (2016-2017) vyko kibernetinio saugumo pratybos. Taigi darome viską, kad duomenys būtų saugūs. Na viešajame sektoriuje tokių problemų kaip ir nėra.

Pranešimų apie incidentus viešojame sektoriuje negaunate?

Žinoma gauname. Visada yra tikimybė, kad įvyks žmogiškoji klaida, pvz. kad netinkamai duomenys bus perduoti tarp institucijų, policininkas pasižiūrėjo informacinėje sistemoje ne tik įtariamojo duomenis, bet ir tarkim kaimyno. Bet aš turiu omenyje, kad viešojo sektoriaus institucijose nėra sisteminių problemų. Valstybės kontrolė, atlikdama informacinių išteklių tyrimą, tiesiog rado trūkumus, kuriuos reikėtų šalinti ir jie yra šalinami. Patys pažeidimai yra panašūs ir viešajame ir privačiame sektoriuose. Gal tiesiog skiriasi pažeidimų skaičius, kadangi viešajame sektoriuje nėra vykdoma tiesioginė rinkodara.

4. Viešajame sektoriuje administracinių paslaugų teikimas vis plačiau teikiamas elektroninėje erdvėje. Kokie pažeidimai, susiję su administracinių paslaugų teikimu elektroninėje erdvėje dažniausiai užfiksuojami? Kaip dažnai?

Teikiant administracines paslaugas el. erdvėje daržniausiai susiduriama su asmens identifikavimo pažeidimais. Kad subjektas galėtų prisijungti, kad prisijungtų tas žmogus, kuris užsako paslaugas ir kuriam jos turi būti suteiktos. Svarbiausia užtikrinti, kad neįvyktų duomenų vagystė, kad aplinka, kurioje yra suteikiama paslauga būtų draugiška ir kad žmogus galėtų prisijungti tada, kada jam reikia. Žmogui nepavyko savęs identifikuoti, bet neaišku ar tai yra jo kaltė, gal te taip ką surinko. O gal tuo pat metu vyksta incidentas ir žmogus jungiasi ne prie institucijos portalo, o prie apsimestinės svetainės. Kiekvienas atvejis yra kitoks. Tiesiog technologijos taip greitai sensta, o mes lėtai mokomės jomis naudotis, mūsų klijentai taip pat. Daugiausia identifikavimo pažeidimus gauna CERT‘as, na mes tiriame tik tuos atvejus, kurie turi asmens duomenų apsaugos pažeidimo požymių. Tokių atvejų yra buvę, et tai yra pavieniai atvejai. Tokių, kaip kaip „Grožio klinika“ atvejų retai pasitaiko. 2003 m. vykusi duomenų vagystė iš SODROS, sakyčiau vienetinis atvejis.

Valstybė žmogui teigdama paslaugas ją teikia arba elektroniniu arba popieriniu būdu. El. paslauga, mano manymu, yra saugesnė. Tačiau vyresnės kartos atstovai lėtai priima pokyčius ir dažniausiai el. dokumento nepripažysta. Kaip žinia, esame senstanti tauta, tai didelė dalis asmenų tiesiog nenori paslaugos gauti el. būdu, todėl esame priversti paslaugas teikti paslaugas popieriniu būdu. Bet šiuo atveju neįžvelgčiau esminio kokybės skirtumo. Elektroniniams dokumentams taikomos saugos priemonės yra informacinių sistemų saugumą užtikrinančios priemonės, sakykim protokolai, ugniasienės ir kita programinė įranga. Tai priklauso nuo investicijų, kiek institucija priemones atnaujina ir pan.

5. Nuo 2018 m. gegužės 25 d. bus pradėtas taikyti Bendrasis duomenų apsaugos reglamentas, kokie esminiai pokyčiai laukia viešojo administravimo institucijų? Kaip vertinate pasiruošimą Bendrojo duomenų apsaugos reglamento taikymui?

Pokyčiai laukia visų duomenų valdytojų ir tvarkytojų. Jie taps atsakingi už visus savo veiksmus ar neveikimą, tvarkant asmens duomenis. Jie bus atsakingi, kad duomenys bus surinkti turint teisinį pagrindą, kad duomenys būtų tvarkomi pagal teisės aktų reikalavimus, kad duomenys nebūtų atskeisti ar surinkti neturint tam pagrindo. Viską, kas yra daroma su asmens duomenimis turės būti fiksuojama ir pateikiama duomenų priežiūros institucijai pareikalavus. Šie reikalavimai bus taikomi apsoliučiai visiems duomenų valdytojams ir tvarkytojams. Žmogaus teisių gynimo srityje negali būti jokių nuolaidų nei vienai kategorijai. Tie subjektai, kurie turi daugiau išskirtinių teisių gauti asmens duomenis ar naudoti savo veikloje, turi ir daugiau pareigų. Atskleidus viešajame sektoriuje kaupiamus duomenis, gali būti padaryta didelė žala.

Svarbus pasikeitimas – asmens duomenų apsaugos pareigūnas. Visos viešojo sektoriaus institucijos, kurios tvarko asmens duomenis turės turėti asmens duomenų apsaugos pareigūną. Šioje srityje mums visiems reiks pasitemsti ir pasimokyti vieniems iš kitų ir iš kitų šalių praktikos. Duomenys jau seniai nebetvarkomi popierinėse laikmenose, tai yra galingos, tarpusavyje integruotos ir realiame laike besikeičiančios duomenimis informacinės sistemos. Asmens duomenų pareigūnas turės turėti ir geras informacinių technologijų bei teisines žinias, turės būti pakankamai nepriklausomas ir savo pastebėjimus ar pasiūlymus pateikti aukščiausiai vadovybei. Nepriklausomumas – sunkaisusiai užtikrinama dalis, nes nėra visiškai nepriklausomo darbuotojo dirbančio įstaigoje. Gal būt organizacijos samdymas būtų patikimesnis būdas, tačiau gerokai brangesnis.

Viešasis sektorius labai daug padarė per pastaruosius metus, kadangi jau keliarius metus yra stebimi valstybės informaciniai ištekliai, tikrinami įvairūs duomenų apsaugos aspektai, konsoliduojami žinybiniai registrai. Po šių pakeitimų iš įvairių institucijų KAM perėmė šių registrų konsolidacijos ir reglamentavimo klausimus.

Mūsų žmonės dirba su savivaldybėmis, pradėjome informavimo kampaniją. Aš manau, kad savivaldybės yra tos institucijos, kurios sugebės pasiruošti artėjantiems pasikeitimams. Čia labiau mažųjų įmonių ir žmonių, nesidominčiais žmogaus teisėmis ir reguliavimo aplinka, problemos. Siekiame, kad žmones pasiektų informacija kuo plačiau ir jie galėtų pasiruošti artėjantiems pasikeitimams.

Šiandien plačiai pripažįstama, kad komunikacija yra labai svarbu, bet teisė į duomenų apsaugą yra dar svarbesnė.

Interviu su VDAI teisės skyriaus vedėja (A2 respondentas)

1. Kaip keitėsi asmens duomenų apsaugos užtikrinimas Lietuvoje nuo 1990-ųjų metų? Prašome, įvardinkite svarbiausius pokyčius. Kas juos lėmė?

Aš inspekcijoje dirbu nuo 2005 m., tai apie ankstesnį laikotarpį nelabai galėčiau komentuoti. Žiūrint nuo pačio inspekcijos įkūrimo, tai ji viso labo buvo įkurta 1997 m. Duomenų apsaugos direktyva buvo priimta 1995 m., asmens duomenų teisinės apsaugos įstatymas priimtas 1996 m. Tai iki šių svarbių datų, duomenų apsaugos užtikrinimo reiktų žiūrėti civiliniame kodekse, kaip reglamentuojama. Bet tai ne ta duomenų apsauga, kaip mes ją dabar suprantame pagal europinius dokumentus. VDAI įkūrimo pradžioje buvo vos 8 etatai. Vėliau inspekcijos funkcijos plėtėsi, etatų skaičius augo (kaip tai vyko nuosekliai galima rasti internetiniame puslapyje). Manau reikšminis pokytis – tai, kad inspekcijos galios pasidarė tokios pačios kaip ir kitų ES priežiūros institucijų. Kas yra visiškai kitaip nei kitose ES šalyse? Tai kad inspekcija prisideda ir prie kibernetinio saugumo politikos vykdymo. Kita vertus mes neprižiūrime žurnalistų. Ta prasme, inspekcija neprižiūri asmens duomenų tvarkymo visuomenės informavimo priemonėse, visuomenės informavimo tikslais. Kai kurios šalys turi specialistus, kurie prižiūri ir šią sritį pvz. Estija. Taigi, kaip svarbiausią pokyti išskirčiau būtent inspekcijos galių išsiplėtimą.

Ar įvykusius asmens duomenų apsaugos pokyčius sietumėte su teisinės bazės pasikeitimais?

Na čia reikėtų žiūrėti labai smulkmeniškai. Pavyzdžiui, tas pats elektroninių ryšių įstatymas, jis buvo priimtas įgyvendinant direktyvą, kas liečia duomenų tvarkymą – elektroninė rinkodara, ryšių priemonės ir t.t. Tai pakeitimai, rodos, buvo 2006 m. jei neklystu... Tai vėl gi, inspekcija pradėjo prižiūrėti juridinius asmenis. Ką tai reiškia? Jei siunčiu rinkodarą abonentu, abonentas gali būti ir juridinis asmuo. Tai toks išskirtinis visiškai atvejis, kada inspekcija gina ne tik fizinio asmens teises, bet ir juridinio asmens teises. Apie kibernetinį saugumą jau minėjau, tai tą pradėjome daryti visai neseniai, įstatymas keitėsi 2014 m. Kompetencija numatyta ir valstybės informacinių išteklių valdymo įstatyme, ko ankščiau nebuvo, tą lėmė tik paskutiniai įstatymo pakeitimai.

2. Kaip (kokiomis priemonėmis) užtikrinama asmens duomenų apsauga viešojo administravimo institucijose?

Realiai reikalavimai jei žiūrėsime į asmens duomenų apsaugos įstatymą, taigi matome apibrėžimą apie asmens duomenų valdytoją ir tvarkytoją. Nėra išskirta, kad tai viešojo sektoriaus duomenų valdytojas. Reiškia, kad bendri reikalavimai yra keliami tie patys. Ką viešasis sektorius turi papildomai? Tai jam ir vidaus reikalų ministerija turi numačiusi papildomus reikalavimus saugumui užtikrinti. Tai išskirčiau tokį skirtumą. Bet realiai, jis vis tiek atitinka tą bendrą principą, kad turi būti taikomos tinkamos organizacinės saugumo priemonės. Patį techninį įrankį renkasi duomenų valdytojas, pagal savo

galimybes. Tai kas turi daugiau lėšų renkasi geresnį įrankį, kas neturi, aišku prastesnį. Tai yra visiška diskrecijos laisvė, kaip duomenų valdytojas tai daro. Išskyrus bendruosius reikalavimus organizacinėms ir techninėms priemonėms, kur aiškiai pasakyta, ką privalu užtikrinti. Bet inspekcija ir duomenų apsaugos įstatymas konkretaus įrankio nenusako. Mes sakome, kad turite užtikrinti saugumą, prieigą riboti ir t.t. bet kokiu būdu tai darys pasirenka pačios institucijos. Asmens duomenų apsaugos įstatymas numato bazę, kaip tokią, jei žiūrėti siauriau yra minėti bendrieji reikalavimai organizacinėms ir techninėms saugumo priemonėms, kurias yra patvirtinęs inspekcijos direktorius. Kita vertus, jei žiūrėti į reglamentą, reglamentas nenumato valstybėms narėms galimybės tvirtinti tokių priemonių, tai reiškia, kad jos bus pripažintos netekusiomis galios. Tai duomenų valdytojams liks absoliuti diskrecija, pasirinkti tokias priemones, kokios jo manymu yra tinkamos. Ir tada jau bus galima diskutuoti su institucija ar jos yra pakankamos, konkrečiu atveju.

3. Kokios asmens duomenų apsaugos grėsmės/iššūkiai kyla viešojo administravimo institucijose? Kiek gaunate pranešimų, susijusių su asmens duomenų apsaugos pažeidimais viešojo administravimo institucijose? Kokio pobūdžio pažeidimai dažniausiai užfiksuojami?

Grėsmės ir iššūkiai visiems yra tokie patys. Radiją klausote, tai girdite, apie kibernetinis saugumas. Nes visada reikalaujama užtikrinti kaip įmanoma didesnes saugumo priemones. Bet mes suprantame, kad viešojo administravimo institucijos turi ribotą biudžetą ir paprastai tokiam dalykui, kaip kibernetinis saugumas, kaip atskirai sričiai nėra skiriama lėšų. Išskyrus, žinoma, KAM. O visiem kitiem, tai yra didelė problema. Pranešimų susijusių su pažeidimais gauname nedaug oficialiai. Bet mes manome, kad problema yra tame, kad pažeidimai vyksta ir jų yra nemažai, bet žmonės galbūt neidentifikuoja, kad tai kažkoks tai incidentas yra susijęs su asmens duomenų saugumo pažeidimu. Kokio pobūdžio pranešimai, negaliu atsakyti, kadangi tai nėra mano veiklos sritis.

4. Viešajame sektoriuje administracinių paslaugų teikimas vis plačiau teikiamas elektroninėje erdvėje. Kokie pažeidimai, susiję su administracinių paslaugų teikimu elektroninėje erdvėje dažniausiai užfiksuojami? Kaip dažnai?

Su elektroninių paslaugų teikimu, kad būtų užfiksuota pranešimų, inspekcija nėra daug užfiksavusi. Greičiau tai apskritai susiję, su asmens duomenų tvarkymu elektroninėje erdvėje. Pavyzdžiui gerai žinomas atvejis, su vyriausia rinkimų komisija.. atvejis, kai dėl techninių kliūčių buvo momentas, kai buvo galima susipažinti su trečiųjų asmenų duomenimis. Buvo atvejis su INFOSTATYBA taip pat. Apie šiuos atvejus plačiau rašoma mūsų svetainėje. Bet tokių atvejų nėra daug, galbūt ne visuomet mums yra pranešama apie tokius incidentus.

5. Nuo 2018 m. gegužės 25 d. bus pradėtas taikyti Bendrasis duomenų apsaugos reglamentas, kokie esminiai pokyčiai laukia viešojo administravimo institucijų? Kaip vertinate pasiruošimą Bendrojo duomenų apsaugos reglamento taikymui?

Daug kas keičiasi minimaliai. Visiškai nauja – tai duomenų apsaugos pareigūnas, pranešimai VDAI apie asmens duomenų pažeidimus. Pareigūnas, nesupraskite klaidingai, tai turėtų būti labiau patarėjas, kuris turėtų išmanyti organizacijos funkcijas. Tai tokia tarpinė tarp vadovybės, žmogaus, inspekcijos ir darbuotojų. Tai turėtų būti universalus žmogus, turėti pakankamai ekspertinių žinių. Tai nereiškia, kad tai būtinai turėtų būti teisininkas, na tiesiog... žmogus, išmanantis organizacijos veiklą. Bet tai yra visiško harmonizavimo klausimas ir papildomų reikalavimų, nei tai yra numatyta reglamente negali buti keliama.

Kalbant apie pasiruošimą, inspekcija parengė metodinę medžiagą, kad institucijoms ir įstaigoms būtų lengviau pasiruošti naujovėms. Organizuojame daug renginių ir seminarų, tame tarpe ir savivaldybėms, kadangi sulaukiame daug klausimų. Tačiau inspekcija nėra didelė institucija, ją sudaro viso labo 30 žmonių. Mes neturime galimybės kalbėtis su kiekviena institucija atskirai, todėl tai darome per renginius, kreipėsi ir savivaldybių asociacija į mus, tai kitais metais vyks renginys visų savivaldybių administracijų atstovams, kad informacija pasiektų ir mažiausius Lietuvos kampelius.