TVARKOMŲ ASMENS DUOMENŲ SAUGUMO PRIEMONIŲ IR RIZIKOS ĮVERTINIMO GAIRĖS DUOMENŲ VALDYTOJAMS IR DUOMENŲ TVARKYTOJAMS

4 versija
2024-08-13

Tvarkomų asmens duomenų saugumo priemonių ir rizikos įvertinimo gairės duomenų valdytojams ir duomenų tvarkytojams (toliau – gairės) parengtos remiantis Europos Sąjungos kibernetinio saugumo agentūros (ENISA) rekomendacijomis („Handbook on Security of Personal Data Processing“, 2018 m.) ir ISO standartais LST ISO/IEC 27001:2022 „Informacijos saugumas, kibernetinis saugumas ir privatumo apsauga. Informacijos saugumo valdymo sistemos. Reikalavimai“, LST ISO/IEC 27002:2022 „Informacijos saugumas, kibernetinis saugumas ir privatumo apsauga. Informacijos saugumo kontrolės priemonės“ bei ISO/IEC 27701:2019 „Saugumo metodai – ISO/IEC 27001 ir ISO/IEC 27002 papildymas dėl privatumo valdymo – Reikalavimai ir gairės“[1].

Dėl gairių taikymo organizacijoje

Prie visų šiose gairėse išvardytų priemonių yra pateikiama nuoroda į susijusį informacijos saugumo valdymo **standarto** LST ISO/IEC 27002:2022 **reikalavimą** ir jį papildantį **privatumo užtikrinimo reikalavimą** pagal ISO/IEC 27701:2019[2]. Paaiškinimai

[1] Oficialus standarto pavadinimas anglų kalba ISO/IEC 27701:2019 „Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines“.

[2] Atkreiptinas dėmesys, kad dalis terminų, vartojamų BDAR ir standarte ISO/IEC 27701:2019, skiriasi. Taip pat yra nežymių skirtumų tarp šių terminų apibrėžimų. BDAR apibrėžtas terminas „Asmens duomenys“ (angl. Personal data) atitinka ISO standarte vartojamą terminą „Asmenį identifikuojanti informacija“ (angl. Personally Identifiable Information (PII)), atitinkamai terminas „Duomenų valdytojas“ (angl. Data controller) – terminą „Asmens duomenų valdytojas“ (angl. PII controller), „Duomenų tvarkytojas“ (angl. Data processor)“ – „Asmens duomenų tvarkytojas“ (angl. PII processor), „Duomenų subjektas“ (angl. Data subject) – „Asmens duomenų subjektas“ (angl. PII principal), „Pritaikytoji duomenų apsauga“ (angl. Data protection by design) – „Pritaikytasis privatumas“ (angl. Privacy by design), „Standartizuotoji duomenų apsauga“ (angl. Data protection by default) – „Standartizuotasis privatumas“ (angl. Privacy by default).

pateikti atsižvelgiant į 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos **reglamentą** (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (toliau – **BDAR**).

Atkreipiame dėmesį, kad kuriant (diegiant) ar vertinant turimas organizacines ir technines saugumo priemones, organizacijos turi visapusiškai atsižvelgti į „duomenų tvarkymo pobūdį, aprėptį, kontekstą bei tikslus ir riziką, susijusią su pavojais fizinių asmenų teisėms ir laisvėms. BDAR 24 ir 32 straipsniai organizacijas įpareigoja **visais atvejais atlikti rizikos vertinimą**.

Gairės parengtos siekiant padėti duomenų valdytojams ir duomenų tvarkytojams, kurie priskiriami prie smulkiojo ar vidutinio verslo subjektų. Gairėmis taip pat gali naudotis ir kitos organizacijos (pvz., viešojo sektoriaus ar didelės įmonės) atsižvelgiant į vykdomos veiklos specifiką.

Gairėse yra pateikiama informacija, kuria gali vadovautis organizacijos, valdančios ir (ar) tvarkančios asmens duomenis (duomenų valdytojai ir duomenų tvarkytojai)[3], atlikdamos duomenų tvarkymo operacijas savo veikloje. Gairės padės įvertinti aktualius pavojus asmens duomenų saugumui ir įgyvendinti tinkamas saugumo priemones.

[3] Nors tekste vietomis yra minimas duomenų valdytojas ar organizacija, tačiau atitinkamos nuostatos yra taikomos ir duomenų tvarkytojams.

Turinys

Rizikos vertinimas

Šiose gairėse pateiktas rizikos vertinimo požiūris yra paremtas šiais keturiais žingsniais:

1. Duomenų tvarkymo operacijos nustatymas ir jos kontekstas;
2. Poveikio supratimas ir vertinimas;
3. Galimų grėsmių nustatymas ir jų atsiradimo tikimybės vertinimas;
4. Rizikos įvertinimas.

Po rizikos įvertinimo organizacija gali įgyvendinti (ar pasitikrinti jau įgyvendintas) technologines ir organizacines saugumo priemones (iš toliau pateikiamo sąrašo), kurios tinka nusistatytam rizikos lygiui. Rizikos vertinimas gali būti atliekamas, procesą skaidant į daugiau žingsnių, kuriuos gali nusistatyti pati organizacija.

1 žingsnis. Duomenų tvarkymo operacijos nustatymas ir jos kontekstas

Rizikos vertinimas prasideda organizacijai nustačius vertinamų asmens duomenų apimtį ir kontekstą. Siekiant padėti organizacijai tiksliau nustatyti asmens duomenų tvarkymo operacijos pobūdį, rekomenduotina atsižvelgti į šiuos klausimus:

1. Kokios yra organizacijos asmens duomenų tvarkymo operacijos?
2. Kokios kategorijos asmens duomenys yra tvarkomi?
3. Koks tvarkymo tikslas?
4. Kokios priemonės naudojamos tvarkyti asmens duomenis?
5. Kur[4] vykdomas asmens duomenų tvarkymas?
6. Kokios yra duomenų subjektų kategorijos?
7. Kas yra duomenų gavėjai?

Atsakydama į šiuos klausimus organizacija turi apsvarstyti įvairius duomenų tvarkymo etapus (rinkimą, saugojimą, naudojimą, perdavimą, sunaikinimą ir kt.).

2 žingsnis. Poveikio supratimas ir vertinimas

Remiantis 1 žingsnio analize organizacija turi įvertinti fizinių asmenų pagrindinėms teisėms ir laisvėms kylantį poveikį dėl galimo asmens duomenų saugumo pažeidimo. Nagrinėjami trys poveikio lygiai (žemas, vidutinis ir aukštas). Poveikio fiziniam asmeniui lygio reikšmių įvertinimas:

- **Žemas**: fizinis asmuo gali susidurti su tam tikrais nepatogumais (pvz., sugaištas laikas iš naujo suvedant informaciją, susierzinimas, nepasitenkinimas ir pan.);
- **Vidutinis**: fizinis asmuo gali patirti didelių nepatogumų, kuriuos jis galės įveikti nepaisant tam tikrų sunkumų (pvz., papildomos išlaidos, prieigos prie reikalingų išteklių praradimas, stresas, nedideli fiziniai negalavimai ir kt.);

[4] Ar asmens duomenys tvarkomi organizacijoje ar už jos ribų. Taip pat svarbu atkreipti dėmesį ar asmens duomenys bus tvarkomi už valstybės ribų, trečiosiose šalyse, nepriklausančiose Europos Ekonominei Erdvei.

- **Aukštas**: fizinis asmuo gali patirti reikšmingas pasekmes ir norint jas ištaisyti, pašalinti reikės susidurti su rimtais sunkumais (pvz., lėšų praradimas, asmens įtraukimas į finansinių institucijų juodąjį sąrašą, turto nuostoliai (žala), darbo vietos praradimas, teisminiai procesai, sveikatos būklės pablogėjimas ir pan.) arba dideles ar negrįžtamas pasekmes, kurių negalės ištaisyti, pašalinti (pvz., negalėjimas dirbti, ilgalaikiai psichiniai ar fiziniai negalavimai, mirtis ir pan.).

Poveikio vertinimas yra kokybinis procesas ir duomenų valdytojas privalo atsižvelgti į įvairius veiksnius, tokius kaip tvarkomų asmens duomenų kategorijos ir kiekis, duomenų tvarkymo operacijos svarba, organizacijos veiklos specifika, taip pat pažeidžiamų duomenų subjektų kategorijos (pvz., vaikai, pacientai) ar veiklos sritys.

Atkreiptinas dėmesys, kad jeigu organizacijoje specialių kategorijų ar pažeidžiamų asmenų asmens duomenys tvarkomi dideliu mastu, tai poveikis dėl galimo asmens duomenų saugumo pažeidimo turėtų būti vertinamas kaip „Aukštas“.

Specialių kategorijų asmens duomenys – tai duomenys, atskleidžiantys rasinę ar etninę kilmę, politines pažiūras, religinius ar filosofinius įsitikinimus, ar narystę profesinėse sąjungose; genetiniai duomenys, biometriniai duomenys, pagal kuriuos galima konkrečiai nustatyti fizinio asmens tapatybę; sveikatos duomenys; duomenys apie fizinio asmens lytinį gyvenimą ir lytinę orientaciją.

Siekiant organizacijai lengviau įvertinti poveikį, rekomenduotina naudotis šių gairių 1 lentele ir įvertinti atskirai poveikį dėl duomenų konfidencialumo, vientisumo ir prieinamumo praradimo. Vertinant poveikį, būtina atsižvelgti į rizikos veiksnius, kylančius ne tik iš organizacijos vidaus, bet ir išorinius, kuriems organizacija neturi įtakos (pvz., IT paslaugų tiekėjo bankrotas ir kt.).

Atlikus šį vertinimą gaunami trys skirtingi poveikio lygiai (dėl konfidencialumo, vientisumo ir prieinamumo praradimo). Aukščiausias nustatytas poveikis laikomas galutiniu poveikio, susijusio su bendru asmens duomenų tvarkymu, įvertinimo rezultatu.

1 lentelė. Poveikio vertinimo klausimai

Nr.	Klausimas	Poveikis
1.	Ar organizacijoje tvarkomi specialių kategorijų asmens duomenys?	☐ Taip ☐ Ne
2.	Nurodykite, kokį poveikį, Jūsų manymu, gali sukelti neleistinas tvarkomų asmens duomenų **atskleidimas**, **konfidencialumo praradimas** Jūsų organizacijos veiklos kontekste ir kokį tai galėtų turėti poveikį fiziniam asmeniui bei pateikite įvertinimą (pažymėkite poveikio lygį).	☐ Žemas ☐ Vidutinis ☐ Aukštas
3.	Nurodykite, kokį poveikį, Jūsų manymu, gali sukelti neleistinas tvarkomų asmens duomenų **pakeitimas**, **vientisumo praradimas** Jūsų organizacijos veiklos kontekste ir kokį tai galėtų turėti poveikį fiziniam asmeniui bei pateikite įvertinimą (pažymėkite poveikio lygį).	☐ Žemas ☐ Vidutinis ☐ Aukštas

4.	Nurodykite, kokį poveikį, Jūsų manymu, gali sukelti neleistinas tvarkomų asmens duomenų **sunaikinimas ar prieigos praradimas** Jūsų organizacijos veiklos kontekste ir kokį tai galėtų turėti poveikį fiziniam asmeniui bei pateikite įvertinimą (pažymėkite poveikio lygį).	☐ Žemas ☐ Vidutinis ☐ Aukštas

3 žingsnis. Galimų grėsmių nustatymas ir jų atsiradimo tikimybės vertinimas

Šiame etape organizacijai reikia nustatyti grėsmes, susijusias su visa asmens duomenų tvarkymo aplinka (išorės ir vidaus), ir įvertinti jų atsiradimo tikimybę.

Siekiant šį procesą supaprastinti yra pateikiami klausimai, skirti įvertinti organizacijos asmens duomenų tvarkymo aplinką (ji yra tiesiogiai susijusi su grėsmėmis) ir galimas grėsmes.

Šie klausimai yra susiję su keturiais pagrindiniais šios aplinkos aspektais (vertinimo
sritimis), tai yra:

- Tinklo ir techniniai ištekliai;
- Procesai ir procedūros, susiję su asmens duomenų tvarkymu;
- Duomenų tvarkymo dalyviai;
- Veiklos sritys ir duomenų tvarkymo mastai.

2 lentelėje pateikiami klausimai, susiję su grėsmių atsiradimo tikimybe ir skirti įvertinti organizacijos asmens duomenų tvarkymo aplinką bei galimas grėsmes.

2 lentelė. Grėsmių ir jų atsiradimo tikimybės vertinimo klausimai

Tinklo ir techniniai ištekliai		
1.	Ar organizacijoje yra sistemų ar įrenginių su asmens duomenimis, kurie prieinami internetu?	☐ Taip ☐ Ne
2.	Ar galima internetu prisijungti prie vidinių asmens duomenų tvarkymo sistemų (pvz., tam tikriems naudotojams arba naudotojų grupėms)?	☐ Taip ☐ Ne
3.	Ar organizacijos sistemos, kuriose tvarkomi asmens duomenys, yra tarpusavyje sujungtos, integruotos su kitomis išorinėmis ar vidinėmis (Jūsų organizacijos) informacinių technologijų (IT) sistemomis arba paslaugomis?	☐ Taip ☐ Ne
4.	Ar neįgalioti asmenys gali lengvai prieiti prie duomenų tvarkymo aplinkos (pvz., neužtikrinamas tinkamas fizinės prieigos prie IT įrangos saugumas)?	☐ Taip ☐ Ne
5.	Ar organizacijoje yra asmens duomenų tvarkymui naudojamų IT sistemų, kurios sukurtos ar įdiegtos nesilaikant gerosios praktikos (pvz., Agile, ISO 27000, ITIL ir kt.)?	☐ Taip ☐ Ne
Procesai ir procedūros, susiję su asmens duomenų tvarkymu		

6.	Ar organizacijoje prieigos ir (ar) atsakomybės yra neaiškios arba neaiškiai apibrėžtos?	☐ Taip ☐ Ne
7.	Ar organizacijoje yra / pasitaiko neaiškumų (dviprasmiškai suprantamų instrukcijų) dėl tinklo, sistemų ar fizinių išteklių naudojimo?	☐ Taip ☐ Ne
8.	Ar darbuotojams leidžiama naudoti asmeninius prietaisus, įrenginius ir jais prisijungti prie organizacijos sistemų, kuriose tvarkomi asmens duomenys?	☐ Taip ☐ Ne
9.	Ar darbuotojams leidžiama perkelti, saugoti ar kitaip tvarkyti organizacijos asmens duomenis už organizacijos ribų (pvz., nešiojamuosiuose įrenginiuose, laikmenose)?	☐ Taip ☐ Ne
10.	Ar asmens duomenų tvarkymo veiksmai gali būti atliekami, nefiksuojant jų (be veiksmų atsekamumo) sistemų žurnalų įrašuose (angl. log files)?	☐ Taip ☐ Ne
Duomenų tvarkymo dalyviai		
11.	Ar asmens duomenis tvarko neapibrėžtas (nenustatytas konkrečiai) darbuotojų skaičius?	☐ Taip ☐ Ne
12.	Ar yra organizacijos valdomų asmens duomenų, kuriuos tvarko duomenų tvarkytojai (pvz., rangovai, trečiosios šalys)?	☐ Taip ☐ Ne
13.	Ar organizacijoje yra dviprasmiškai arba neaiškiai apibrėžtų asmens duomenų tvarkymo prievolių, susijusių su trečiosiomis šalimis / asmenimis?	☐ Taip ☐ Ne
14.	Ar organizacijoje yra darbuotojų, dalyvaujančių asmens duomenų tvarkyme, bet kuriems trūksta kompetencijų konfidencialiai tvarkyti informaciją techniniu ar asmeninio sąžiningumo požiūriu?	☐ Taip ☐ Ne
15.	Ar organizacijoje yra darbuotojų arba duomenų tvarkytojų, dalyvaujančių asmens duomenų tvarkyme, kurie neturi galimybių tinkamai sunaikinti asmens duomenų laikmenų?	☐ Taip ☐ Ne
Veiklos sritys ir duomenų tvarkymo mastai		
16.	Ar manote, kad Jūsų organizacija, atsižvelgiant į jos veiklos sritį, potencialiai galėtų tapti dažnesniu kibernetinių atakų taikiniu?	☐ Taip ☐ Ne
17.	Ar per pastaruosius dvejus metus Jūsų organizacijoje buvo įvykęs asmens duomenų saugumo pažeidimas ar kitas saugumo incidentas?	☐ Taip ☐ Ne
18.	Ar per pastaruosius metus gavote kokius nors pranešimus ir (arba) skundus dėl IT sistemų, naudojamų asmens duomenų tvarkymui, saugumo?	☐ Taip ☐ Ne
19.	Ar organizacija tvarko asmens duomenis dideliu mastu?	☐ Taip ☐ Ne
	(Atsižvelgiama į šiuos veiksnius: susijusių duomenų subjektų skaičių – konkretų skaičių arba atitinkamo gyventojų skaičiaus procentinę dalį; duomenų vienetų kiekį ir (arba) intervalą; duomenų tvarkymo veiklos trukmę arba pastovumą; geografinę duomenų tvarkymo aprėptį (pvz.,	

	duomenys tvarkomi regioniniu, nacionaliniu ar tarpvalstybiniu lygmeniu).	
20.	Ar yra veiklai (veiklos sričiai) būdingos gerosios saugumo praktikos ar standartų, kurių Jūsų organizacijoje nesilaikoma?	☐ Taip ☐ Ne

Kiekvienai vertinamai sričiai gali būti nustatytas grėsmės atsiradimo tikimybės lygis:

- **Žemas**: mažai tikėtina, kad grėsmė pasitvirtins (jeigu iš penkių klausimų gautas ne daugiau kaip vienas atsakymai „Taip“);
- **Vidutinis**: yra reali galimybė, kad grėsmė pasitvirtins (jeigu iš penkių klausimų gauti ne mažiau kaip du ir ne daugiau kaip trys atsakymai „Taip“);
- **Aukštas**: tikėtina, kad grėsmė pasitvirtins (jeigu iš penkių klausimų gauti daugiau kaip trys atsakymai „Taip“).

Tuomet, pasinaudojant 3 ir 4 lentelėmis, galima nustatyti grėsmės atsiradimo tikimybę kiekvienai vertinamai sričiai ir atitinkamai apskaičiuoti jos galutinę vertę.

3 lentelė. Grėsmės atsiradimo tikimybės įvertinimas kiekvienai sričiai

Vertinimo sritis	Tikimybė	
	Lygis	Balas
Tinklo ir techniniai ištekliai	☐ Žemas	1
	☐ Vidutinis	2
	☐ Aukštas	3
Procesai ir procedūros, susiję su asmens duomenų tvarkymu	☐ Žemas	1
	☐ Vidutinis	2
	☐ Aukštas	3
Duomenų tvarkymo dalyviai	☐ Žemas	1
	☐ Vidutinis	2
	☐ Aukštas	3
Veiklos sritys ir duomenų tvarkymo mastai	☐ Žemas	1
	☐ Vidutinis	2
	☐ Aukštas	3

4 lentelė. Grėsmės atsiradimo įvertinimas

Bendra grėsmės atsiradimo balų suma	Grėsmės atsiradimo tikimybės lygis
4–5	Žemas
6–8	Vidutinis

9–12	Aukštas

Galutinis grėsmės atsiradimo tikimybės lygis apskaičiuojamas sudėjus kiekvienos iš keturių vertinimo sričių balus, gautus pagal 3 lentelę, ir susiejus rezultatą su 4 lentelės balais.

4 žingsnis. Rizikos įvertinimas

Įvertinus asmens duomenų tvarkymo operacijos **poveikį** ir atitinkamos **grėsmės atsiradimo tikimybę**, pasinaudojant 5 lentele galima atlikti galutinį **rizikos įvertinimą**.

5 lentelė. Rizikos įvertinimas

		Poveikio lygis		
		Žemas	**Vidutinis**	**Aukštas**
Grėsmės atsiradimo tikimybės lygis	**Žemas**	**(Ž)**	**(V)**	**(A)**
	Vidutinis	**(Ž)**	**(V)**	**(A)**
	Aukštas	**(V)**	**(A)**	**(A)**

Rizikos lygio žymėjimas:						
(Ž)	žemas	**(V)**	vidutinis	**(A)**	aukštas	

Organizacija, įvertinusi rizikos lygį, gali pasirinkti tinkamas saugumo priemones asmens duomenų saugumui užtikrinti. Duomenų saugumo priemonės skirstomos į keturias grupes: organizacines kontrolės priemones, žmonių kontrolės priemones, fizines kontrolės priemones ir technologines kontrolės priemones, kurios atitinka BDAR 32 str. nurodytas organizacines ir technines saugumo priemones.

Duomenų saugumo priemonės toliau papildomai skirstomos ir žymimos spalvomis ir raidėmis pagal rizikos lygį: žemas – žalia, raidėmis (Ž); vidutinis – geltona, raidėmis (V); aukštas – raudona, raidėmis (A).

Siekiant, kad skirtingų rizikos lygių priemonės būtų tarpusavyje suderintos, laikytina, kad visos žemam rizikos lygiui (žalios spalvos, žymimos raidėmis (Ž)) siūlomos priemonės tinka visiems lygiams. Priemonės, pateiktos vidutiniam rizikos lygiui (geltona spalva, žymimos raidėmis (V)), taikomos ir aukštam rizikos lygiui. O aukštam rizikos lygiui (raudonos spalvos, žymimos raidėmis (A)) siūlomos priemonės nėra taikomos jokiam kitam rizikos lygiui.

Nepaisant gauto galutinio rezultato, organizacija gali patikslinti gautą rizikos lygį atsižvelgdama į konkrečias duomenų tvarkymo operacijos savybes (kurių nebuvo vertinimo proceso metu) ir tinkamai pateisindama ir pagrįsdama šį koregavimą.

Pažymėtina, kad priemonių taikymas konkretiems rizikos lygiams neturėtų būti suprantamas kaip absoliutus. Priklausomai nuo asmens duomenų tvarkymo konteksto, organizacija gali svarstyti papildomų priemonių įgyvendinimą, net jei jos priskirtos aukštesniam rizikos lygiui. Taip pat gali prireikti papildomų priemonių, neįtrauktų

į šį dokumentą, kad būtų atsižvelgta į konkrečius organizacijos poreikius ir nustatytas rizikas. Be to, siūlomame priemonių sąraše neatsižvelgiama į kitus papildomai konkrečiam veiklos sektoriui taikomus ar būdingus saugumo reikalavimus ar į konkrečias įstatymų nustatytas prievoles.

Kai kuriais atvejais, įvertinus organizacijos asmens duomenų tvarkymo operacijas, **gali būti nustatomas ne bendras visos organizacijos saugumo lygis, bet atskiri saugumo lygiai** (jie gali skirtis) pagal veiklos sritis ar veiklos procesus, ir tada atitinkamai parenkamos ir įgyvendinamos techninės ir organizacinės saugumo priemonės.

Organizacinės kontrolės priemonės

Nr.	Priemonės	Atitikmuo ISO 27002:2022	Atitikmuo BDAR ir paaiškinimai
Asmens duomenų saugumo politika ir procedūros			
1. (Ž)	Asmens duomenų ir jų tvarkymo saugumas organizacijoje (asmens duomenų saugumo politika) turi būti dokumentuotas kaip informacijos saugumo politikos dalis, kurioje numatyta asmens duomenų konfidencialumo, vientisumo ir prieinamumo kontrolės priemonės.	**5.1 Informacijos saugumo politika** **5.33 Įrašų apsauga** **5.36 Atitiktis informacijos saugumo politikai, taisyklėms ir standartams** **5.37 Dokumentuotos veiklos procedūros**	Saugumo politika yra svarbus dokumentas, nustatantis pagrindinius informacijos saugumo ir asmens duomenų apsaugos principus organizacijoje. Tai yra visų konkrečių techninių ir organizacinių duomenų saugumo priemonių įgyvendinimo pagrindas pagal BDAR 32 straipsnį ir jį papildantį 24 straipsnį dėl duomenų valdytojo įgyvendinamos atitinkamos duomenų apsaugos politikos. Remiantis saugumo politika, konkrečios techninės ir organizacinės (išskiriamos į organizacines, žmonių, fizines ir technologines) kontrolės priemonės aprašomos detalesnėse politikose (pvz., prieigos kontrolės, įrenginių valdymo, išteklių valdymo ir kt.). Saugumo politika nustato bendrą organizacijos informacijos saugos valdymą ir joje turi būti aiškiai išskirta asmens duomenų apsauga.
2. (Ž)	Asmens duomenų saugumo politika turi atitikti teisinius, įstatyminius, reguliavimo ir sutartinius reikalavimus bei būti peržiūrima ir prireikus atnaujinama ne rečiau kaip kartą per metus.		
3. (V)	Asmens duomenų saugumo politika turi būti perduota susipažinti atitinkamam personalui ir suinteresuotosioms šalims. Asmens duomenų saugumo politikos gavėjai turi būti patvirtinę, jog jie ją supranta ir sutinka jos laikytis (jei taikoma).		

4. (V)	Asmens duomenų saugumo politika turi nustatyti bent: prieigos valdymą, turto valdymą, informacijos perdavimą, asmens duomenų saugumo pažeidimų valdymą, atsarginių kopijų darymo tvarką, personalo pareigas (funkcijas) ir atsakomybes, organizacines, žmonių, fizines ir technologines informacijos saugumo priemones, įdiegtas asmens duomenų saugumui užtikrinti, taip pat duomenų tvarkytojų ar trečiųjų šalių, susijusių su asmens duomenų tvarkymu, sąrašą.		
5. (V)	Atsižvelgiant į asmens duomenų saugumo politiką, turi būti sukurtos ir prižiūrimos su asmens duomenų tvarkymu susijusios veiklos procedūros. Veiklos procedūrose turėtų būtų nurodyti atsakingi asmenys, saugaus asmens duomenų tvarkymo taisyklės ir reagavimas į asmens duomenų saugumo pažeidimus.		
6. (A)	Asmens duomenų saugumo politika turi būti peržiūrima ir, prireikus, tikslinama ne rečiau kaip kas pusmetį		

	arba įvykus reikšmingiems pokyčiams.		
7. (A)	Organizacijos atitikties asmens duomenų saugumo politikai vertinimas turi būti atliekamas ne rečiau kaip kartą per metus.		
Vaidmenys ir atsakomybės[5]			
8. (Ž)	Su asmens duomenų tvarkymu susiję vaidmenys ir atsakomybės turi būti aiškiai apibrėžti ir paskirstyti pagal asmens duomenų saugumo politiką.	**5.2 Informacijos saugumo vaidmenys ir atsakomybės** **5.3 Pareigų atskyrimas**	BDAR 32 straipsnio 4 dalis numato, kad duomenų valdytojas ir duomenų tvarkytojas imasi priemonių, siekdami užtikrinti, kad bet kuris duomenų valdytojui arba duomenų tvarkytojui pavaldus fizinis asmuo, galintis susipažinti su asmens duomenimis, jų netvarkytų, išskyrus atvejus, kai duomenų valdytojas duoda nurodymus juos tvarkyti, nebent tas asmuo privalo tai daryti pagal Europos Sąjungos arba valstybės narės teisę. Pagrindinės asmens duomenų saugumo priemonės organizacijos personalui, turinčiam prieigą prie asmens duomenų – aiškiai apibrėžta ir dokumentuota atsakomybė bei vaidmenys, taip pat darbo su asmens duomenimis kompetencijos. Pvz., saugos specialistas (ar įgaliotinis), kuris yra atsakingas už tinkamos saugumo politikos įgyvendinimą. Duomenų apsaugos pareigūnas (toliau – DAP), kurio viena iš užduočių yra stebėti, kaip organizacijoje laikomasi BDAR (tam tikrais atvejais pagal BDAR 37 straipsnį DAP paskyrimas yra privalomas). Institucinis skaitmeninimo įgaliotinis, kuris pagal Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymą atsako už skaitmeninimo veiklos ir skaitmenizavimo veiklos įgyvendinimo koordinavimą ir kontrolę. Duomenų valdymo įgaliotinis, kuris pagal Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymą yra atsakingas už institucijos
9. (Ž)	Turi būti aiškiai apibrėžtas darbuotojų teisių ir pareigų atšaukimas taikant atitinkamas vaidmenų ir atsakomybių perdavimo ar perleidimo procedūras (vidaus organizacijos pertvarkymo ar darbuotojų atleidimo, funkcijų pasikeitimo metu).		
10. (V)	Turi būti paskirti atsakingi asmenys, saugos specialistas (saugos įgaliotinis) ir duomenų apsaugos pareigūnas (jei taikoma), už konkrečias asmens duomenų saugumo užduotis organizacijoje.		

[5] Mažose įmonėse (kai dirba tik vienas ar keli darbuotojai) tas pats asmuo dažnai atlieka kelis vaidmenis. Svarbu užtikrinti, kad darbuotojai turėtų aiškiai apibrėžtus vaidmenis ir atsakomybes. Jei įmanoma, tam tikras funkcijas galima deleguoti išoriniams tiekėjams.

11. (A)	Nesuderinamos pareigybės (funkcijos) ir atsakomybių sritys, pavyzdžiui, saugos specialisto pareigybė turėtų būti atskirta nuo duomenų apsaugos pareigūno, IT administratoriaus, vadovo pareigybių, siekiant sumažinti neleistino ar netyčinio asmens duomenų keitimo ar netinkamo naudojimo galimybes, bei saugumo kontrolės priemonių apėjimo riziką.		skaitmeninimą, duomenų valdysenos tikslų, valdymo ir tvarkymo principų, metodų ir priemonių įgyvendinimą. Tiek saugos specialistas (ar įgaliotinis), tiek DAP, tiek institucinis skaitmeninimo įgaliotinis, tiek duomenų valdymo įgaliotinis turi glaudžiai bendradarbiauti.
12. (A)	Turi būti paskirti atsakingi asmenys už organizacijos IT (IS, tarnybinių stočių, kompiuterinių darbo vietų, mobilių / nešiojamų įrenginių, programinės įrangos) išteklių (naudojamų asmens duomenims tvarkyti) priežiūrą.		
Prieigos valdymas ir teisės			
13. (Ž)	Bendrieji prieigos valdymo reikalavimai (prieigos teisių suteikimo / keitimo / panaikinimo tvarka) turi būti dokumentuoti kaip asmens duomenų saugumo politikos dalys.	**5.15 Prieigos valdymas** **5.18 Prieigos teisė**	Būtina nustatyti prieigos kontrolės politiką sistemoms, naudojamoms tvarkant asmens duomenis. Kontrolė turi būti grindžiama principais „būtina žinoti“ bei „būtina naudoti“, t. y. kiekvienam vaidmeniui ar naudotojui turi būti suteiktas tik toks asmens duomenų prieinamumo lygis, kuris yra būtinas jo užduotims atlikti. Šie reikalavimai glaudžiai susiję su vientisumo ir konfidencialumo principu (BDAR 5 straipsnio 1 dalies f punktas). Prieigos kontrolės politika turi būti įgyvendinama taikant tinkamas technologines priemones (taip pat žiūrėti technologines priemones,
14. (Ž)	Kiekvienam vaidmeniui, susijusiam su asmens duomenų tvarkymu, turi būti priskirtos konkrečios prieigos		

	kontrolės teisės, vadovaujantis „būtina žinoti“ (angl. need to know) ir / arba „būtina naudoti“ (angl. need to use) principais.		nurodytas šių gairių 84–93 punktuose „Prieigų kontrolė ir autentifikavimas“).
15. (V)	Prieigos valdymo politika turi būti išsami ir dokumentuota. Organizacija šiame dokumente turi nustatyti atitinkamas prieigos kontrolės taisykles, prieigos teises ir apribojimus pagal konkrečias naudotojų pareigas, susijusias su asmens duomenų tvarkymo procesais ir procedūromis.		
16. (V)	Prieigos valdymo kontrolę užtikrinančių funkcijų atskyrimas (pvz., prieigos užklausų, prieigos leidimų, pačios prieigos administravimas) turi būti aiškiai apibrėžtas ir dokumentuotas.		
17. (V)	Tam tikros pareigybės (funkcijos), turinčios dideles prieigos teises (privilegijuotosios prieigos teisės), turi būti aiškiai apibrėžtos ir priskirtos tik ribotam darbuotojų skaičiui.		
18. (A)	Prieigos teisės turi būti suteikiamos / keičiamos pagal veiklos reikalavimus (vaidmenis) ir prieigos valdymo taisykles, bei gavus vadovybės leidimą / patvirtinimą (prieigos teisės		

	būtų aktyvuojamos tik sėkmingai atlikus visas procedūras). Prieigos teisės turi būti panaikinamos kai nebereikia prieigos (pasikeitė veikla, pareigos) prie asmens duomenų. Ypatingai svarbu, kad organizacija nedelsiant panaikintų prieigos teises naudotojams, kurie nutraukė darbo / sutartinius santykius su organizacija (laikas, pvz., ne vėliau kaip paskutinę darbo / sutartinių santykių dieną, turi būti numatytas prieigos valdymo politikoje).		
19. (A)	Būtina turėti registrą, kuriame saugoma informacija (įskaitant prašymus) apie prieigos teisių suteikimą, keitimą ir panaikinimą.		
20. (A)	Prieigos teisės (ypač privilegijuotosios prieigos teisės) turi būti peržiūrimos ne rečiau kaip kartą per metus.		
Išteklių ir turto valdymas			
21. (Ž)	Organizacija turi turėti išteklių, naudojamų asmens duomenims tvarkyti, registrą. Išteklių registras turi apimti bent tokią informaciją: IT išteklių tipą (pvz., tarnybinę stotį,	**5.9 Informacijos ir kito susijusio turto apyrašas** **5.10 Priimtinas informacijos ir**	Tinkamas techninės, programinės ir tinklo įrangos valdymas yra būtinas asmens duomenų saugumui ir vientisumui (vientisumo ir konfidencialumo principas apibrėžtas BDAR 5 straipsnio 1 dalies f punkte), nes tai leidžia kontroliuoti duomenų tvarkymo priemones. Išteklių valdymas būtinai turi

	kompiuterinę darbo vietą, virtualias mašinas), vietą (fizinę ar elektroninę), išorės paslaugų tiekėjus (jeigu pasitelkiami). Išteklių registro tvarkymas turi būti priskirtas konkrečiam asmeniui.	**kito susijusio turto naudojimas 5.11 Turto grąžinimas**	apimti IT išteklių ir tinklo topologijos (schemos), kuri yra naudojama tvarkant asmens duomenis, registravimą.
22. (Ž)	Išteklių registras turi būti reguliariai peržiūrimas ir atnaujinamas.		
23. (V)	Visos pareigybės, turinčios prieigą prie išteklių, turi būti apibrėžtos ir patvirtintos dokumentais.		
24. (V)	Turi būti nustatytos, dokumentuotos ir įgyvendintos išteklių (pvz. debesijos paslaugų, asmeninių įrenginių, duomenų tvarkytojų paslaugų) naudojimo taisyklės bei tvarkymo procedūros.		
25. (A)	Ne rečiau kaip kartą per metus turi būti atliekamas informacijos ir kito susijusio turto atitikties vertinimas pagal organizacijos išteklių (naudojamų asmens duomenims tvarkyti) registrą (techninės, programinės ir tinklo įrangos sąrašą).		
26. (A)	Turi būti nustatytos, dokumentuotos ir įgyvendintos tvarkomų asmens duomenų grąžinimo / sunaikinimo bei išteklių grąžinimo procedūros		

	pasibaigus darbo santykiams / sutarčiai.		
Duomenų tvarkytojai			
27. (Ž)	Prieš pradedant vykdyti asmens duomenų tvarkymą, duomenų valdytojai turi apibrėžti, dokumentuoti ir suderinti formalias gaires ir procedūras, taikomas duomenų tvarkytojams (pvz., rangovams ar užsakomųjų paslaugų tiekėjams) dėl asmens duomenų tvarkymo. Šios gairės ir procedūros turi nustatyti tokį patį (ne žemesnį) asmens duomenų saugumo lygį, koks yra numatytas organizacijos saugumo politikoje.	**5.19 Informacijos saugumas palaikant santykius su tiekėjais (teikėjais)** **5.20 Informacijos saugumo užtikrinimas su tiekėjais (teikėjais) susitarimuose** **5.22 Tiekėjų (teikėjų) paslaugų stebėsena, peržiūra ir pakeitimų valdymas** **5.23 Informacijos saugumas naudojantis debesijos paslaugomis**	BDAR 28 straipsnis numato, kad „duomenų valdytojas pasitelkia tik tuos duomenų tvarkytojus, kurie pakankamai užtikrina, kad tinkamos techninės ir organizacinės priemonės bus įgyvendintos tokiu būdu, kad duomenų tvarkymas atitiktų šio reglamento reikalavimus ir būtų užtikrinta duomenų subjekto teisių apsauga.“ Tame pačiame straipsnyje nurodoma, kad duomenų valdytojo ir duomenų tvarkytojo santykiai turi būti apibrėžti sutartyje ar teisės akte. Analogiški saugumo reikalavimai turi būti taikomi ir tais atvejais, kai duomenų tvarkytojas konkrečiai duomenų tvarkymo veiklai duomenų valdytojo vardu atlikti pasitelkia kitą duomenų tvarkytoją.
28. (Ž)	Duomenų tvarkytojas privalo nedelsdamas (rekomenduotina ne vėliau nei per 24 valandas) pranešti duomenų valdytojui apie nustatytus asmens duomenų saugumo pažeidimus. Turi būti numatyta aiški privaloma informacija, kurią duomenų tvarkytojas pranešime turi pateikti duomenų valdytojui, bei turi būti numatytas kontaktinis asmuo asmens duomenų saugumo klausimais.		

29. (Ž)	Duomenų valdytojas turi gauti iš duomenų tvarkytojo dokumentais pagrįstus įrodymus dėl atitikties keliamiems asmens duomenų saugumo reikalavimams ir įsipareigojimams.		
30. (V)	Duomenų valdytojas turi reguliariai tikrinti duomenų tvarkytojo atitiktį nustatytiems reikalavimams ir įsipareigojimams.		
31. (A)	Duomenų tvarkytojo darbuotojams, dirbantiems su asmens duomenimis, turi būti taikomi konkretūs, dokumentais įtvirtinti, informacijos konfidencialumo, neatskleidimo įsipareigojimai.		
32. (A)	Turi būti aiškiai nustatytos ir dokumentuotos atsakomybės, dalyko politika [6] dėl santykių su tiekėjais (teikėjais) bei dėl debesijos paslaugų naudojimo, taip pat turi būti nustatyti informacijos saugumo reikalavimai, susiję su duomenų tvarkytojais ir debesijos paslaugų naudojimu.		
Asmens duomenų saugumo pažeidimai ir saugumo incidentai			

[6] Dalyko politika - konkretaus dalyko, klausimo ar srities politika, kuria reguliuojami tam tikri veiklos aspektai, tvarkos ir procedūros. Tai gali apimti įvairius politikos dokumentus, taisykles ar gaires, nustatytas siekiant užtikrinti tinkamą veiklos reguliavimą ir valdymą tam tikroje srityje.

33. (Ž)	Turi būti nustatytas reagavimo į saugumo incidentus planas, vaidmenys ir atsakomybės, kontaktinis asmuo, užtikrinantys greitą ir veiksmingą incidentų, susijusių su asmens duomenų saugumu, valdymą. Visa organizacija turi būti supažindinta su reagavimo į saugumo incidentus planu.	**5.5 Ryšiai su institucijomis** **5.24 Informacijos saugumo incidentų valdymo planavimas ir parengimas** **5.25 Informacijos saugumo įvykių vertinimas ir sprendimų dėl jų priėmimas** **5.26 Reagavimas į informacijos saugumo incidentus** **5.27 Mokymasis iš informacijos saugumo incidentų** **5.28 Įrodymų rinkimas**	Asmens duomenų saugumo pažeidimas – saugumo pažeidimas, dėl kurio netyčia arba neteisėtai sunaikinami, prarandami, pakeičiami, be leidimo atskleidžiami persiųsti, saugomi arba kitaip tvarkomi asmens duomenys arba prie jų be leidimo gaunama prieiga (BDAR 4 straipsnio 12 dalis). Duomenų valdytojai turi būti tikri, kad jie laikosi savo įsipareigojimų pagal BDAR 33 ir 34 straipsnius, susijusius su pranešimu apie asmens duomenų saugumo pažeidimus priežiūros institucijai ir duomenų subjektams. Duomenų tvarkytojai taip pat turi būti tikri, kad jie laikosi savo įsipareigojimų pagal BDAR 33 straipsnį ir galės nedelsdami pranešti duomenų valdytojui apie minėtus pažeidimus. Bet kuriuo atveju, tiek duomenų valdytojai, tiek ir duomenų tvarkytojai turi turėti tinkamas procedūras ne tik pranešti apie asmens duomenų pažeidimus, bet ir juos suvaldyti.
34. (Ž)	Asmens duomenų saugumo pažeidimai turi būti fiksuojami (dokumentuojami). Apie juos turi būti nedelsiant pranešama vadovybei. Turi būti nustatyta pranešimo apie asmens duomenų saugumo pažeidimus kompetentingoms institucijoms ir duomenų subjektams tvarka pagal Bendrojo duomenų apsaugos reglamento (BDAR) 33 ir 34 straipsnius. Žinios, įgytos iš asmens duomenų saugumo pažeidimų, turėtų būti naudojamos asmens duomenų saugumo kontrolės priemonėms stiprinti ir gerinti.		
35. (V)	Saugumo incidentų likvidavimo planas turi būti patvirtintas dokumentais, tarp kurių būtų galimų		

	saugumo incidento poveikio mažinimo priemonių sąrašas ir aiškus atskirų funkcijų paskirstymas.		
36. (A)	Visi saugumo incidentai, įskaitant ir asmens duomenų saugumo pažeidimus, turi būti fiksuojami kartu su visa susijusia informacija apie įvykį ir vėliau atliktus incidento poveikio mažinimo veiksmus.		
Veiklos tęstinumas			
37. (Ž)	Organizacija turi nustatyti pagrindines procedūras, kurių reikia laikytis saugumo incidento ar asmens duomenų saugumo pažeidimo atveju, kad būtų užtikrintas reikiamas asmens duomenų tvarkymo IT sistemomis tęstinumas ir prieinamumas.	**5.29 Informacijos saugumas sutrikdymo metu**	Veiklos ar paslaugų tęstinumo planas yra būtinas nustatant procesus ir technologines priemones, kurių organizacija turi laikytis saugumo incidento ar asmens duomenų saugumo pažeidimo atveju. Šis planas papildo organizacijos saugumo politiką. Ši priemonė aiškiai susijusi su BDAR 32 straipsnio 1 dalies c punktu, kuris įpareigoja duomenų valdytoją ir tvarkytoją „laiku atkurti sąlygas ir galimybes naudotis asmens duomenimis fizinio ar techninio incidento atveju“.
38. (V)	Veiklos tęstinumo planas turi būti išsamiai dokumentuotas (laikantis bendros saugumo politikos). Jame turi būti pateiktas aiškus veiksmų planas ir funkcijų paskirstymas.		
39. (V)	Veiklos tęstinumo plane turi būti apibrėžtas garantuotas paslaugų lygio susitarimas (angl. Service-level agreement (SLA)), kuriuo nustatomas teikiamų paslaugų mąstas.		

40. (A)	Turi būti paskirti darbuotojai, kurie turi reikiamą atsakomybę, įgaliojimus ir kompetenciją valdyti veiklos tęstinumą asmens duomenų saugumo pažeidimo atveju.		
41. (A)	Turi būti numatyta ir išbandyta organizacijos darbui skirta alternatyvi infrastruktūros priemonė, atsižvelgiant į organizaciją ir jai priimtiną IT sistemų prastovą.		
Asmens duomenų perdavimas			
42. (Ž)	Organizacijoje turi būti numatytos ir taikomos asmens duomenų perdavimo procedūros ir priemonės.	**5.14 Informacijos perdavimas**	Asmens duomenų perdavimas yra svarbi asmens duomenų tvarkymo proceso dalis. Siekiant apsisaugoti nuo konfidencialumo praradimo asmens duomenų perdavimo metu, reikia nustatyti pagrindinius informacijos perdavimo principus organizacijoje.
43. (V)	Asmens duomenų perdavimo politika turi būti dokumentuota asmens duomenų saugumo politikoje. Asmens duomenų perdavimo politiką turi sudaryti taisyklės reglamentuojančios informacijos perdavimą elektroniniu, fiziniu ir verbaliniu perdavimo būdu.		
44. (A)	Asmens duomenų perdavimo politikoje turi būti numatyta, kad kai asmens duomenys perduodami elektroninių ryšių priemonėmis (pvz., el. paštu, per el. duomenų saugyklas) iš pradžių jie turi būti		

	užšifruojami ir apsaugomi slaptažodžiu. Slaptažodis turi būti perduodamas atskiru, alternatyviu, komunikacijos kanalu.		
45. (A)	Asmens duomenų perdavimo politikoje turi būti numatyta, kad kai asmens duomenys perduodami naudojantis fizinėmis laikmenomis, fizinės laikmenos turi būti naudojamos užšifruotos (pvz., BitLocker, VeraCrypt), apsaugotos slaptažodžiu arba informacija prieš keliant į fizines laikmenas turi būti užšifruojama ir apsaugoma slaptažodžiu. Slaptažodis turi būti perduodamas atskiru, alternatyviu, komunikacijos kanalu.		
46. (A)	Asmens duomenų perdavimo politikoje turi būti numatyta, kad už organizacijos ribų, viešose vietose, personalas nesileistų į konfidencialius pokalbius, kad neįgaliotiems asmenims asmens duomenys nebūtų atskleidžiami.		

Žmonių kontrolės priemonės

Nr.	Priemonės	Atitikmuo ISO 27002:2022	Atitikmuo BDAR ir paaiškinimai
Darbo santykiai			
47. (Ž)	Darbo sutartyje arba kitame dokumente turi būti aiškiai numatyti vaidmenys ir atsakomybės, bei įsipareigojimai susiję su organizacijoje taikoma asmens duomenų saugumo politika.	**6.2 Įdarbinimo sąlygos** **6.5 Atsakomybės po darbo santykių nutraukimo arba pakeitimo**	Siekiant užtikrinti asmens duomenų konfidencialumą pagal BDAR 32 straipsnį, organizacija turi užtikrinti, kad jos darbuotojai gebėtų konfidencialiai tvarkyti informaciją tiek techniniu, tiek asmeninio sąžiningumo požiūriu. Be to, BDAR 32 straipsnio 4 dalis (atitinkamai BDAR 29 straipsnis) numato, kad „duomenų valdytojas ir duomenų tvarkytojas imasi priemonių, siekdami užtikrinti, kad bet kuris duomenų valdytojui arba duomenų tvarkytojui pavaldus fizinis asmuo, galintis susipažinti su asmens duomenimis, jų netvarkytų, išskyrus atvejus, kai duomenų valdytojas duoda nurodymus juos tvarkyti, nebent tas asmuo privalo tai daryti pagal Sąjungos arba valstybės narės teisę“. Šiuo tikslu turi būti nustatytos specialios priemonės, užtikrinančios, kad asmenys, dalyvaujantys tvarkant asmens duomenis, būtų tinkamai informuojami apie savo pareigą laikytis konfidencialumo. Taip pat turi būti užtikrinta, kad šios pareigos būtų pakankamai apibrėžtos organizacijos žmogiškųjų išteklių politikoje.
48. (Ž)	Turi būti aiškiai numatytos atsakomybės bei įsipareigojimai pasibaigus darbo santykiams (pvz., konfidencialumo; asmens duomenų grąžinimo / sunaikinimo).		
Personalo ugdymas			
49. (Ž)	Organizacijoje personalas turi suprasti savo atsakomybes, pagrindines asmens duomenų saugumo procedūras ir pagrindines kontrolės priemones, užtikrinant asmens duomenų saugumą.	**6.3 Informacijos saugumo suvokimas, švietimas ir mokymai**	Personalo mokymai apie duomenų apsaugos ir saugumo procedūras (pvz., slaptažodžių naudojimas ir prieiga prie konkrečių IT sistemų) yra svarbūs tinkamam organizacinių ir techninių duomenų saugumo priemonių įgyvendinimui ir prevencijai dėl „netyčinio duomenų sunaikinimo, praradimo, pakeitimo, atskleidimo be leidimo ar neteisėtos prieigos prie jų“ (BDAR 32 straipsnio 2 dalis). Žinios apie konkrečius

50. (Ž)	Organizacija turi užtikrinti, kad visi darbuotojai būtų tinkamai informuoti apie IT sistemų saugumo reikalavimus, susijusius su jų kasdieniu darbu. Darbuotojai, susiję su asmens duomenų tvarkymu, turi būti mokomi apie atitinkamus duomenų saugumo reikalavimus ir atsakomybes, rengiant reguliarius mokymus, informavimo renginius ar instruktažus. Siūlomas mokymų periodiškumas – kartą per metus.	**6.4 Drausminis procesas**	duomenų apsaugos teisinius įsipareigojimus taip pat yra svarbios, ypač tiems asmenims, kurie dalyvauja didelės rizikos asmens duomenų tvarkymo procesuose.
51. (Ž)	Organizacija turi užtikrinti, kad personalas suprastų asmens duomenų saugumo politikos pažeidimo pasekmes, organizacijos drausminį procesą, tam, kad nepažeistų asmens duomenų saugumo politikos, su asmens duomenų saugumu susijusios konkretaus dalyko politikos ir procedūrų.		
52. (V)	Organizacijos nuolatinėse personalo mokymų programose turi būti įtraukta speciali programa, skirta mokyti naujus darbuotojus duomenų apsaugos bei kibernetinio saugumo tema.		

53. (A)	Kiekvienais metais turi būti parengtas ir įgyvendintas mokymų planas, kuriame būtų nustatyti siektini tikslai ir uždaviniai.		
Personalo konfidencialumas			
54. (Ž)	Vaidmenys ir atsakomybės turi būti aiškiai išdėstyti darbuotojui prieš pradedant vykdyti jam paskirtas funkcijas ir darbus.	**6.6 Konfidencialumo arba informacijos neatskleidimo susitarimai**	Siekiant užtikrinti asmens duomenų konfidencialumą pagal BDAR 32 straipsnį, organizacija turi užtikrinti, kad jos darbuotojai gebėtų konfidencialiai tvarkyti informaciją tiek techniniu, tiek asmeninio sąžiningumo požiūriu. Be to, BDAR 32 straipsnio 4 dalis (atitinkamai BDAR 29 straipsnis) numato, kad „duomenų valdytojas ir duomenų tvarkytojas imasi priemonių, siekdami užtikrinti, kad bet kuris duomenų valdytojui arba duomenų tvarkytojui pavaldus fizinis asmuo, galintis susipažinti su asmens duomenimis, jų netvarkytų, išskyrus atvejus, kai duomenų valdytojas duoda nurodymus juos tvarkyti, nebent tas asmuo privalo tai daryti pagal Sąjungos arba valstybės narės teisę“. Šiuo tikslu turi būti nustatytos specialios priemonės, užtikrinančios, kad asmenys, dalyvaujantys tvarkant asmens duomenis, būtų tinkamai informuojami apie savo pareigą laikytis konfidencialumo. Taip pat turi būti užtikrinta, kad šios pareigos būtų pakankamai apibrėžtos organizacijos žmogiškųjų išteklių politikoje.
55. (V)	Darbuotojai, prieš pradėdami eiti savo pareigas, turi būti pasirašytinai supažindinti su asmens duomenų saugumo politika, taip pat pasirašyti atitinkamus informacijos konfidencialumo ir neatskleidimo įsipareigojimus.		
56. (A)	Darbuotojai, atsakingi už aukštos rizikos asmens duomenų tvarkymo operacijas, turi laikytis konkrečių jiems taikomų konfidencialumo sąlygų (pagal jų darbo sutartį ar kitus teisės aktus).		
Nuotolinis darbas			
57. (Ž)	Organizacija turi užtikrinti, kad nuotolinio darbo vietoje būtų laikomasi ir įgyvendinama organizacijos asmens duomenų saugumo politika.	**6.7 Nuotolinis darbas**	Kai darbuotojai dirba nuotoliniu būdu (ne organizacijos patalpose), organizacija turi užtikrinti naudotojų asmens duomenų ir organizacijos administruojamų asmens duomenų tvarkymo saugumą.

58. (V)	Nuotolinio darbo politika turi būti dokumentuota kaip asmens duomenų saugumo politikos dalis.		
59. (A)	Nuotolinio darbo politikoje turi būti nustatytos atitinkamos sąlygos ir apribojimai (fizinės saugos, nuotolinės prieigos apsaugos, techninės ir programinės įrangos), kad užtikrinti asmens duomenų saugumą. Pvz., draudimas naudotis vieša interneto prieiga, reikalaujama naudoti patvirtintas VPN paslaugas ir organizacijos suteiktą arba jos reikalavimus atitinkančią antivirusinę programinę įrangą.		
Reagavimas į informacijos saugumo incidentus			
60. (Ž)	Personalas turi būti informuotas apie atsakomybę nedelsiant pranešti apie informacijos saugumo incidentus.	**6.8 Informacijos saugumo incidentų ataskaitų teikimas**	Duomenų valdytojai ir tvarkytojai turi būti tikri, kad jie laikosi savo įsipareigojimų pagal BDAR 33 straipsnį, susijusį su pranešimu apie asmens duomenų saugumo pažeidimus priežiūros institucijai.
61. (Ž)	Personalas turi žinoti pranešimo apie informacijos saugumo incidentų procedūrą ir kontaktinį asmenį, kuriam reikia pranešti apie įvykusį incidentą.		
62. (V)	Pranešimo apie įvykius mechanizmas turėtų būti kuo paprastesnis (visų pasiekiamas, prieinamas ir žinomas).		

Fizinės kontrolės priemonės

Nr.	Priemonės	Atitikmuo ISO 27002:2022	Atitikmuo BDAR ir paaiškinimai
Fizinė sauga			
63. (Ž)	Turi būti užtikrinama, kad organizacijoje prie tvarkomų asmens duomenų būtų galima fiziškai prieiti tik organizacijos nustatytu ir leistinu būdu.	**7.1 Fizinės apsaugos ribos** **7.2 Fizinis patekimas** **7.3 Biurų, kabinetų ir patalpų apsauga** **7.4 Fizinio saugumo stebėjimas** **7.5 Apsauga nuo fizinių ir aplinkos grėsmių** **7.12 Kabelių saugumas**	Fizinė apsauga yra ne mažiau svarbi, negu techninės saugumo priemonės, nes tiesioginės fizinės prieigos kontrolė prie IT infrastruktūros yra visos taikomos saugos strategijos pagrindas. Taip pat fizinė apsauga yra nemažiau svarbi, nes dažnai tarnybinės stotys (su IT sistemomis) ir tinklo įranga nėra specialioje izoliuotoje, saugomoje zonoje ar patalpoje; tarnybinės stotys yra fiziškai prieinamos, pasiekiamos naudotojams ar pašaliniams asmenims. Taipogi galimas neautorizuotas tarnybinės stoties užvaldymas, konfidencialios informacijos atskleidimas.
64. (Ž)	Fizinės saugos politika turi būti dokumentuota kaip asmens duomenų saugumo politikos dalis.		
65. (Ž)	Turi būti įgyvendinta fizinė aplinkos, patalpų, kuriose yra IT sistemų infrastruktūra, apsauga nuo neautorizuotos prieigos. Taip pat turi būti užtikrinta, kad nebūtų paliktų laisvai prieinamų tinklo įrenginių, nenaudojamų tinklo kabelių.		
66. (V)	Būtina naudoti aiškią visų darbuotojų ir lankytojų identifikavimo sistemą, naudojant tinkamas priemones, pvz., visiems norintiems patekti į organizacijos patalpas tapatybę patvirtinančius darbo leidimus.		

67. (V)	Atitinkamos saugios zonos turėtų būti apibrėžtos ir apsaugotos tinkamomis patekimo kontrolės priemonėmis. Popierinis ar elektroninis registravimo rinkmenų žurnalas turi būti saugiai laikomas, prižiūrimas ir stebimas.		
68. (V)	Įsilaužimo (įsibrovimo) aptikimo sistemos turi būti įdiegtos visose saugumo zonose.		
69. (V)	Prireikus turi būti kuriamos fizinės kliūtys, kad būtų užkirstas kelias neteisėtam fiziniam prieinamumui.		
70. (V)	Laisvos saugios zonos turi būti fiziškai rakinamos ir periodiškai patikrinamos.		
71. (V)	Tarnybinių stočių patalpoje turėtų būti: įdiegta automatinė gaisro gesinimo sistema, uždara valdoma oro kondicionavimo sistema ir nepertraukiamo maitinimo šaltinis.		
72. (V)	Išorės subjektų personalui, teikiančiam paslaugas, turi būti suteikta ribota prieiga prie saugių zonų.		
73. (A)	Reguliariai turi būti atliekamas taikomų fizinių kontrolės priemonių fizinės saugos politikos vertinimas ir atitiktis.		

Švaraus „stalo“, „ekrano“ politika			
74. (Ž)	Organizacijoje turi būti įgyvendinama švaraus „stalo“, „ekrano“ politika. Galiniai įrenginiai turi būti apsaugoti (pvz., slaptažodžiais, PIN kodais, biometriniais duomenimis ar kitomis apsaugos priemonėmis). Nepalikti laisvai prieinamų, matomų asmens duomenų darbo vietoje.	**7.7 Švarus“ stalas ir „švarus“ ekranas** **7.8 Įrangos išdėstymas ir apsauga**	Fizinė apsauga yra ne mažiau svarbi, nei techninės saugumo priemonės, nes tiesioginės fizinės prieigos kontrolė prie IT infrastruktūros yra visos taikomos saugos strategijos pagrindas.
75. (V)	Dokumentus ir galinius įrenginius išdėstyti tvarkingai, naudoti kitas priemones (pvz., naudoti stalus su pertvara, nelaikyti ekranų atsuktų į klientus / langus, naudoti monitorių privatumo filtrus [7]), kad sumažinti riziką, jog naudojamą informaciją (tvarkomus asmens duomenis) pamatys leidimo neturintys asmenys.		
76. (V)	Informacinėse sistemose turi būti sukonfigūruota užrakinimo po tam tikro laiko arba atjungimo funkcija (pvz., po 15 min. neaktyvumo		

[7] Monitoriaus privatumo filtras – tai speciali ekranui skirta plėvelė, kuri riboja matomumą iš šonų, apsaugodama ekrane rodomą informaciją nuo pašalinių asmenų žvilgsnių. Kai privatumą užtikrinantis filtras yra uždėtas ant monitoriaus, tik asmuo, tiesiogiai žiūrintis į ekraną, gali matyti aiškų vaizdą, o kitiems žmonėms, žiūrintiems tam tikru kampu, vaizdas pasirodo tamsintas arba visai nematomas.

	automatiškai užsirakinantis kompiuterio ekranas).		
77. (V)	Po darbo valandų nepalikti darbo vietoje laisvai prieinamų svarbių dokumentų ar laikmenų su asmens duomenimis (pvz., padėti į rakinamą stalčių).		
Duomenų naikinimas, šalinimas			
78. (Ž)	Prieš pašalinant bet kokią duomenų laikmeną, turi būti sunaikinti visi joje esantys duomenys, naudojant tam skirtą programinę įrangą, kuri palaiko patikimus duomenų naikinimo algoritmus. Jei to padaryti neįmanoma (pvz., DVD laikmenos), turi būti įvykdytas fizinis duomenų laikmenos sunaikinimas be galimybės atstatyti.	**7.10 Laikmenos** **7.14 Saugus įrangos pašalinimas arba pakartotinis naudojimas**	Pagrindinis duomenų naikinimo tikslas yra negrįžtamas asmens duomenų šalinimas, sunaikinimas be teorinės ir praktinės galimybės juos pakartotinai nuskaityti ar atstatyti. Kai yra šalinama pasenusi, nenaudojama, nebereikalinga techninė įranga, duomenų valdytojas privalo užtikrinti, kad visi prieš tai joje buvę sukaupti asmens duomenys būtų negrįžtamai sunaikinti. Pagal BDAR 5 straipsnį asmens duomenys neturi būti saugomi, kaupiami ilgiau, negu tai yra būtina tais tikslais, kuriais asmens duomenys yra tvarkomi. **Galimos grėsmės ir pavojai** Nekorektiškai naikinant informaciją iš duomenų laikmenų (kai laikmenos be patikros tiesiogiai išmetamos kartu su kita elektronine įranga; laikmenos, be patikros yra perduodamos sunaikinti trečiosioms šalims; laikmenos, be patikros, yra parduodamos varžytinėse ir pan.), atsiranda galimybė atkurti neautorizuotą turinį (pvz., standieji diskai, DVD laikmenos, USB raktai ir kt.). Galimi socialinės inžinerijos metodai, kai popierinės laikmenos, išorinės laikmenos (kietieji diskai ir pan.) nėra fiziškai sunaikinami, o tiesiogiai šalinami (išmetami) į atitinkamus popierinės ar elektroninės įrangos konteinerius esančius šalia įstaigos, įmonės.
79. (Ž)	Popierinės ir nešiojamosios duomenų laikmenos (pvz., DVD laikmenos), kuriose buvo saugomi, kaupiami asmens duomenys, turi būti naikinamos tam skirtais smulkintuvais arba kitomis mechaninėmis priemonėmis.		
80. (V)	Prieš šalinant laikmenas, turi būti atlikti visų šalinamų laikmenų daugybiniai programinės įrangos		

	perrašymai (angl. Multiple passes of Software-based Overwriting).		
81. (V)	Jei saugiems duomenų naikinimo ir šalinimo duomenų laikmenose ar popieriniuose dokumentuose darbams atlikti yra pasitelkiamos trečiosios šalies paslaugos, turi būti sudaryta atitinkama paslaugų sutartis ir atliekamas sunaikintų įrašų protokolavimas.		
82. (A)	Po duomenų ištrynimo reikėtų imtis papildomų priemonių, pvz., gali būti atliktas nepageidaujamos magnetinės informacijos pašalinimas (išmagnetinimas). Priklausomai nuo konkretaus atvejo, reikėtų įvertinti fizinio sunaikinimo galimybes.		
83. (A)	Jei saugiems įrašų naikinimo ir šalinimo duomenų laikmenose ar popieriniuose dokumentuose darbams atlikti yra pasitelkiamos trečiosios šalies paslaugos, turi būti užtikrinta, kad šis procesas vyktų duomenų valdytojo ir (ar) tvarkytojo patalpose, siekiant išvengti duomenų perdavimo trečiosioms šalims. Atskirais atvejais, kai to neįmanoma atlikti duomenų		

	valdytojo ir (ar) tvarkytojo patalpose, sunaikinimas gali būti atliekamas kitoje fizinėje vietoje.		

Technologinės kontrolės priemonės

Nr.	Priemonės	Atitikmuo ISO 27002:2022	Atitikmuo BDAR ir paaiškinimai
Prieigų kontrolė ir autentifikavimas			
84. (Ž)	Turi būti įdiegta, įgyvendinta prieigų kontrolės sistema, kuri taikoma visiems IT sistemos naudotojams. Prieigų kontrolės sistema turi leisti kurti, patvirtinti, peržiūrėti ir panaikinti naudotojų paskyras.	**8.2 Privilegijuotosios prieigos teisės** **8.5 Saugus autentiškumo patvirtinimas**	Prieigų kontrolė ir autentifikavimas yra esminiai saugos reikalavimai, siekiant apsisaugoti nuo neautorizuotos prieigos prie IT sistemos, kurioje yra tvarkomi asmens duomenys. Šie saugos reikalavimai įgyvendina organizacijos prieigų kontrolės politiką (taip pat žiūrėti organizacines priemones, nurodytas šių gairių 14–21 punktuose „Prieigos valdymas ir teisės“) techniškai panaudojant specifinius, techninius komponentus ir taikomąsias programas. **Galimos grėsmės ir pavojai** Nesukontroliuojamos neautorizuotų naudotojų prieigos prie asmens duomenų; neautorizuotas duomenų bazės turinio (asmens duomenų) atskleidimas, peržiūrėjimas, kopijavimas, redagavimas, naikinimas (angl. Broken access control; Broken authentification).
85. (Ž)	Turi būti vengiama naudoti bendras naudotojų paskyras. Vietose, kur bendra naudotojų paskyra yra būtina, turi būti užtikrinta, kad visi bendros paskyros naudotojai turi tokias pat teises ir pareigas.		
86. (Ž)	Turi būti veikiantis autentifikavimo mechanizmas, leidžiantis prieigą prie IT sistemos (paremtas Prieigų kontrolės politika). Minimalus reikalavimas naudotojui prisijungti prie IT sistemos – naudotojo		

	prisijungimo vardas ir slaptažodis. Slaptažodis sudaromas atsižvelgiant į tam tikrą kompleksiškumo lygį.		
87. (Ž)	Prieigų kontrolės sistema turi turėti galimybę aptikti ir neleisti naudoti slaptažodžių, kurie neatitinka tam tikro kompleksiškumo lygio.		
88. (Ž)	Naudototojo slaptažodžiai turi būti saugomi naudojant kodavimo formą (angl. Hash form).		
89. (V)	Turi būti nustatytos ir dokumentais patvirtintos slaptažodžių naudojimo taisyklės. Taisyklėse turi būti apibrėžtas slaptažodžio ilgis, sudėtingumas, galiojimo laikas, nesėkmingų bandymų įvesti slaptažodį skaičius, taip pat turi būti užtikrinta, kad slaptažodžiai nesikartotų.		
90. (V)	Registruoti žurnaliniuose įrašuose prisijungimus ir nesėkmingus bandymus. Po nustatyto nesėkmingų bandymų prisijungti, blokuoti prisijungimą / paskyrą.		
91. (V)	Privilegijuotiems naudotojams (pvz., sistemų administratoriams) prisijungimui prie asmens duomenų tvarkymo sistemų turi būti taikomas		

	kelių veiksnių autentifikavimas. Visais atvejais, kai į tokias sistemas jungiamasi ne iš vidinio kompiuterių tinklo, turi būti naudojamos ir papildomos saugumo priemonės, tokios kaip IP adreso kontrolė, virtualus privatus tinklas (angl. VPN) ir kiti atitinkami saugumo mechanizmai. Autentifikavimo veiksniais gali būti slaptažodžiai, saugumo žetonai, USB raktai su slapta žyma, biometriniai duomenys ir kt.		
92. (A)	Turi būti naudojamas įrenginio autentifikavimas, garantuojantis, kad asmens duomenys tvarkomi tik naudojant konkrečius tinklo įrenginius (pvz., 802.1X, RADIUS ir kt.).		
93. (A)	Prisijungimo procedūros metu neteikti pagalbos pranešimų, kurie padėtų leidimo neturinčiam naudotojui (pvz., jei nepavyksta prisijungti, sistema neturi nurodyti, kuri duomenų dalis yra teisinga ar neteisinga).		

Naudotojo galiniai įrenginiai (kompiuterinės darbo vietos)			
94. (Ž)	Naudotojams negalima turėti galimybės išjungti ar apeiti, išvengti IT sistemų saugos nustatymų.	**8.1 Naudotojo galiniai įrenginiai**	Šis reikalavimas yra susijęs su saugos nustatymais naudotojų darbo stotyse ar kituose įrenginiuose. Yra svarbu priverstinai nustatyti specifinę saugos politiką ir apriboti naudotojų veiksmus, siekiant apsaugoti IT sistemas (pvz., antivirusinės programinės įrangos išjungimas, neautorizuotos programinės įrangos diegimas). **Galimos grėsmės ir pavojai** Galimybė apeiti, išjungti saugos nustatymus, antivirusines sistemas; vykdyti, kaupti neleistiną turinį; neteisėtai įgyti privilegijuotas (administratoriaus) teises. Neteisėtas tarnybinių, darbo stočių užvaldymas, neautorizuotos prieigos prie duomenų bazės turinio. Negebėjimas aptikti, užkardyti ir informuoti apie nustatytus netinkamus, piktybiškus naudotojų veiksmus, naudotojų kaupiamą neleistiną turinį, išorės atakas. Neleistinos, kenksmingos programinės įrangos diegimas, vykdymas, siekiant užvaldyti tarnybinę, darbo stotį, neteisėtai atskleisti informaciją apie kitus naudotojus ar įgyti prieigą prie duomenų bazės turinio. Apsaugos priemonių (pvz., antivirusinės programinės įrangos) šalinimas, išjungimas, papildomų neteisėtų naudotojų paskyrų kūrimas. Nenutraukiant neaktyvaus naudotojo sesijos, galimi įvairūs socialinės inžinerijos metodai nukreipiant naudotojų dėmesį į pašalines detales, dėl to galimas neautorizuotas informacijos atskleidimas, neteisėtas programinės įrangos naudojimas, kenksmingos išorės laikmenos panaudojimas. Didelė grėsmė neteisėtai užvaldyti operacines sistemas tarnybinėse stotyse, kompiuterinėse darbo vietose, neteisėtai užvaldyti programinę įrangą, atskleisti duomenų bazių turinį.
95. (Ž)	Turi būti įdiegta antivirusinė programinė įranga. Antivirusinės programinės įrangos duomenų bazės turi būti atnaujinamos ne rečiau, kaip kartą per parą. Rekomenduojama atnaujinti duomenų bazes dažniau, priklausomai nuo grėsmių lygio ir sistemos saugumo reikalavimų, kad būtų užtikrinta efektyvi apsauga nuo naujausių virusų ir kenkėjiškų programų.		
96. (Ž)	Naudotojams negalima turėti privilegijuotų teisių diegti, šalinti, administruoti neautorizuotos programinės įrangos.		
97. (Ž)	Kritiniai operacinės sistemos saugos atnaujinimai privalo būti diegiami reguliariai ir nedelsiant.		
98. (V)	IT sistemos turi turėti nustatytą sesijos laiką, t. y. naudotojui esant neaktyviam sistemoje nustatytą laiką, jo sesija privalo būti nutraukta.		

	Rekomenduojamas neaktyvios sesijos laikas – ne ilgiau kaip 15 min.		
99. (V)	Antivirusinės programinės įrangos ir informacija apie virusus bei kenkimo programinę įrangą duomenų bazėse turi būti atnaujinama ne rečiau kaip kartą per parą.		
100. (V)	Turi būti uždrausta perduoti asmens duomenis iš kompiuterinių darbo vietų į išorinius saugojimo įrenginius (pvz., USB raktai, DVD, išorinius standžiuosius diskus ir kt.). Išjungti / blokuoti fizinius prievadus (USB raktų naudojimą).		
101. (A)	Pageidautina, kad asmens duomenų tvarkymui naudojamos kompiuterinės darbo vietos nebūtų prijungtos prie kompiuterinio tinklo su interneto prieiga, išskyrus atvejus, kai imamasi papildomų saugumo priemonių (pvz., tinklo prieigos kontrolės, kelių veiksnių autentifikavimo, šifravimo ir kt.), kad būtų išvengta neteisėto asmens duomenų tvarkymo, kopijavimo ir perdavimo.		

102. (A)	Kompiuterinėse darbo vietose naudojamuose operacinės sistemos diskuose turi būti įgalintas pilnas standžiojo disko šifravimas (angl. Full-disk encryption).		
Mobilieji, nešiojamieji įrenginiai			
103. (Ž)	Mobiliųjų, nešiojamųjų įrenginių administravimo procedūros privalo būti nustatytos ir dokumentuotos, aiškiai aprašant tinkamą tokių įrenginių naudojimą, įskaitant asmeninius įtaisus, jei organizacija leidžia juos naudoti (angl. BYOD – Bring You Own Device).[8]	**8.1 Naudotojo galiniai įrenginiai**	Kai naudojami mobilūs ir nešiojami įrenginiai (pvz., išmanieji telefonai, planšetiniai ir nešiojami kompiuteriai), organizacija turi užtikrinti naudotojų asmens duomenų ir organizacijoje administruojamų asmens duomenų tvarkymo saugumą. **Galimos grėsmės ir pavojai** Galimi įvairūs socialinės inžinerijos metodai, siekiant surinkti patalpų, darbo aplinkos informaciją, informaciją apie darbuotojus; neteisėtas fotografijų, vaizdo, garso įrašų darymas. Pvz., IT infrastruktūros fotografavimas, naudojamos kompiuterinės, programinės įrangos, prisijungimų (slaptažodžių) informacijos surinkimas. Mobilieji ir nešiojamieji įrenginiai be naudotojo žinios gali persiųsti informaciją trečiosioms šalims, galimas neautorizuotas informacijos atskleidimas, nutekėjimas.
104. (Ž)	Mobilieji ir nešiojamieji įrenginiai, kuriais bus naudojamasi darbui su informacinėmis sistemomis, prieš naudojimąsi turi būti užregistruoti ir autorizuoti.		
105. (Ž)	Mobilieji, nešiojamieji įrenginiai turi būti pakankamo prieigos kontrolės procedūrų lygio, kaip ir kita naudojama įranga asmens duomenims tvarkyti.		

[8] Jei organizacija darbuotojams leidžia naudoti asmeninius įrenginius (angl. BYOD – Bring Your Own Device), turi būti įgyvendinti visi šių gairių 103 – 111 punktų reikalavimai.

106. (V)	Mobiliųjų, nešiojamųjų įrenginių valdymo funkcijos ir atsakomybės turi būti aiškiai apibrėžtos.		
107. (V)	Organizacija turi turėti galimybę nuotoliniu būdu ištrinti asmens duomenis mobiliuosiuose, nešiojamuose įrenginiuose, kurių saugumas buvo sukompromituotas (pvz., pažeistos saugumo nuostatos, prarastas patikimumas).		
108. (V)	Mobiliuosiuose, nešiojamuosiuose įrenginiuose turi būti atskirti privatūs ir organizacijos veiklos duomenys, naudojant saugias programinės įrangos talpyklas (konteinerius [9]) arba skirtingas paskyras.		
109. (V)	Nenaudojami mobilieji, nešiojamieji įrenginiai turi būti fiziškai apsaugoti nuo vagystės.		
110. (A)	Prieigai prie mobiliųjų, nešiojamųjų įrenginių turėtų būti naudojamas dviejų veiksnių autentifikavimas.		
111. (A)	Asmens duomenys, saugomi mobiliajame įrenginyje turi būti užšifruoti.		

[9] Konteineriai mobiliuosiuose ir nešiojamuosiuose įrenginiuose yra programinės įrangos technologija, leidžianti atskirti ir izoliuoti skirtingus duomenis bei programas. Konteineriai sukuria saugias ir atskiras talpyklas, kuriose gali būti laikomi organizacijos veiklos duomenys ar programos, atskirai nuo privačių naudotojo duomenų.

Tarnybinių stočių, duomenų bazių apsauga			
112. (Ž)	Duomenų bazės ir taikomųjų programų tarnybinės stotys turi būti sukonfigūruotos taip, kad veiktų naudodamos atskiras paskyras su priskirtomis žemiausiomis operacinės sistemos privilegijomis.	**8.1 Naudotojo galiniai įrenginiai**	Informacinių sistemų pagrindas yra tarnybinės stotys ir duomenų bazės. Jų apsauga privalo būti sustiprinta, siekiant užtikrinti saugią darbo aplinką. **Galimos grėsmės ir pavojai** Nekorektiški naudojamų operacinių sistemų, taikomųjų programų konfigūracijos nustatymai; gamyklinių nustatymų (angl. Default settings), perteklinių funkcijų naudojimas, atnaujinimo funkcijų nepalaikymas. Programinės įrangos, servisų, perteklinių funkcijų vykdymas operacinių sistemų administratoriaus (angl. Root) teisėmis; tiesioginė prieiga internetu prie tarnybinės stoties ir duomenų bazės įgyjant administratoriaus teises; neteisėtas tarnybinės stoties užvaldymas, duomenų bazės turinio peržiūrėjimas, kopijavimas, redagavimas, naikinimas. Atskiroje paskyroje (ne administratoriaus), su žemiausiomis operacinėmis sistemos privilegijomis, naudojant kelias, keliolika skirtingų taikomųjų programų, duomenų bazių iš skirtingų IT sistemų, neteisėtas tarnybinės stoties ir (ar) taikomosios programos užvaldymas suteiks prieigas prie visų tarnybinėje stotyje esančių duomenų bazių turinio. Galimas duomenų bazių turinio peržiūrėjimas, kopijavimas, redagavimas, naikinimas.
113. (Ž)	Duomenų bazėse ir taikomųjų programų tarnybinėse stotyse turi būti tvarkomi tik tie asmens duomenys, kurie yra reikalingi darbui, atitinkančiam duomenų tvarkymo tikslus.		
114. (V)	Saugomoms byloms ar įrašams apsaugoti turėtų būti naudojamas šifravimas, įdiegiant atitinkamą programinę ar techninę įrangą.		
115. (V)	Duomenų bazėse turi būti taikomi pseudonimizavimo metodai, atskiriant tiesioginius identifikatorius nuo esamų sąsajų su kitais duomenimis.		
116. (A)	Duomenų bazėje turi būti taikomi autorizuotų užklausų, šifruotos		

	paieškos ir kiti privatumo užtikrinimo metodai.		
Techninių žurnalų įrašai ir stebėsena			
117. (Ž)	Techninių žurnalų įrašai turi būti įgyvendinti kiekvienai IT sistemai, naudojamai asmens duomenims tvarkyti. Techninių žurnalų įrašuose turi būti matoma visa įmanoma prieigų prie asmens duomenų informacija (pvz., data, laikas, peržiūrėjimo, keitimo, panaikinimo veiksmai). Rekomenduojamas saugojimo terminas – ne trumpiau kaip 6 mėnesiai.	**8.15 Registravimas įvykių žurnale** **8.16 Stebėsenos veikla**	Techninių žurnalų įrašai yra esminis saugos reikalavimas, kuris leidžia identifikuoti ir stebėti, sekti naudotojų veiksmus (kurie susiję su asmens duomenų tvarkymu), taip užtikrinant atskaitingumą (jei įvyktų neautorizuotas asmens duomenų atskleidimas, keitimas ar panaikinimas). Taip pat svarbu nuolat stebėti techninių žurnalų įrašus, kurie leistų identifikuoti potencialius vidinius ar išorinius bandymus pažeisti sistemos saugumą ir integralumą. **Galimos grėsmės ir pavojai** Sudėtingas autorizuotų ir neautorizuotų naudotojų atliktų veiksmų atsekamumas, galimas atliktų veiksmų slėpimas, užmaskavimas; esamų ir sukauptų techninių žurnalų įrašų redagavimas, klastojimas, naikinimas (angl. Log file cleaning). Datos ir laiko redagavimas, klastojimas techninių žurnalų įrašuose (nenaudojant bendro, sinchronizuoto atskaitos mechanizmo); nenaudojama, neaktyvi techninių žurnalų įrašų pokyčių stebėsena, monitoringas.
118. (Ž)	Techninių žurnalų įrašai turi turėti laiko žymas ir būti apsaugoti nuo galimo sugadinimo, suklastojimo ar neautorizuotos prieigos. IT sistemose naudojami laiko apskaitos mechanizmai turi būti sinchronizuoti pagal bendrą laiko atskaitos šaltinį.		
119. (V)	Visi sistemų administratorių veiksmai (taip pat ir jų atliekamas naudotojų teisių papildymas,		

	panaikinimas, keitimas) turi būti registruojami.		
120. (V)	Turi būti neįmanoma ištrinti ar pakeisti techninių įrašų turinio. Prieiga prie įrašų taip pat turi būti registruojama, siekiant atlikti neįprastų veiksmų susekimo stebėseną.		
121. (V)	Stebėsenos sistema turi apdoroti techninius įrašus, ruošti sistemos būklės ataskaitas ir įspėti apie galimus pavojus.		
122. (V)	Stebėti išeinantį ir įeinantį tinklo, sistemos bei programų duomenų srautą, resursų (pvz., CPU, standžiųjų diskų, atminties, pralaidumo) naudojimą ir jų našumą. Organizacija turi nusistatyti įprastą resursų naudojimą / našumą ir pagal jį stebėti, ar nėra neatitikimų.		
Tinklo ir komunikacijos sauga			
123. (Ž)	Kai prieiga prie naudojamų IT sistemų yra vykdoma internetu, privaloma naudoti šifruotą komunikacijos kanalą, t. y. kriptografinius protokolus (pvz., TLS/SSL).	**8.20 Tinklų saugumas** **8.21 Tinklo paslaugų saugumas**	Tinklo ir komunikacijos sauga yra ypač svarbi, siekiant užtikrinti asmens duomenų saugą (tiek vidinių, tiek išorinių tinklų). Komunikacijai naudojamose susirašinėjimo programose, esant galimybei, rekomenduojama aktyvuoti ištisinio šifravimo (angl. End-to-end encryption) nuostatas. BDAR 32 straipsnis numato, kad „[...]atsižvelgdamas į techninių galimybių išsivystymo lygį, įgyvendinimo

124. (V)	Belaidis ryšys prie IT sistemų turi būti leidžiamas tik tam tikriems naudotojams ir procesams. Belaidžio ryšio potinklis turi būti atskirtas nuo kitų potinklių. Belaidė prieiga turi būti apsaugota patikimais šifravimo mechanizmais.	**8.22 Tinklų atskyrimas**	sąnaudas bei duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus, taip pat duomenų tvarkymo keliamus įvairios tikimybės ir rimtumo pavojus fizinių asmenų teisėms ir laisvėms, duomenų valdytojas ir duomenų tvarkytojas įgyvendina tinkamas technines ir organizacines priemones, kad būtų užtikrintas pavojų atitinkančio lygio saugumas, įskaitant inter alia, jei reikia: - pseudonimų suteikimą asmens duomenims ir jų šifravimą; - gebėjimą užtikrinti nuolatinį duomenų tvarkymo sistemų ir paslaugų konfidencialumą, vientisumą, prieinamumą ir atsparumą [...]“. **Galimos grėsmės ir pavojai** Galimybė klausytis (angl. Sniff) duomenų srautų, keliaujančių komunikacijos kanalu, bei galimybė perimti, modifikuoti keliaujančią informaciją (angl. Man-in-the-middle). Pvz., vieši, belaidžiai, nemokamą interneto prieigą teikiantys taškai (WiFi) bei interneto svetainės, neužtikrinančios SSL/TLS (HTTPS) kriptografinių protokolų. Taip pat vidiniai įstaigų, organizacijų kompiuterių tinklai, nenaudojantys MAC adresų filtravimo, susiejimo su fiziniais Ethernet prievadais; nevykdomas kompiuterių tinklų duomenų srautų monitoringas, nevykdomas įsilaužimų aptikimas ir prevencija (pvz., IDS/IPS).
125. (V)	Reikėtų vengti nuotolinės prieigos prie IT sistemų. Tais atvejais, kai ši prieiga yra išties reikalinga, ji yra galima tik organizacijos paskirtam darbuotojui (pvz., sistemų administratoriui, saugumo specialistui) kontroliuojant ir stebint jos veikimą per iš anksto nustatytus įrenginius.		
126. (V)	Bet koks duomenų judėjimas iš, į IT sistemą turi būti stebimas ir kontroliuojamas naudojant ugniasienes ir įsibrovimo (įsilaužimo) aptikimo ir prevencijos sistemas.		
127. (V)	Jei organizacijoje yra aptarnaujami klientai, turi būti atskirtas viešas tinklas skirtas klientas, nuo organizacijos vidinio tinklo iš kuriuo yra pasiekiamos IT sistemos.		
128. (A)	Prisijungimas prie interneto neturi būti leidžiamas tarnybinėms stotims		

	ir jose esančiai programinei įrangai, naudojamai asmens duomenims tvarkyti.		
129. (A)	Informacinės sistemos tinklas turi būti atskirtas nuo kitų duomenų valdytojo tinklų.		
130. (A)	Prieiga prie IT sistemos turi būti atliekama tik iš patvirtintų įrenginių ir terminalų, naudojant tam skirtas technologijas, pvz., MAC adresų filtravimą arba tinklo prieigos kontrolę / naudojantis virtualiu privačiuoju tinklu (VPN).		
Atsarginės kopijos			
131. (Ž)	Atsarginės kopijos ir duomenų atstatymo procedūros privalo būti apibrėžtos, dokumentuotos ir aiškiai susietos su vaidmenimis ir pareigomis.	**8.13 Informacijos atsarginės kopijos**	Atsarginių kopijų sistema yra esminis veiksnys, užtikrinantis organizacijos darbo ir procesų atstatymą, įvykus duomenų praradimui ar sugadinimui. Duomenų kopijų darymo dažnumas ir poreikis priklauso nuo organizacijos ir joje tvarkomų asmens duomenų. BDAR 32 straipsnis numato „gebėjimą laiku atkurti sąlygas ir galimybes naudotis asmens duomenimis fizinio ar techninio incidento atveju“. **Galimos grėsmės ir pavojai** Esant nepakankamai apibrėžtai duomenų atstatymo procedūrai, galimas konfidencialios informacijos nutekėjimas, neteisėtas duomenų bazės turinio atskleidimas, programinės įrangos, operacinių sistemų informacijos, informacijos apie naudotojus atskleidimas.
132. (Ž)	Atsarginių kopijų laikmenoms privalo būti užtikrintas tinkamas fizinis aplinkos, patalpų saugos lygis, priklausantis nuo saugomų duomenų.		
133. (Ž)	Atsarginių kopijų darymo procesas turi būti stebimas, siekiant užtikrinti užbaigtumą ir išsamumą.		

134. (Ž)	Pilnos atsarginės duomenų kopijos privalo būti daromos reguliariai. Rekomenduojamas atsarginių kopijų darymo dažnumas: - kasdien – pridedamoji kopija; - kas savaitę – pilna kopija.		Neautorizuotų asmenų patekimas į patalpas; įvairūs socialinės inžinerijos panaudojimo metodai. Nekorektiškas atsarginių kopijų atlikimo bei duomenų iš atsarginių kopijų atstatymo procesas lemia negrįžtamą duomenų praradimą, neužtikrinamą duomenų prieinamumą, nutekėjimą.
135. (V)	Atsarginės kopijos turi būti reguliariai testuojamos, siekiant užtikrinti, kad jos galėtų būti patikimai naudojamos ekstremalioje situacijoje.		
136. (V)	Atsarginės kopijos turi būti saugiai laikomos skirtingose vietose, kurios turi būti geografiškai nutolusios viena nuo kitos.		
137. (A)	Atsarginės kopijos turi būti šifruojamos ir saugiai laikomos visiškai atjungus (angl. Offline) nuo kompiuterinių tinklų.		
Keitimų valdymas			
138. (Ž)	Organizacija turi užtikrinti, kad visi esminiai IT sistemų keitimai būtų stebimi ir registruojami konkretaus asmens (pvz., IT arba saugos specialisto).	**8.32 Pakeitimų valdymas**	Keitimų valdymo tikslas – sinchronizuoti ir kontroliuoti visus IT sistemose, naudojamose tvarkant asmens duomenis, atliekamus keitimus. Tai yra svarbi saugumo priemonė, nes nesėkmingas keitimų įgyvendinimas gali sukelti neteisėtą duomenų atskleidimą, pakeitimą ar sunaikinimą. Keitimų valdymas yra būtinas duomenų tvarkymo vientisumui užtikrinti (BDAR 5 straipsnio 1 dalies f punktas) ir duomenų valdytojo atskaitomybės principui įgyvendinti (BDAR 5 straipsnio 2 dalis).
139. (V)	Turi būti įdiegta išsami ir dokumentais pagrįsta IT keitimų valdymo politika. Keitimų valdymo		

	politiką turi apibrėžti: pokyčių įvedimo ir įdiegimo procedūras, pareigybes ir naudotojus, kurių teisės buvo pakeistos, pokyčių įdiegimo laiko terminus. Pokyčių valdymo politika turi būti reguliariai atnaujinama.		
Programinės įrangos sauga			
140. (Ž)	Informacinėse sistemose naudojama programinė įranga (asmens duomenims tvarkyti) turi atitikti programinės įrangos saugos gerąją praktiką, programinės įrangos kūrime taikomą saugos gerąją praktiką, programinės įrangos kūrimo struktūras (angl. Frameworks), standartus (pvz., Agile, OWASP ir kt.).	**8.19 Programinės įrangos diegimas operacinėse sistemose** **8.26 Programų saugumo reikalavimai** **8.28 Saugus programavimas**	Visuose programinės įrangos kūrimo ir administravimo etapuose organizacija turi užtikrinti tinkamą asmens duomenų saugumą. Projektuojant ir kuriant naujas programinės įrangos sistemas, kuriose numatoma tvarkyti asmens duomenis, būtina laikytis BDAR 25 straipsnyje (Pritaikytoji duomenų apsauga ir standartizuotoji duomenų apsauga – angl. Privacy by Design and Privacy by Default) numatytų principų. **Galimos grėsmės ir pavojai** Galimos programinės įrangos spragos (angl. Bug), sutrikimai (angl. Malfunction). Galimybės pasinaudoti programinės įrangos spragomis siekiant apeiti, išjungti programinės įrangos saugą, užvaldyti programinę įrangą, įgyti privilegijuotas teises (administratoriaus), administruoti naudotojų paskyras, tarnybines, darbo stotis, kuriose yra talpinama programinė įranga.
141. (Ž)	Specifiniai saugos reikalavimai, susiję su organizacijos veiklos ypatumais, turi būti apibrėžti pradiniuose programinės įrangos kūrimo etapuose.		
142. (Ž)	Turi būti laikomasi duomenų saugą užtikrinančių programavimo standartų ir gerosios praktikos.		
143. (Ž)	Po programinės įrangos kūrimo, testavimo ir verifikacijos, pradedant sistemos įdiegimą ir eksploataciją,		

	turi būti laikomasi pagrindinių saugos reikalavimų.		
144. (V)	Prieš pradedant naudoti programinę įrangą, turi būti atliktas programinės įrangos ir infrastruktūros pažeidžiamumo ir atsparumo testavimas. Programinė įranga turi atitikti reikiamą saugumo lygį.		
145. (V)	Turi būti atliekami periodiški infrastruktūros atsparumo grėsmėms testavimai.		
146. (V)	Programinės įrangos atnaujinimai turi būti testuojami ir vertinami prieš juos diegiant į darbo aplinką.		
147. (V)	Programinės įrangos kūrimas turi būti atliekamas specialioje aplinkoje, kuri nėra prijungta prie IT sistemų, naudojamų tvarkant asmens duomenis. Testuojant sistemas, reikia naudoti testinius duomenis. Tais atvejais, kai tai neįmanoma, turi būti nustatytos specialios testavimo metu naudojamų asmens duomenų apsaugos procedūros, saugumo reikalavimai.		

Pagrindinių priemonių, skirtų asmens duomenų saugumui užtikrinti, sąrašas

1. Reguliariai informuokite ir švieskite darbuotojus apie su asmens duomenų tvarkymu susijusias rizikas;
2. Sukurkite vidaus asmens duomenų saugumo politiką ir jos privalomą taikymą organizacijoje;
3. Įgyvendinkite pritaikytosios ir numatytosios duomenų apsaugos principus;
4. Užtikrinkite, kad tvarkomi asmens duomenys būtų adekvatūs, aktualūs ir apimtų tik tai, kas būtina (duomenų kiekio mažinimas);
5. Žinokite dokumentus, kuriuose yra tvarkomi jautrūs asmens duomenys;
6. Periodiškai vykdykite asmens duomenų saugumo mokymus;
7. Pasirašykite konfidencialumo sutartis su savo darbuotojais;
8. IT sistemos nustatykite neaktyvios sesijos laiką – ne ilgiau kaip 15 min.;
9. Naudokite ugniasienę ir antivirusinę programinę įrangą su automatiniais atnaujinimais;
10. Nenaudokite gamintojo oficialiai nebepalaikomos programinės įrangos (pvz., operacinių sistemų, atvirojo kodo programų ir t. t.);
11. Darykite asmens duomenų atsargines kopijas;
12. Apribokite fizinių prievadų naudojimą (pvz., USB raktų, išorinius standžiuosius diskus ir kt.) galiniuose naudotojų įrenginiuose;
13. Apsaugokite organizacijos patalpas (pvz., leidimai patekti į konkrečias zonas, praėjimo kontrolės priemonės);
14. Visada suteikite unikalius identifikatorius naudotojams, nenaudokite bendrų paskyrų;
15. Galiniuose naudotojo įrenginiuose naudokite autentifikavimą;
16. Numatykite autorizacijos reikalavimus (pvz., atskirti naudotojų profiliai pagal poreikius, sudėtingi slaptažodžiai);
17. Vertinkite kaip yra laikomasi nuotolinio darbo saugos politikos;
18. Reguliariai peržiūrėkite ir pašalinkite perteklines / nebenaudojamas prieigos teises;
19. Pseudonimizuokite arba anonimizuokite asmens duomenis;
20. Šifruokite duomenis, kad išvengtumėte neautorizuotos prieigos;
21. Naudokite virtualų privatų tinklą (angl. VPN) nuotoliniam darbui;
22. Įsitikinkite, kad organizacijoje yra laikomasi asmeninių įrenginių naudojimo darbui politikos (angl. BYOD).