Saugumo priemonių ir rizikos vertinimo ataskaita

Duomenų valdytojas

Trakų suaugusiųjų mokymo centras

2026 m. rugsėjo 16 d.

I. Bendra informacija
II. Duomenų tvarkymo operacijos nustatymas ir jos kontekstas
III. Poveikio vertinimo klausimai
IV. Galimų grėsmių nustatymas ir jų atsiradimo tikimybės vertinimas
V. Rizikos įvertinimas
VI. Pagal rizikos įvertinimą nustatomos techninės ir organizacinės priemonės

I. BENDROJI INFORMACIJA

Duomenų valdytojas Trakų suaugusiųjų mokymo centras, kodas 303085806, buveinės adresas Birutės g. 42, Trakai, vadovaudamasis 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamento (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (toliau – BDAR) 24 ir 32 straipsniais, atliko saugumo priemonių ir rizikos vertinimą.

Saugumo priemonių ir rizikos vertinimas įstaigoje atliktas pagal Valstybinės duomenų apsaugos inspekcijos parengtas Tvarkomų asmens duomenų saugumo priemonių ir rizikos įvertinimo gaires (4 versija), kurios 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“.

II. DUOMENŲ TVARKYMO OPERACIJOS NUSTATYMAS IR JOS KONTEKSTAS

Duomenų valdytojas automatizuotomis ir neautomatizuotomis priemonėmis tvarko asmens duomenis, kuriuos gauna vykdydamas ugdymo programas, neformalųjį švietimą, savo kaip darbdavio funkcijas bei atlikdamas kitas teisės aktuose pavestas užduotis.

1 lentelė

DUOMENŲ TVARKYMO TIKSLAS	DUOMENŲ TVARKYMO TEISINIS PAGRINDAS	DUOMENŲ APIMTIS (kokie asmens duomenys tvarkomi nurodytu tikslu)	DUOMENŲ SUBJEKTŲ KATEGORIJOS	DUOMENŲ GAVĖJŲ KATEGORIJOS (kam perduodami asmens duomenys)	DUOMENŲ GAVIMO ŠALTINIS	DUOMENŲ SAUGOJIMO TRUKMĖ
Personalo atrankos, kandidatų tinkamumo pareigoms įvertinimo ir teisės aktuose nustatytų reikalavimų atitikties patikrinimo tikslais:	Reglamento 6 str. 1 d. (a) p. (duomenų subjekto sutikimas, kai CV saugomas būsimoms atrankoms arba kreipiamasi į esamą darbdavį), Reglamento 6 str. 1 d. (b) p. (siekiant imtis veiksmų duomenų subjekto prašymu prieš sudarant sutartį), Reglamento 6 str. 1 d. (c) punktas (duomenų valdytojui taikoma teisinė prievolė, kai tikrinamas atitikimas teisės aktuose nustatytiems reikalavimams), Reglamento 10 str., Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo 5 str., Vaiko teisių apsaugos pagrindų įstatymo 30 str. (atrinkto kandidato teistumo duomenų tvarkymui), Lietuvos Respublikos darbo kodeksas, Lietuvos Respublikos korupcijos prevencijos įstatymo 16–19 str. (tuo atveju, kai asmuo atrenkamas į pareigas, numatytas Lietuvos	Vardas, pavardė, telefono numeris, parašas, elektroninio pašto adresas, gyvenimo aprašymas, duomenys apie išsilavinimą ir kvalifikaciją, asmens tapatybės dokumento kopija (tik tais atvejais, kai tai aiškiai nustatyta teisės aktuose), išsilavinimą patvirtinančio dokumento kopija, pedagogo kvalifikaciją patvirtinančio dokumento kopija (jeigu toks reikalavimas taikomas), pedagoginių ir psichologinių žinių kursų išklausymo dokumento kopija (jeigu toks reikalavimas taikomas), informacija apie darbo patirtį, kita informacija, kuri patvirtina atitiktį keliamiems kvalifikaciniams reikalavimams, kandidato savanoriškai pateikta informacija, reikalinga jo tinkamumui pareigoms įvertinti, kita informacija, kuri patvirtina atitiktį Lietuvos Respublikos vaiko teisių apsaugos pagrindų įstatymo 30 str. reikalavimams (tuo atveju, kai asmuo atrenkamas į pareigas), kita informacija, kuri patvirtina atitiktį Lietuvos Respublikos švietimo įstatymo 48 str. reikalavimams (tuo atveju, kai asmuo atrenkamas į mokytojo pareigas), kita informacija, kuri patvirtina atitiktį Lietuvos Respublikos korupcijos prevencijos įstatymo 16 str. reikalavimams (tuo atveju, kai asmuo atrenkamas į pareigas numatytas Lietuvos Respublikos korupcijos prevencijos įstatymo 17 str. 4 d.),	Asmenys, pageidaujantys įsidarbinti įstaigoje.	Viešojo valdymo agentūra (vykdant konkursą per VATIS), Specialiųjų tyrimų tarnyba (tuo atveju, kai asmuo atrenkamas į pareigas, numatytas Lietuvos Respublikos korupcijos prevencijos įstatymo 17 str. 4 d.), Lietuvos Respublikos švietimo, mokslo ir sporto ministerija (Pedagogų registro informacinės sistemos valdytojas, Švietimo valdymo informacinės sistemos valdytojas), Informatikos ir ryšių departamentas (Įtariamųjų, kaltinamųjų ir nuteistųjų registro valdytojas, kai atliekamas teisės aktuose numatytas nepriekaištingos reputacijos arba teisės dirbti su vaikais patikrinimas.), prieglobos (hostingo) paslaugų teikėjas - duomenų tvarkytojas, UAB „NEVDA“ (Deka Office) – duomenų tvarkytojas,	Duomenų subjektas, Viešojo valdymo agentūra (vykdant konkursą per VATIS), Specialiųjų tyrimų tarnyba (kai asmuo atrenkamas į pareigas, numatytas Lietuvos Respublikos korupcijos prevencijos įstatymo 17 str. 4 d.), Lietuvos Respublikos švietimo, mokslo ir sporto ministerija (Pedagogų registro informacinės sistemos valdytojas, Švietimo valdymo informacinės sistemos valdytojas), Informatikos ir ryšių departamentas (Įtariamųjų, kaltinamųjų ir nuteistųjų registras), buvęs arba esamas kandidato darbdavys (iš buvusio darbdavio – prieš tai informavus kandidatą, o iš esamo darbdavio – tik kandidato sutikimu).	Atrankos ir konkursų duomenys saugomi 3 metus po atrankos pasibaigimo arba iki kol įsiteisės galutinis sprendimas dėl atrankos rezultatų ir šis sprendimas nebegalės būti skundžiamas.

	Respublikos korupcijos prevencijos įstatymo 17 str. 4 d.), Konkursų valstybės ir savivaldybių įmonėse, iš valstybės, savivaldybių ir valstybinio socialinio draudimo fondo biudžetų bei iš kitų valstybės įsteigtų fondų lėšų finansuojamose valstybės ir savivaldybių įstaigose ir viešosiose įstaigose, kurių savininkė yra valstybė ar savivaldybė, ir savivaldybių kultūros centruose, kurių teisinė forma yra viešoji įstaiga ir kurių dalininkės yra dvi ar daugiau savivaldybių, organizavimo ir vykdymo tvarkos aprašas, Mokytojų priėmimo ir atleidimo iš darbo tvarkos aprašas, prašymas dalyvauti atrankoje ar konkurse.	konkurso atveju, kai tai numato teisės aktai – konkurso eigos metu užfiksuoto pokalbio garso įrašas.		teisės aktų nustatyta tvarka asmens duomenys gali būti teikiami kompetentingoms valstybės institucijoms, įskaitant teisėsaugos institucijas ir teismus.		

Darbo santykių administravimo, įskaitant darbo sutarties sudarymo, vykdymo, nutraukimo, darbo organizavimo bei visų darbo sutartyje ar teisės aktuose numatytų teisių ir pareigų įgyvendinimo tikslais:	Reglamento 6 str. 1 d. (b) p. (siekiant tinkamai vykdyti sutartį ir įgyvendinti iš sutarties kylančias teises ir pareigas), Reglamento 6 str. 1 d. (c) p. (siekiant įvykdyti teisinę prievolę), Reglamento 10 str., Respublikos asmens duomenų teisinės apsaugos įstatymo 5 str., Vaiko teisių apsaugos pagrindų įstatymo 30 str. (darbuotojo teistumo duomenų tvarkymui), Lietuvos Respublikos darbo kodeksas, Lietuvos Respublikos švietimo įstatymas, Pedagogų registro informacinės sistemos nuostatai, kiti įstaigos kaip darbdavio pareigas bei darbo teisinius santykius reglamentuojantys teisės aktai, darbo sutartis.	Vardas, pavardė, paso ar asmens tapatybės kortelės duomenys (jei nėra šių dokumentų – duomenys iš kitų asmens tapatybę patvirtinančių dokumentų), gyvenamosios vietos adresas, telefono numeris, elektroninio pašto adresas, pareigos, parašas, pareigybės lygis, etato dydis, kvalifikacinė kategorija, darbo patirtis, duomenys apie priėmimą (perkėlimą) į pareigas, atleidimą iš pareigų, duomenys apie atostogas, duomenys apie darbo užmokestį, išeitines išmokas, kompensacijas, pašalpas, banko sąskaitų numeriai, informacija apie darbo laiką, informacija apie skatinimus ir nuobaudas, informacija apie atliktus darbus ir užduotis, duomenys apie išsilavinimą, duomenys apie mokymus, kvalifikacijos atestatų kopijos, nepilnamečių vaikų gimimo liudijimų kopijos ar kitų teisę į darbo ir socialines garantijas patvirtinančių dokumentų duomenys ir (ar) kopijos (kai tai būtina darbuotojo teisėms įgyvendinti, darbdavio teisės aktuose nustatytoms pareigoms vykdyti, mokesčių ir socialinio draudimo prievolėms įvykdyti arba priimtų sprendimų pagrįstumui užtikrinti atliekant kontrolę ar auditą), santuokos (jeigu keitėsi pavardė ir negalima nustatyti tapatybės pagal asmens kodą), mirties (mirus darbuotojui arba jo artimiesiems) išrašai, kiti duomenys reikalingi tvarkyti finansinei apskaitai, kita informacija, kuri patvirtina atitiktį Lietuvos Respublikos vaiko teisių apsaugos pagrindų įstatymo 30 str. reikalavimams (tvarkoma tik tiek, kiek būtina darbuotojo atitikčiai teisės aktuose nustatytiems nepriekaištingos reputacijos reikalavimams įvertinti ir periodiškai tikrinti, kai tai numatyta teisės aktuose),	Esami ir buvę darbuotojai, darbuotojo vaikai ar kiti šeimos nariai.	Valstybinio socialinio draudimo fondo valdyba, Valstybinė mokesčių inspekcija, Lietuvos Respublikos švietimo, mokslo ir sporto ministerija, Lietuvos Respublikos sveikatos apsaugos ministerija, Trakų rajono savivaldybės administracija, Nacionalinė švietimo agentūra, Valstybės duomenų agentūra, Informatikos ir ryšių departamentas prie Lietuvos Respublikos vidaus reikalų ministerijos, kvalifikacijos kėlimo įstaigos – duomenų tvarkytojai, UAB „NEVDA“ (Deka Office) – duomenų tvarkytojas, prieglobos (hostingo) paslaugų teikėjas - duomenų tvarkytojas, Teisės aktų nustatyta tvarka asmens duomenys gali būti teikiami kompetentingoms valstybės institucijoms,	Duomenų subjektas; Pedagogų registro informacinė sistema, Įtariamųjų, kaltinamųjų ir nuteistųjų registras (gaunama informacija apie teistumą ir atitiktį nepriekaištingos reputacijos reikalavimui), darbuotojas (darbuotojo vaikų ar kitų šeimos narių duomenys).	Dokumentai dėl priėmimo į pareigas, perkėlimo, pavadavimo, atleidimo iš pareigų, darbo užmokesčio, atostogų vaikui prižiūrėti, tėvystės atostogų, prastovų – 50 m.; Dokumentai dėl grafikų (periodinių sveikatos tikrinimų, pamainų, budėjimo, atostogų), kasmetinių, nemokamų, tikslinių, pailgintų, papildomų ir kitų atostogų, komandiruočių, papildomų poilsio dienų, sutrumpinto darbo laiko, darbo atlikimo būdo (nuotolinio darbo) – 3 m. Asmens bylos dokumentai – 3 m. (nuo tarnybos (darbo) santykių pabaigos); Darbo sutartys ir jų priedai (susitarimai dėl

		kita informacija, kuri patvirtina atitiktį Lietuvos Respublikos švietimo įstatymo 48 str. reikalavimams (mokytojams).		įskaitant teisėsaugos institucijas ir teismus.		papildomų darbo sutarties sąlygų ir kt.) –50 m. (nuo sutarties nutraukimo). Pastaba. Neįsigaliojusios darbo sutartys – 3 m.; Veiklos vertinimo dokumentai – 3 m.; Įspėjimai dėl darbo sutarties nutraukimo, atleidimo iš pareigų, pranešimai apie darbo sąlygas – 3 m.; Įstaigos (draudėjo) pranešimai apie apdraustuosius valstybiniu socialiniu draudimu (priėmimą, atleidimą, atostogas) ir draudėją, gauti pranešimai apie išduotus nedarbingumo ar nėštumo ir gimdymo atostogų pažymėjimus – 10 m.; Komandiruočių ataskaitos – 3 m.;

						Darbuotojų mokymo metų planai ir ataskaitos – 3 m.; Darbo laiko apskaitos žiniaraščiai – 10 m.; Darbuotojų neblaivumo nustatymo dokumentai (pasiaiškinimai, nušalinimo aktai, siuntimai, žurnalai ir kt.) – 3 m. Pastaba. Jei pradedamas vidaus tyrimas – 5 m. (nuo tyrimo pabaigos); Darbuotojų prašymai (atostogų ir kt.) – 3 m.; Direktoriaus įsakymai personalo klausimais – 50 m.
Darbuotojų saugos ir sveikatos užtikrinimo, saugių darbo sąlygų sudarymo tikslais:	Reglamento 6 str. 1 d. (c) p. (kai asmens duomenų tvarkymas būtinas darbdaviui vykdant teisės aktuose nustatytas pareigas); Reglamento 9 str. 2 d. (b) p. (kai tvarkomi specialių kategorijų asmens duomenys (sveikatos duomenys), būtini	Darbuotojo vardas, pavardė; pareigos, darbo funkcija, darbo vieta; privalomųjų sveikatos patikrinimų duomenys; sveikatos priežiūros įstaigos išvada apie darbuotojo tinkamumą dirbti pagal pareigas; sveikatos patikrinimo data ir galiojimo terminas; darbuotojų saugos ir sveikatos instruktavimo duomenys (instruktavimo data, rūšis, darbuotojo parašas);	Esami ir buvę darbuotojai.	Sveikatos priežiūros įstaigos, prieglobos (hostingo) paslaugų teikėjas - duomenų tvarkytojas. Teisės aktų nustatyta tvarka asmens duomenys gali būti teikiami kompetentingoms valstybės institucijoms,	Duomenų subjektas, sveikatos priežiūros įstaigos.	Profesinių ligų priežasčių tyrimo aktai, profesinių ligų patvirtinimo aktai, Centrinės darbo medicinos ekspertų komisijos išvados ir kiti tyrimo dokumentai – 50 m.

	darbdavio prievolėms ir darbuotojo teisėms darbo ir socialinės apsaugos srityje įgyvendinti); Lietuvos Respublikos darbo kodekso 158 str., Lietuvos Respublikos darbuotojų saugos ir sveikatos teisės aktai, reglamentuojantys privalomuosius sveikatos patikrinimus, profesinės rizikos vertinimą, nelaimingų atsitikimų darbe tyrimą, darbuotojų instruktavimą ir kitas darbdavio pareigas; kiti teisės aktai, nustatantys darbdavio pareigas darbuotojų saugos ir sveikatos srityje.	profesinės rizikos vertinimo ir darbuotojų saugos užtikrinimo dokumentuose esantys duomenys; duomenys, susiję su nelaimingais atsitikimais darbe, incidentais ar profesinėmis ligomis (kai darbuotojas yra susijęs su įvykiu); darbuotojų neblaivumo nustatymo duomenys (kai atliekamas patikrinimas); asmeninių apsaugos priemonių išdavimo ir apskaitos duomenys; kiti duomenys, būtini teisės aktuose nustatytoms darbuotojų saugos ir sveikatos pareigoms įgyvendinti.		įskaitant teisėsaugos institucijas ir teismus.		Darbo sąlygų ir aplinkos, profesinės rizikos, darbuotojų saugos ir sveikatos būklės tyrimo, vertinimo ir kontrolės dokumentai – 50 m. Darbuotojų saugos ir sveikatos instruktavimų apskaitos dokumentai (žurnalai ir kt.) – 3 m. Įvykių darbe, nelaimingų atsitikimų darbe, nelaimingų atsitikimų pakeliui į darbą ar iš darbo aktų registravimo žurnalas – 25 m. Sunkių, lengvų, mirtinų nelaimingų atsitikimų darbe aktai ir kiti tyrimo dokumentai – 25 m. Incidentų darbe registravimo dokumentai (žurnalai ir kt.) – 5 m. Incidentų darbe tyrimo aktai ir kiti

						tyrimo dokumentai 3 m. Periodinių sveikatos tikrinimų dokumentai (patikrinimo išvada / pažyma) – 3 m. (nuo tarnybos (darbo) santykių pabaigos); Darbuotojų neblaivumo nustatymo dokumentai (pasiaiškinimai, nušalinimo aktai, siuntimai, žurnalai ir kt. 3 m. Pastaba. Jei pradedamas vidaus tyrimas, saugoma 5 m. (nuo tyrimo pabaigos), Darbuotojams išduodamų asmeninių apsaugos priemonių apskaitos dokumentai – 1 m. (nuo priemonės tinkamumo naudoti termino pabaigos), Gaisrinės saugos instruktažų apskaitos

						dokumentai (žurnalai ir kt.) – 3 m.
Darbuotojų sveikinimo gimimo dienos proga tikslu:	Reglamento 6 str. 1 d. (a) p. (duomenų subjekto sutikimas).	Gimimo mėnuo ir diena	Esami darbuotojai.		Duomenų subjektas.	Iki darbuotojo sutikimo atšaukimo arba darbo santykių pabaigos (priklausomai nuo to, kuris įvykis įvyks anksčiau). Sutikimų davimo ir atšaukimo faktą patvirtinantys duomenys saugomi 2 metus nuo sutikimo atšaukimo arba darbo santykių pabaigos.
Studentų praktikos organizavimo ir vykdymo tikslais:	Reglamento 6 str. 1 d. (b) p. (praktikos sutarties sudarymui ir vykdymui), praktikos atlikimo sutartis.	Vardas, pavardė, kontaktiniai duomenys (telefono numeris, elektroninio pašto adresas), gimimo data ir (ar) kiti tapatybės nustatymo duomenys – kai būtina praktikos sutarčiai sudaryti, parašas, gyvenimo aprašyme pateikti duomenys apie išsilavinimą, kompetencijas ir patirtį, kita praktikos organizavimui ir vykdymui būtina praktikanto pateikta informacija.	Praktikantai, studentai, pageidaujantys atlikti praktiką.	Praktikos sutarties šalis, prieglobos (hostingo) paslaugų teikėjas - duomenų tvarkytojas, UAB „NEVDA“ (Deka Office) – duomenų tvarkytojas, teisės aktų nustatyta tvarka asmens duomenys gali būti teikiami kompetentingoms valstybės institucijoms, įskaitant teisėsaugos institucijas ir teismus.	Duomenų subjektas.	Praktikos sutartys ir su praktikos atlikimu susiję dokumentai saugomi 3 metus nuo praktikos sutarties pabaigos.
Mokymo sutarties sudarymo, vykdymo bei	Reglamento 6 str. 1 d. (b) p. (kai asmens duomenų tvarkymas būtinas ugdymo	Mokinio vardas, pavardė, gimimo data, asmens kodas (jeigu kodo nėra – gimimo data ir lytis), telefono numeris, el. pašto	Mokiniai,	Lietuvos Respublikos švietimo, mokslo ir sporto ministerija,	Duomenų subjektas,	Mokymo sutartys – 10 m.

ugdymo proceso organizavimo tikslais:	sutarčiai sudaryti, vykdyti ir iš sutarties kylančioms teisėms bei pareigoms įgyvendinti), Reglamento 6 str. 1 d. (c) p. (siekiant įvykdyti teisinę prievolę), Reglamento 9 str. 2 d. (g) p. (kai specialiųjų kategorijų asmens duomenų (sveikatos duomenų, duomenų apie specialiuosius ugdymosi poreikius) tvarkymas būtinas dėl svarbaus viešojo intereso priežasčių, vadovaujantis Lietuvos Respublikos teisės aktais), Lietuvos Respublikos švietimo įstatymas, Mokinių registro informacinės sistemos nuostatai, Dienynų sudarymo elektroninio dienyno pagrindu tvarkos aprašas, Mokinių, turinčių specialiųjų ugdymosi poreikių, ugdymo ir švietimo pagalbos teikimo organizavimo tvarkos aprašą, Mokinių lankomumo apskaitos ir mokyklos nelankymo prevencijos tvarkos aprašas,	adresas, deklaruotos gyvenamosios vietos adresas ir deklaravimo data, faktinės gyvenamosios vietos adresas, parašas, gimtoji kalba (-os), specialiųjų ugdymo ir poreikių lygis (jeigu asmuo nurodė, pateikė tai įrodančius dokumentus), užsienio kalbos, mokymas namie dėl ligos ar patologinės būklės (dalykai, valandų skaičius per savaitę), sveikatos duomenys, patirtos fizinės traumos ugdymo proceso metu data (jeigu patyrė), klasė (grupė), įvertinimai, programa, lankomumo informacija, nelankymo dienas pagrindžiantys dokumentai, kita informacija, kuri būtina sutarčiai vykdyti. Mokinio tėvų (kitų atstovų) vardai, pavardės, telefono numeriai, el. pašto adresai.	mokinio tėvai (kiti atstovai).	Nacionalinė švietimo agentūra, Trakų rajono savivaldybės administracija, el. dienyno administratorius – duomenų tvarkytojas, prieglobos (hostingo) paslaugų teikėjas - duomenų tvarkytojas, UAB „NEVDA“ (Deka Office) – duomenų tvarkytojas, Trakų visuomenės sveikatos biuras.	Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinė sistema (E. Sveikata).	(pasibaigus sutarčiai); Mokinių, mokinių tėvų (globėjų, rūpintojų) prašymai – 3 m.; Mokinių nelaimingų atsitikimų aktai ir kiti tyrimo dokumentai – 50 m.; Direktoriaus įsakymai mokinių klausimais ir registras – 10 m.

	kiti įstaigos veiklą reglamentuojantys teisės aktai, mokymo sutartis.					
Užkrečiamųjų ligų (pedikuliozės, niežų ir kt.) plitimo prevencijos tikslu:	Reglamento 6 str. 1 d. (b) p. (siekiant tinkamai vykdyti sutartį ir įgyvendinti iš sutarties kylančias teises ir pareigas), Reglamento 9 str. 2 d. (g) p. (tvarkyti duomenis būtina dėl svarbaus viešojo intereso priežasčių), Lietuvos Respublikos žmonių užkrečiamųjų ligų profilaktikos ir kontrolės įstatymas, Visuomenės sveikatos priežiūros organizavimo mokykloje tvarkos aprašas, Vaikų sveikatos stebėsenos informacinės sistemos nuostatai, mokymo sutartis.	Mokinio vardas, pavardė, gimimo data, grupė, informacija apie užkrečiamas ligas. Siekiant užtikrinti tinkamą užkrečiamųjų ligų ir jų plitimo profilaktikos priemonių taikymą ir dalyvaujant įgyvendinant užkrečiamosios ligos židinio ar protrūkio kontrolės priemones gali būti tvarkomas ir mokinio asmens kodas. Tėvų (kitų atstovų) kontaktinė informacija: telefono numeris, el. pašto adresas.	Mokiniai, mokinio tėvai (kiti atstovai).	Lietuvos Respublikos sveikatos apsaugos ministerija, Higienos institutas, Trakų visuomenės sveikatos biuras.	Duomenų subjektas arba jo įstatyminis atstovas.	Nesaugomi.
Pagalbos organizavimo ir koordinavimo procedūrų užtikrinimo tikslais:	Reglamento 6 str. 1 d. (a) p. (duomenų subjekto sutikimas), Reglamento 6 str. 1 d. (b) p. (siekiant tinkamai vykdyti sutartį ir įgyvendinti iš sutarties kylančias teises ir pareigas), Reglamento 6 str. 1 d. (c) p. (siekiant įvykdyti teisinę prievolę),	Mokiniai vardas, pavardė, gimimo data, gyvenamoji vieta, sveikatos duomenys, ugdymosi ir elgesio ypatumai, pirminis vaiko specialiųjų ugdymosi poreikių, kylančių ugdymo(si) procese, įvertinimas. Tėvų (kitų atstovų) vardas, pavardė, kontaktai, parašas.	Mokiniai, mokinio tėvai (kiti atstovai).	Pedagoginė – psichologinė tarnyba, Valstybės vaiko teisių apsaugos ir įvaikinimo tarnyba, prieglobos (hostingo) paslaugų teikėjas - duomenų tvarkytojas,	Duomenų subjektas, Psichologinė – pedagoginė tarnyba, Valstybės vaiko teisių apsaugos ir įvaikinimo tarnyba.	5 metai.

	Reglamento 9 str. 2 d. (g) p. (tvarkyti duomenis būtina dėl svarbaus viešojo intereso priežasčių), Lietuvos Respublikos švietimo įstatymo 43 str. 20 d., Lietuvos Respublikos vaiko minimalios ir vidutinės priežiūros įstatymo 30 str., Mokinio specialiųjų ugdymosi poreikių (išskyrus atsirandančius dėl išskirtinių gabumų) pedagoginiu, psichologiniu, medicininiu ir socialiniu pedagoginiu aspektais įvertinimo ir specialiojo ugdymosi skyrimo tvarkos aprašas; Specialiosios pedagoginės pagalbos teikimo asmenims tvarkos aprašas; Psichologinės pagalbos teikimo tvarkos aprašas; Socialinės pedagoginės pagalbos teikimo vaikams ir mokiniams tvarkos aprašas, Vaiko gerovės komisijos funkcijų, sudarymo ir jos darbo organizavimo tvarkos aprašas.			UAB „NEVDA“ (Deka Office) – duomenų tvarkytojas, el. dienyno administratorius – duomenų tvarkytojas.		
Pagalbos teikimo užtikrinimo tikslu:	Reglamento 6 str. 1 d. (b) p. (siekiant tinkamai vykdyti	Mokinio vardas, pavardė, gimimo data, gyvenamoji vieta, sveikatos duomenys,	Mokiniai,	Pedagoginė – psichologinė tarnyba,	Duomenų subjektas,	Pagalbos teikimo dokumentai – 5 m.

	sutartį ir įgyvendinti iš sutarties kylančias teises ir pareigas), Reglamento 6 str. 1 d. (c) p. (siekiant įvykdyti teisinę prievolę), Reglamento 9 str. 2 d. (g) p. (tvarkyti duomenis būtina dėl svarbaus viešojo intereso priežasčių), Reglamento 6 str. 1 d. (a) p. (duomenų subjekto ar jo atstovo sutikimas, kai pagalba teikia sutikimo pagrindu); Lietuvos Respublikos švietimo įstatymo 43 str. 20 d., Lietuvos Respublikos vaiko minimalios ir vidutinės priežiūros įstatymo 30 str., Specialiosios pagalbos teikimo mokyklose (išskyrus aukštąsias mokyklas) tvarkos aprašas, Vaiko gerovės komisijos funkcijų, sudarymo ir jos darbo organizavimo tvarkos aprašas.	ugdymosi ir elgesio ypatumai, pirminis vaiko specialiųjų ugdymosi poreikių, kylančių ugdymo(si) procese, įvertinimas, kalba (kuria mokosi ir kalba namuose), fizinės brandos duomenys, vaiko kalbėjimo ir kalbos gebėjimai, sutrikimai ir sunkumai, kalbėjimo ir kalbos vertinimo išvada, informacija apie lankomas logopedines pratybas, iškelti tikslai ir jų įgyvendinimas. Tėvų (kitų atstovų) vardas, pavardė, kontaktai, parašas.	mokinio tėvai (kiti atstovai).	Valstybės vaiko teisių apsaugos ir įvaikinimo tarnyba, prieglobos (hostingo) paslaugų teikėjas - duomenų tvarkytojas, el. dienyno administratorius – duomenų tvarkytojas, UAB „NEVDA“ (Deka Office) – duomenų tvarkytojas.	Psichologinė – pedagoginė tarnyba, Valstybės vaiko teisių apsaugos ir įvaikinimo tarnyba.	
Mokinių, turinčių ugdymosi sunkumų ar švietimo pagalbos poreikių, nustatymo tikslu:	Reglamento 6 str. 1 d. (a) p. (duomenų subjekto sutikimas), Reglamento 6 str. 1 d. (b) p. (siekiant tinkamai vykdyti sutartį ir įgyvendinti iš	Mokinio vardas, pavardė, gimimo data, gyvenamoji vieta, sveikatos duomenys, ugdymosi ir elgesio ypatumai, pirminis vaiko specialiųjų ugdymosi poreikių, kylančių ugdymo(si) procese, įvertinimas.	Mokiniai, mokinio tėvai (kiti atstovai).	Pedagoginė-psichologinė tarnyba, Valstybės vaiko teisių apsaugos ir įvaikinimo tarnyba,	Duomenų subjektas, Psichologinė – pedagoginė tarnyba,	5 metai;

	sutarties kylančias teises ir pareigas), Reglamento 6 str. 1 d. (c) p. (siekiant įvykdyti teisinę prievolę), Reglamento 9 str. 2 d. (g) p. (kai tvarkomi duomenys apie kalbos sutrikimus, specialiuosius ugdymosi poreikius ar kitą informaciją, susijusią su vaiko sveikatos būkle), Lietuvos Respublikos švietimo įstatymo 43 str. 20 d., Lietuvos Respublikos vaiko minimalios ir vidutinės priežiūros įstatymo 30 str., Vaiko gerovės komisijos funkcijų, sudarymo ir jos darbo organizavimo tvarkos aprašas.	Tėvų (kitų atstovų) vardas, pavardė, kontaktai, parašas.		prieglobos (hostingo) paslaugų teikėjas - duomenų tvarkytojas, el. dienyno administratorius – duomenų tvarkytojas, UAB „NEVDA“ (Deka Office) – duomenų tvarkytojas.	Valstybės vaiko teisių apsaugos ir įvaikinimo tarnyba.	
Pažymų, pažymėjimų ir atestatų išdavimo, registravimo, apskaitos ir teisės aktuose nustatyto jų saugojimo tikslu:	Reglamento 6 str. 1 d. (c) p. (siekiant įvykdyti teisinę prievolę), Pažymėjimų ir brandos atestatų išdavimo tvarkos aprašas, kiti konkrečiam dokumentui taikomi švietimo srities ir dokumentų valdymo teisės aktai.	Mokinio vardas, pavardė, mokomieji dalykai, įvertinimai, pažymėjimo / atestato serija ir numeris, išdavimo data, registracijos numeris, kiti konkrečiam dokumentui išduoti bei apskaityti būtini duomenys.	Mokiniai	Nacionalinė švietimo agentūra, Lietuvos Respublikos švietimo, mokslo ir sporto ministerija.	Duomenų subjektas, Mokinių registro informacinė sistema.	25 arba 50 metų.
Egzaminų ir mokinių pasiekimų patikrinimų	Reglamento 6 str. 1 d. (c) p. (siekiant įvykdyti teisinę prievolę),	Mokinio vardas, pavardė, klasė, mokomoji kalba, lytis, mokymo programa ir kiti asmens duomenys, kurių tvarkymas	Mokiniai	Nacionalinė švietimo agentūra,	Duomenų subjektas, Mokinių registras,	Pradinio ugdymo pažymėjimų

organizavimo, vykdymo, administravimo, rezultatų apskaitos ir teisės aktuose nustatytų pareigų vykdymo tikslais:	Nacionalinių mokinių pasiekimų patikrinimų organizavimo ir vykdymo tvarkos aprašas, Pagrindinio ugdymo pasiekimų patikrinimo organizavimo ir vykdymo tvarkos aprašas.	konkrečiai numatytas taikomuose teisės aktuose ir yra būtinas egzaminui / pasiekimų patikrinimui organizuoti ir vykdyti.		Lietuvos Respublikos švietimo, mokslo ir sporto ministerija.	NECIS.	apskaitos žurnalas, Mokymosi pasiekimų pažymėjimų apskaitos žurnalas – 25 m. Pagrindinio ugdymo pasiekimų patikrinimų protokolai – 25 m.
Nesimokančių vaikų ir mokyklos nelankančių mokinių apskaitos, lankymo užtikrinimo, mokyklos nelankymo prevencijos ir teisės aktuose nustatytų pareigų vykdymo tikslais:	Reglamento 6 str. 1 d. (c) p. (siekiant įvykdyti teisinę prievolę), Nesimokančių vaikų ir mokyklos nelankančių mokinių informacinės sistemos nuostatai, Savivaldybės teritorijoje gyvenančių vaikų apskaitos tvarkos aprašas.	Mokinio vardas, pavardė, asmens kodas arba, kai teisės aktuose nustatyta, gimimo data, gyvenamosios vietos adresas, lytis, mokykla / klasė, mokyklos nelankymo faktas, praleistų pamokų skaičius, nelankymo priežastys ir kiti NEMIS nuostatuose konkrečiai nustatyti bei šiam tikslui būtini duomenys.	Mokiniai, mokinio tėvai (kiti atstovai).	Nacionalinė švietimo agentūra, Lietuvos Respublikos švietimo, mokslo ir sporto ministerija.	Duomenų subjektas.	10 metų.
Elektroninio mokinio pažymėjimo išdavimo, apskaitos ir administravimo tikslais:	Reglamento 6 str. 1 d. (c) p. (siekiant įvykdyti teisinę prievolę), Mokinio pažymėjimo išdavimo tvarkos aprašas.	Mokinio vardas, pavardė, nuotrauka, gimimo data, švietimo teikėjo pavadinimas, elektroninio mokinio pažymėjimo numeris, galiojimo data ir kiti teisės aktuose nustatyti bei pažymėjimui išduoti būtini duomenys.	Mokiniai.	Lietuvos Respublikos švietimo, mokslo ir sporto ministerija,	Duomenų subjektas.	4 m. (po paskutinio įrašo).
Prašymų, skundų ar kitų kreipimųsi nagrinėjimo tikslu:	Reglamento 6 str. 1 d. (c) p. (siekiant įvykdyti teisinę prievolę), Lietuvos Respublikos švietimo įstatymas, Lietuvos Respublikos viešojo administravimo įstatymas,	Vardas, pavardė, el. pašto adresas, telefono numeris, parašas bei kita prašyme ar kreipimesi pateikta informacija, būtina jo išnagrinėjimui.	Asmenys, pateikę prašymą, skundą ar kitą kreipimąsi ir jų atstovai, Asmens, galinčio suteikti daugiau informacijos apie pranešime aprašytas aplinkybes duomenys.	Valstybės institucijos, kurios pateikė prašymą ar kitą kreipimąsi, valstybės institucijos, kompetentingos nagrinėti kreipimąsi (kai duomenų valdytojas nekompetentingas nagrinėti),	Duomenų subjektas arba jo atstovas.	1 m. (nuo sprendimo priėmimo įstaigoje); Dėl ginčijamo sprendimo saugoma 5 m. (nuo ginčą nagrinėjusios institucijos

	Lietuvos Respublikos teisės gauti informaciją ir duomenų pakartotinio naudojimo įstatymas, Asmenų prašymų ir skundų nagrinėjimo viešojo administravimo subjektuose taisyklės.			valstybės institucijos, kurios kreipimesi nurodytos kaip papildomi adresatai ar su kuriomis susijęs kreipimasis, prieglobos (hostingo) paslaugų teikėjas - duomenų tvarkytojas, el. dienyno administratorius – duomenų tvarkytojas, UAB „NEVDA“ (Deka Office) – duomenų tvarkytojas. Teisės aktų nustatyta tvarka asmens duomenys gali būti teikiami kompetentingoms valstybės institucijoms, įskaitant teisėsaugos institucijas ir teismus.		galutinio sprendimo priėmimo);
Elektroninio dienyno administravimo tikslu:	Reglamento 6 str. 1 d. (c) p. (siekiant įvykdyti teisinę prievolę), Reglamento 9 str. 2 d. (g) p. (kai specialiųjų kategorijų asmens duomenų (sveikatos duomenų, duomenų apie specialiuosius ugdymosi poreikius tvarkymas būtinas dėl svarbaus viešojo intereso priežasčių, vadovaujantis Lietuvos Respublikos teisės aktais), Dienynų sudarymo elektroninio dienyno duomenų pagrindu tvarkos aprašas,	Mokinio vardas, pavardė, gimimo data, klasė, mokslo metai, įvertinimai, duomenys apie sveikatą (kai jų tvarkymas būtinas elektroniniame dienyne), elektroninio pašto adresas, telefono numeris; Tėvų (kitų teisėtų atstovų) duomenys: vardas, pavardė, gyvenamosios vietos adresas, elektroninio pašto adresas, telefono numeris, ryšys su mokiniu. Darbuotojų duomenys: vardas, pavardė, pareigos, elektroninio pašto adresas (prieigų administravimo tikslu). Kiti duomenys: sistemoje pateikti prašymai, susirašinėjimas ir kita informacija, kurioje gali būti asmens duomenų.	Mokiniai, mokinio tėvai (kiti atstovai), darbuotojai.	Lietuvos Respublikos švietimo, mokslo ir sporto ministerija (Mokinių registro informacinė sistema ir Pedagogų registras), Nacionalinė švietimo agentūra, el. dienyno administratorius – duomenų tvarkytojas.	Duomenų subjektas arba jo įstatyminis atstovas, Mokinių registro informacinė sistema, Pedagogų registras.	2 metai po ugdymo programos baigimo, jeigu teisės aktai nenustato ilgesnio saugojimo termino.

	Trakų suaugusiųjų mokymo centro elektroninio dienyno tvarkymo nuostatai.					
Neformaliojo vaikų švietimo organizavimo tikslu:	Reglamento 6 str. 1 d, (b) p. (kai asmens duomenys tvarkomi siekiant sudaryti ir vykdyti mokymo sutartį dėl neformaliojo vaikų švietimo); Reglamento 6 str. 1 d. (c) p. (kai asmens duomenys tvarkomi vykdant duomenų valdytojui teisės aktuose nustatytas pareigas, susijusias su NVŠ organizavimu, mokinių registravimu, apskaita ir mokymo sutarčių saugojimu), Lietuvos Respublikos švietimo įstatymas, Neformaliojo vaikų švietimo programų finansavimo ir administravimo tvarkos aprašas. mokymo sutartis dėl neformaliojo vaikų švietimo.	Mokinio vardas, pavardė, asmens kodas, parašas (kai mokinys pats pasirašo mokymo sutartį). Vardas, pavardė, telefono numeris, elektroninio pašto adresas, gyvenamosios vietos adresas, parašas (kai mokymo sutartį sudaro ir pasirašo mokinio tėvai / kiti teisėti atstovai). Mokinio tėvų (kitų įstatyminių atstovų) vardai, pavardės, tel. Nr., el. paštas, gyvenamosios vietos adresas, parašas (kai vaikui mažiau nei 14 m.).	Mokiniai, mokinio tėvai (kiti atstovai).		Duomenų subjektas.	Neformaliojo švietimo dienynas - 2 m. (po programos baigimo).
Nemokamo maitinimo organizavimo tikslu:	Reglamento 6 str. 1 d. (c) p. (siekiant įvykdyti duomenų valdytojui taikomą teisinę prievolę organizuoti ir administruoti mokinių nemokamą maitinimą),	Mokinio vardas, pavardė, asmens kodas, gyvenamosios vietos adresas, telefono numeris, elektroninio pašto adresas; kiti teisės aktuose nustatyti duomenys ir dokumentai (ar jų kopijos), reikalingi nemokamam maitinimui skirti ir administruoti. Vardas, pavardė, asmens kodas, gyvenamosios vietos adresas, kontaktinis	Mokiniai, mokinio tėvai (kiti atstovai).	Trakų rajono savivaldybės administracija, Lietuvos Respublikos socialinės apsaugos ir darbo ministerija.	Duomenų subjektas.	Socialinės paramos mokiniams organizavimo dokumentai – 5 m.

	Lietuvos Respublikos socialinės paramos mokiniams įstatymas; Lietuvos Respublikos Vyriausybės patvirtintas Mokinių nemokamo maitinimo mokyklose tvarkos aprašas; savivaldybės teisės aktai, reglamentuojantys mokinių nemokamo maitinimo organizavimą ir administravimą.	telefono numeris, parašas; kiti teisės aktuose nustatyti duomenys ir dokumentai (ar jų kopijos).				
Savirūpos pagalbos suteikimo tikslu:	Reglamento 6 str. 1 d. (c) p. (siekiant įvykdyti teisinę prievolę), Reglamento 6 str. 1 d. (e) p. (kai tvarkymas būtinas viešojo intereso labui / vykdant viešosios valdžios funkcijas), Reglamento 9 str. 2 d. (h) p. (sveikatos ar socialinės priežiūros ar gydymo teikimo arba sveikatos ar socialinės priežiūros sistemų ir paslaugų valdymo), Visuomenės sveikatos priežiūros organizavimo mokykloje tvarkos aprašas, Mokinių, sergančių lėtinėmis neinfekcinėmis ligomis, savirūpos proceso organizavimo tvarkos aprašas, mokinio tėvų (kitų atstovų) prašymas.	Mokinio vardas, pavardė, klasė, gimimo data, gyvenamosios vietos adresas, tėvų pateikti duomenys/medicininės pažymos apie savirūpos poreikį. Mokinio tėvų (kitų atstovų) vardai, pavardės, kontaktiniai telefonai, giminystės ryšys su mokiniu.	Mokiniai, mokinio tėvai (kiti atstovai).	Trakų visuomenės sveikatos biuras.	Duomenų subjektas arba jo atstovas, Vaikų sveikatos stebėsenos informacinė sistema (VSS IS).	Iki mokymo sutarties pabaigos.

Finansinės apskaitos tvarkymo ir teisės aktuose nustatytų finansinės apskaitos prievolių vykdymo tikslais:	Reglamento 6 str. 1 d. (c) p. (siekiant įvykdyti teisinę prievolę), Lietuvos Respublikos finansinės apskaitos įstatymas.	Vardas, pavardė, gimimo data arba asmens kodas (kai tvarkomas), gyvenamosios vietos adresas, telefono numeris, elektroninio pašto adresas, banko sąskaitos numeris, bankinių mokėjimų duomenys ir išrašai, individualios veiklos pažymos ar verslo liudijimo duomenys (prekių, darbų ar paslaugų teikėjų ir gavėjų), mokėjimų ir įsiskolinimų informacija, apskaitos dokumentų duomenys bei kiti finansinei apskaitai tvarkyti būtini asmens duomenys.	Darbuotojai, prekių, darbų ar paslaugų teikėjai ir gavėjai (įskaitant nuomininkus bei kitus bendradarbiaujančius asmenis) ir jų atstovai.	Valstybinio socialinio draudimo fondo valdyba, Valstybinė mokesčių inspekcija, Trakų rajono savivaldybės administracija, Valstybės duomenų agentūra, prieglobos (hostingo) paslaugų teikėjas - duomenų tvarkytojas.	Duomenų subjektas.	Darbo užmokesčio apskaičiavimo dokumentai (žiniaraščiai arba kiti darbo užmokesčio apskaičiavimo dokumentai) - 50 m.; Pastaba. 50 m. saugojimo terminas taikomas tik vienam iš įstaigoje sudaromų darbo užmokesčio apskaičiavimo dokumentų. Kiti darbo užmokesčio apskaičiavimo dokumentai ir Vidaus administravimo dokumentų saugojimo terminų rodyklėje nenurodyti darbo užmokesčio apskaitos dokumentai saugomi 10 m.; Prašymai dėl neapmokestinamojo pajamų dydžio taikymo, darbo užmokesčio pervedimo į banko sąskaitą - 3 m. (nuo naujo prašymo pateikimo arba tarnybos (darbo)

						santykių pabaigos); Ūkinę operaciją ar ūkinį įvykį patvirtinantys apskaitos dokumentai (sąskaitos faktūros, mokėjimo pavedimai, avanso apyskaitos, kasos pajamų ir išlaidų orderiai ir kt.) - 10 m.; Pirkimo ar paslaugų sutartys, prekių ar paslaugų perėmimo aktai - 10 m. (nuo sutarties įvykdymo); Autorinės, atlikėjo intelektinių paslaugų teikimo sutartys, darbų (kūrinių) priėmimo aktai - 50 m. (nuo sutarties nutraukimo). Pastaba. Iki 2009 m. pasibaigusios sutartys saugomos 10 m. (nuo sutarties nutraukimo);
Viešųjų pirkimų vykdymo, organizavimo ir sudarytų sutarčių vykdymo tikslais:	Reglamento 6 str. 1 d. (c) p. (siekiant įvykdyti teisinę prievolę),	Vardas, pavardė, asmens kodas ir (ar) gimimo data (kai jų pateikimą nustato teisės aktai arba pirkimo dokumentai), individualios veiklos pažymėjimo ar verslo liudijimo duomenys, išsilavinimo	Viešųjų pirkimų dalyvių ir jų atstovų (darbuotojų duomenys).	Viešųjų pirkimų tarnyba (CVP IS),	Duomenų subjektas, viešųjų pirkimų dalyviai.	Planavimo ir pasirengimo pirkimams dokumentai, pirkimo

	Lietuvos Respublikos viešųjų pirkimų įstatymas.	ir kvalifikacijos duomenys (kai taikoma), adresas, telefono numeris, elektroninio pašto adresas, banko sąskaitos numeris, parašas, kiti pirkimo dokumentuose pateikti asmens duomenys.		prieglobos (hostingo) paslaugų teikėjas - duomenų tvarkytojas, kitos institucijos teisės aktų nustatytais atvejais.		dokumentai, paraiškos, pasiūlymai bei jų nagrinėjimo ir vertinimo dokumentai, sprendimų priėmimo, derybų, dialogo ar kiti protokolai, susirašinėjimo su tiekėjais dokumentai, kiti su pirkimo organizavimu susiję dokumentai – 5 m. (nuo pirkimo pabaigos); Viešuosius pirkimus vykdančių asmenų konfidencialumo pasižadėjimai ir nešališkumo deklaracijos – 5 m. (nuo pirkimo pabaigos); Preliminariosios sutartys – 5 m. (nuo pirkimo (paslaugų) sutarties sudarymo); Viešųjų pirkimų, atliekamų įgyvendinant Europos Sąjungos ir užsienio institucijų ar fondų lėšomis finansuojamus

						projektus, dokumentai – 10 m. (nuo projekto įgyvendinimo); Viešųjų pirkimų, atliekamų vykdant investicijų projektus, dokumentai – 10 m. (nuo investicijų projekto įgyvendinimo).
Bendruomenės ir visuomenės informavimo apie įstaigos veiklą tikslu:	Reglamento 6 str. 1 d. (a) p. (duomenų subjekto ar jo atstovo sutikimas).	Vardas, pavardė, kūrybiniai darbai, informacija apie pasiekimus, dalyvavimą renginiuose, konkursuose, nuotrauka, vaizdo bei garso medžiaga, kurioje užfiksuotas duomenų subjektas.	Mokiniai, mokinių tėvai (kiti atstovai), darbuotojai.	Meta Platforms Ireland Ltd. (Facebook); prieglobos (hostingo) paslaugų teikėjas - duomenų tvarkytojas. Asmens duomenys gali būti perduodami į trečiąsias valstybes pagal Europos Komisijos sprendimus arba taikant kitas Reglamento V skyriaus numatytas tinkamas apsaugos priemones, jeigu tai susiję su naudojama platforma.	Duomenų subjektas.	Duomenys saugomi ir viešinami iki kitų mokslo metų pabaigos, o pasibaigus šiam terminui ištrinami ir pašalinami iš viešai prieinamų vietų bei kitų sistemų, kuriose jų ištrynimas yra techniškai įmanomas. Sutikimo davimo ir atšaukimo faktą patvirtinantys duomenys saugomi 2 metus nuo sutikimo atšaukimo arba ugdymo sutarties pabaigos.
Apklausų vykdymo tikslu:	Reglamento 6 str. 1 d. (a) p. (apklausoms, kuriose dalyvavimas yra visiškai savanoriškas ir nėra susijęs su įstaigos teisės aktuose nustatytų funkcijų vykdymu).	Vardas, pavardė, elektroninio pašto adresas.	Mokiniai, mokinio tėvai (kiti atstovai), darbuotojai.	Prieglobos (hostingo) paslaugų teikėjas - duomenų tvarkytojas, el. dienyno administratorius – duomenų tvarkytojas.	Duomenų subjektas.	Kontaktiniai duomenys saugomi iki ugdymo sutarties pabaigos arba sutikimo atšaukimo.

						Sutikimo davimo ir atšaukimo faktą patvirtinantys duomenys saugomi 2 metus nuo sutikimo atšaukimo arba apklausos pabaigos.
Turto nuomos sutarčių sudarymo ir vykdymo tikslais:	Reglamento 6 str. 1 d. (b) p. (siekis tinkamai vykdyti sutartį ir įgyvendinti iš sutarties kylančias teises ir pareigas).	Vardas, pavardė, asmens kodas (tvarkomas tik tais atvejais, kai tai būtina pagal teisės aktus arba tinkamam sutarties vykdymui), gyvenamoji vieta, telefono numeris, elektroninio pašto adresas, banko sąskaitos numeris, įsiskolinimas, parašas.	Turto nuomininkai.	Trakų rajono savivaldybės administracija, prieglobos (hostingo) paslaugų teikėjas - duomenų tvarkytojas.	Duomenų subjektas.	10 m. nuo sutarties pasibaigimo.
Duomenų apsaugos pareigūno funkcijų vykdymo tikslais, įskaitant duomenų subjektų prašymų nagrinėjimą, asmens duomenų saugumo pažeidimų vertinimą:	Reglamento 6 str. 1 d. (c) p. (vykdyti Lietuvos Respublikos įstatymuose nustatytas teisines prievoles), Reglamento 12, 15–21 str., 33 str. 5 d., 34 str., 38 str. 4 d.	Vardas, pavardė, gimimo data, asmens kodas (pavyzdžiui, kai prašymas pasirašomas elektroniniu parašu, jei taikoma), asmens dokumento kopija (kai prašymas teikiamas paštu); Telefono ryšio numeris ir (ar) elektroninio pašto adresas ir (ar) korespondencijos adresas ir (ar) elektroninės siuntos pristatymo dėžutės adresas; Prašymo (pranešimo) pateikimo įstaigai faktas, data, laikas (kai taikoma), prašymo (pranešimo) turinys (ir jame ar jo prieduose esantys asmens duomenys), atsakymo į prašymą (pranešimą) faktas, data, laikas (kai taikoma); Atstovo vardas, pavardė (pavadinimas), gimimo data arba asmens kodas (įmonės kodas), atstovavimo faktą patvirtinančio dokumento kopija; Susirašinėjimas (kai iš jo galima identifikuoti fizinį asmenį), darbovietė, pareigos, parašas, kt.	Prašymą ar pranešimą pateikusio asmens ar asmens, galinčio suteikti daugiau informacijos apie pranešime aprašytas aplinkybes duomenys, duomenų subjektų ir jų atstovų duomenys.	Valstybės institucijos, kurios pateikė prašymą ar kitą kreipimąsi, valstybės institucijos, kompetentingos nagrinėti kreipimąsi (kai duomenų valdytojas nekompetentingas nagrinėti), valstybės institucijos, kurios kreipimesi nurodytos kaip papildomi adresatai ar su kuriomis susijęs kreipimasis, prieglobos (hostingo) paslaugų teikėjas - duomenų tvarkytojas. Teisės aktų nustatyta tvarka asmens duomenys gali būti perduoti teisėsaugos, teisminėms ar ikiteisminėms institucijoms dėl jų atliekamų tyrimų.	Duomenų subjektas ar jo atstovas.	Prašymų dėl duomenų subjektų teisių įgyvendinimo nagrinėjimo dokumentai – 2 metus nuo atsakymo išsiuntimo; Pranešimai apie galimai įvykusį asmens duomenų saugumo pažeidimą ir pranešimo nagrinėjimo dokumentai – 2 metai; Asmens duomenų saugumo pažeidimų registravimo žurnalas – 2 metai nuo paskutinio įrašo žurnale padarymo.

Specializuotos ir (ar) kitos reikalingos pagalbos asmeniui suteikimo tikslu:	Reglamento 6 str. 1 d. (c) p. (siekiant įvykdyti teisinę prievolę), Lietuvos Respublikos apsaugos nuo smurto artimoje aplinkoje įstatymo 13 str. 4 d.	Vardas, pavardė, kontaktiniai duomenys (telefono numeris, elektroninio pašto adresas), informacija apie galimą smurto artimoje aplinkoje atvejį ir kiti asmens duomenys, būtini Lietuvos Respublikos apsaugos nuo smurto artimoje aplinkoje įstatyme nustatytai pareigai įvykdyti.	Mokiniai, mokinio tėvai (kiti atstovai), darbuotojai.	Policija, specializuotos kompleksinės pagalbos centras, Valstybės vaiko teisių apsaugos ir įvaikinimo tarnyba prie Socialinės apsaugos ir darbo ministerijos, prieglobos (hostingo) paslaugų teikėjas - duomenų tvarkytojas. Teisės aktų nustatyta tvarka asmens duomenys gali būti teikiami kompetentingoms valstybės institucijoms, įskaitant teisėsaugos institucijas ir teismus.	Duomenų subjektas.	1 metus.
Interneto svetainės veikimo užtikrinimo, svetainės naudojimo analizės ir lankytojų patirties gerinimo tikslais:	Reglamento 6 str. 1 d. (a) p. (sutikimas) – analitinių, statistinių ir rinkodaros slapukų naudojimas, Reglamento 6 str. 1 dalies (f) p. (teisėtas interesas) – būtinųjų interneto svetainės veikimui užtikrinti reikalingų slapukų naudojimas.	Priklausomai nuo faktiškai naudojamų slapukų gali būti tvarkoma: IP adresas, naršyklės ir įrenginio informacija, apsilankymo svetainėje duomenys, slapukų identifikatoriai, naudojimosi svetaine statistinė informacija.	Įstaigos interneto svetainės lankytojai.	Svetainės prieglobos paslaugų teikėjas, statistikos įrankių teikėjas (jeigu naudojamas), slapukų valdymo platformos teikėjas (jeigu naudojamas), Teisės aktų nustatyta tvarka asmens duomenys gali būti teikiami kompetentingoms valstybės institucijoms, įskaitant teisėsaugos institucijas ir teismus.	Naudojami slapukai.	Pagal konkretaus slapuko galiojimo terminą, nurodytą Interneto svetainės ir slapukų naudojimo politikoje.

Informacinių pranešimų mokiniams ir jų atstovams siuntimo tikslu:	Reglamento 6 str. 1 d. (a) p. (duomenų subjekto ar jo atstovo sutikimas, kai siunčiama informacija, kuri nėra būtina ugdymo procesui).	Vardas, pavardė, el. pašto adresas.	Mokiniai, mokinio tėvai (kiti atstovai).	Prieglobos (hostingo) paslaugų teikėjas - duomenų tvarkytojas, el. dienyno administratorius – duomenų tvarkytojas.	Duomenų subjektas ar jo įstatyminis atstovas.	Iki sutikimo atšaukimo arba mokymo sutarties pabaigos.
DUOMENŲ TVARKYMO TIKSLAS	**DUOMENŲ TVARKYTOJO VYKDOMOS VEIKLOS TEISINIS PAGRINDAS**	**DUOMENŲ APIMTIS** (kokie asmens duomenys tvarkomi nurodytu tikslu)	**DUOMENŲ SUBJEKTŲ KATEGORIJOS**	**DUOMENŲ GAVĖJŲ KATEGORIJOS** (kam perduodami asmens duomenys)	**DUOMENŲ GAVIMO ŠALTINIS**	**DUOMENŲ SAUGOJIMO TRUKMĖ**
Mokinių registro informacinės sistemos tvarkymo tikslu:	Reglamento 28 str. (duomenų tvarkytojas, t. y. įstaiga Mokinių registro informacinės sistemos veikloje dalyvauja teisės aktų nustatyta tvarka kaip registro tvarkytojas vadovaujantis Mokinių registro informacinės sistemos nuostatais.	Asmens duomenų kategorijos nustatytos Mokinių registro informacinės sistemos nuostatų 21 p.	Mokiniai, mokinio tėvai (kiti atstovai).	Lietuvos Respublikos švietimo, mokslo ir sporto ministerija, Nacionalinė švietimo agentūra.	Duomenų subjektas ar jo atstovas. Mokinių registro informacinė sistema.	Archyviniai duomenys saugomi teisės aktų nustatyta tvarka 10 metų.
Pedagogų registro informacinės sistemos tvarkymo tikslu:	Reglamento 28 str. (duomenų tvarkytojas, t. y. įstaiga Pedagogų registro informacinės sistemos veikloje dalyvauja teisės aktų nustatyta tvarka kaip registro tvarkytojas vadovaujantis Pedagogų registro informacinės sistemos nuostatais.	Asmens duomenų kategorijos nustatytos Pedagogų registro informacinės sistemos nuostatų 17 p.	Pedagoginiai darbuotojai ir kiti asmenys, kurių duomenys tvarkomi vadovaujantis Pedagogų registro informacinės sistemos nuostatais.	Lietuvos Respublikos švietimo, mokslo ir sporto ministerija, Nacionalinė švietimo agentūra.	Duomenų subjektas, Pedagogų registro informacinė sistema.	Archyviniai duomenys saugomi teisės aktų nustatyta tvarka 50 metų.

I. POVEIKIO VERTINIMO KLAUSIMAI

Įvertinamas kylantis poveikis fizinių asmenų pagrindinėms teisėms ir laisvėms 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.);

• 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.).

2 lentelė

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

II. GALIMŲ GRĖSMIŲ NUSTATYMAS IR JŲ ATSIRADIMO TIKIMYBĖS

3 lentelė

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 vartotojams arba vartotojų 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 asmens duomenų tvarkymo sistemų?	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, dalyvaujančių asmens duomenų tvarkyme, kurie neturi galimybių tinkamai sunaikinti asmens duomenų laikmenas?	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? (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).	Taip / Ne
20.	Ar yra veiklai (veiklos sričiai) būdingos gerosios saugumo praktikos ar standartų, kurių Jūsų organizacijoje nesilaikoma?	Taip / Ne

III. RIZIKOS VERTINIMAS

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“).

Pasinaudojant lentele nustatoma grėsmės atsiradimo tikimybė kiekvienai vertinamai sričiai ir atitinkamai apskaičiuojama jos galutinė vertė.

4 lentelė

Vertinimo sritis	**Tikimybė**	
	Lygis	**Balas**
Tinklo techniniai ištekliai	Žemas	1
	Vidutinis	2
	Aukštas	3
Procesai ir procedūros, susijusios 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

Bendra grėsmės atsiradimo balų suma	Grėsmės atsiradimo tikimybės lygis
4-5	žemas
6-8	vidutinis
9-12	aukštas

		Poveikio lygis		
		Žemas	Vidutinis	Aukštas
Grėsmės atsiradimo lygis	Žemas			
	Vidutinis			
	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.

Poveikio ir rizikos įvertinimas: Gautas rezultatas – 5 balai. Grėsmės atsiradimo tikimybė žema, poveikis fizinių asmenų pagrindinėms teisėms ir laisvėms dėl galimo asmens duomenų saugumo pažeidimo – žemas, t. y. fizinis asmuo galėtų susidurti su tam tikrais nepatogumais, tačiau reikšmingo poveikio nepatirtų.

IV. PAGAL RIZIKOS ĮVERTINIMĄ NUSTATOMOS TECHNINĖS IR ORGANIZACINĖS PRIEMONĖS

5 lentelė

Priemonės	Atitikmuo BDAR, paaiškinimai ir galimos grėsmės
Asmens duomenų saugumo politika ir procedūros	
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	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 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.
Asmens duomenų saugumo politika turi atitikti teisinius, įstatyminius, reguliavimo ir sutartinius reikalavimus bei būti peržiūrima ir prireikus atnaujinama ne rečiau kaip kartą per metus.	
Vaidmenys ir atsakomybės	
Su asmens duomenų tvarkymu susiję vaidmenys ir atsakomybės turi būti aiškiai apibrėžti ir paskirstyti pagal asmens duomenų saugumo politiką.	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
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).	

	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 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.
Prieigos valdymo politika	
Bendrieji prieigos valdymo reikalavimai (prieigos teisių suteikimo / keitimo / panaikinimo tvarka) turi būti dokumentuoti kaip asmens duomenų saugumo politikos dalys. Kiekvienam vaidmeniui, susijusiam su asmens duomenų tvarkymu, turi būti priskirtos konkrečios prieigos kontrolės teisės, vadovaujantis „būtina žinoti“ (angl. need to know) principu.	Būtina nustatyti prieigos kontrolės politiką sistemoms, naudojamoms tvarkant asmens duomenis. Kontrolė turi būti grindžiama principu „būtina žinoti“, 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, nurodytas šių gairių 84–93 punktuose „Prieigų kontrolė ir autentifikavimas“).
Išteklių ir turto valdymas	
Organizacija turi turėti IT išteklių (naudojamų asmens duomenims tvarkyti) registrą (techninės, programinės ir tinklo įrangos sąrašą). IT išteklių registras turi apimti bent tokią informaciją: IT išteklių tipą (pvz., tarnybinę stotį, kompiuterinę darbo vietą), vietą (fizinę ar elektroninę). IT išteklių registras turi būti reguliariai peržiūrimas ir atnaujinamas.	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 apimti IT išteklių ir tinklo topologijos (schemos), kuri yra naudojama tvarkant asmens duomenis, registravimą.
Duomenų tvarkytojai	
Prieš pradedant asmens duomenų tvarkymo veiklą, duomenų valdytojai turi apibrėžti, dokumentuoti ir suderinti formalias gaires ir procedūras, taikomas duomenų tvarkytojams (pvz., rangovams ar	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

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.	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.
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.	
Duomenų valdytojas turi gauti iš duomenų tvarkytojo dokumentais pagrįstus įrodymus dėl atitikties keliamiems asmens duomenų saugumo reikalavimams ir įsipareigojimams.	
Asmens duomenų saugumo pažeidimai ir saugumo incidentai	
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.	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).
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.	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.
Veiklos tęstinumas	
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.	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“.
Asmens duomenų perdavimas	
Organizacijoje turi būti numatytos ir taikomos asmens duomenų perdavimo procedūros ir priemonės.	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.
Darbo santykiai	
Darbo sutartyje arba kitame dokumente turi būti aiškiai numatyti vaidmenys ir atsakomybės, bei	Siekiant užtikrinti asmens duomenų konfidencialumą pagal BDAR 32 straipsnį, organizacija turi užtikrinti, kad jos

įsipareigojimai susiję su organizacijoje taikoma asmens duomenų saugumo politika.	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.
Turi būti aiškiai numatytos atsakomybės bei įsipareigojimai pasibaigus darbo santykiams (pvz., konfidencialumo; asmens duomenų grąžinimo / sunaikinimo).	
Personalo konfidencialumas	
Vaidmenys ir atsakomybės turi būti aiškiai išdėstyti darbuotojui prieš pradedant vykdyti jam paskirtas funkcijas ir darbus.	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.
Personalo ugdymas	
Organizacijoje personalas turi suprasti savo atsakomybes, pagrindines asmens duomenų saugumo procedūras ir pagrindines kontrolės priemones, užtikrinant asmens duomenų saugumą.	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 duomenų apsaugos teisinius įsipareigojimus taip pat yra svarbios, ypač tiems asmenims, kurie dalyvauja didelės rizikos asmens duomenų tvarkymo procesuose.
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.	

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.	
Nuotolinis darbas	
Organizacija turi užtikrinti, kad nuotolinio darbo vietoje būtų laikomasi ir įgyvendinama organizacijos asmens duomenų saugumo politika.	Kai darbuotojai dirba nuotoliniu būdu (ne organizacijos patalpose), organizacija turi užtikrinti naudotojų asmens duomenų ir organizacijos administruojamų asmens duomenų tvarkymo saugumą.
Reagavimas į informacijos saugumo incidentus	
Personalas turi būti informuotas apie atsakomybę nedelsiant pranešti apie informacijos saugumo incidentus.	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.
Personalas turi žinoti pranešimo apie informacijos saugumo incidentų procedūrą ir kontaktinį asmenį, kuriam reikia pranešti apie įvykusį incidentą.	
Fizinė sauga	
Turi būti užtikrinama, kad organizacijoje prie tvarkomų asmens duomenų būtų galima fiziškai prieiti tik organizacijos nustatytu ir leistinu būdu.	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.
Fizinės saugos politika turi būti dokumentuota kaip asmens duomenų saugumo politikos dalis.	
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.	
Švaraus „stalo“, „ekrano“ politika	
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.	Fizinė apsauga yra ne mažiau svarbi, nei techninės saugumo priemonės, nes tiesioginės fizinės prieigos kontrolė prie IT infrastruktūros yra visos taikomos saugos strategijos pagrindas.
Dokumentus ir galinius įrenginius išdėstyti tvarkingai, naudoti kitas priemones (pvz., naudoti stalus su pertvara, nelaikyti ekranų atsuktų į klientus / langus, naudoti monitorių privatumo filtrus), kad sumažinti riziką, jog naudojamą informaciją (tvarkomus asmens duomenis) pamatys leidimo neturintys asmenys.	
Informacinėse sistemose turi būti sukonfigūruota užrakinimo po tam tikro laiko arba atjungimo funkcija (pvz., po 15 min. neaktyvumo automatiškai užsirakinantis kompiuterio ekranas).	
Prieigų kontrolė ir autentifikavimas	
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.	Prieigų kontrolė ir autentifikavimas yra esminiai saugos reikalavimai, siekiant apsisaugoti nuo neautorizuotos prieigos prie IT sistemos, kurioje yra tvarkomi asmens duomenys.

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.	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).
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.	
Prieigų kontrolės sistema turi turėti galimybę aptikti ir neleisti naudoti slaptažodžių, kurie neatitinka tam tikro kompleksiškumo lygio.	
Naudototojo slaptažodžiai turi būti saugomi naudojant kodavimo formą (angl. Hash form).	
Naudotojo galiniai įrenginiai (kompiuterinės darbo vietos)	
Naudotojams negalima turėti galimybės išjungti ar apeiti, išvengti IT sistemų saugos nustatymų.	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.
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.	
Naudotojams negalima turėti privilegijuotų teisių diegti, šalinti, administruoti neautorizuotos programinės įrangos.	
Kritiniai operacinės sistemos saugos atnaujinimai privalo būti diegiami reguliariai ir nedelsiant**.**	
Mobilieji, nešiojamieji įrenginiai	
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).	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
Mobilieji ir nešiojamieji įrenginiai, kuriais bus naudojamasi darbui su informacinėmis sistemomis, prieš naudojimąsi turi būti užregistruoti ir autorizuoti.	

Mobilieji, nešiojamieji įrenginiai turi būti pakankamo prieigos kontrolės procedūrų lygio, kaip ir kita naudojama įranga asmens duomenims tvarkyti.	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.
Tarnybinių stočių, duomenų bazių apsauga	
Duomenų bazės ir taikomųjų programų tarnybinės stotys turi būti sukonfigūruotos taip, kad veiktų naudodamos atskiras paskyras su priskirtomis žemiausiomis operacinės sistemos privilegijomis.	Informacinių sistemų pagrindas yra tarnybinės stotys ir duomenų bazės. Jų apsauga privalo būti sustiprinta, siekiant užtikrinti saugią darbo aplinką.
Duomenų bazėse ir taikomųjų programų tarnybinėse stotyse turi būti tvarkomi tik tie asmens duomenys, kurie yra reikalingi darbui, atitinkančiam duomenų tvarkymo tikslus.	
Techninių žurnalų įrašai ir stebėsena	
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.	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.
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.	
Tinklo ir komunikacijos sauga	
Kai prieiga prie naudojamų IT sistemų yra vykdoma internetu, privaloma naudoti šifruotą komunikacijos kanalą, t. y. kriptografinius protokolus (pvz., TLS/SSL).	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 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 [...]“.
Atsarginės kopijos	
Atsarginės kopijos ir duomenų atstatymo procedūros privalo būti apibrėžtos, dokumentuotos ir aiškiai susietos su vaidmenimis ir pareigomis.	Atsarginių kopijų sistema yra esminis veiksnys, užtikrinantis organizacijos darbo ir procesų atstatymą, įvykus duomenų praradimui ar sugadinimui. Duomenų kopijų darymo

Atsarginių kopijų laikmenoms privalo būti užtikrintas tinkamas fizinis aplinkos, patalpų saugos lygis, priklausantis nuo saugomų duomenų.	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“.
Atsarginių kopijų darymo procesas turi būti stebimas, siekiant užtikrinti užbaigtumą ir išsamumą.	
Pilnos atsarginės duomenų kopijos privalo būti daromos reguliariai. Rekomenduojamas atsarginių kopijų darymo dažnumas: - kasdien – pridedamoji kopija; - kas savaitę – pilna kopija.	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. 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.
Keitimų valdymas	
Organizacija turi užtikrinti, kad visi esminiai IT sistemų keitimai būtų stebimi ir registruojami konkretaus asmens (pvz., IT arba saugos specialisto).	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).
Programinės įrangos sauga	
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.).	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.
Specifiniai saugos reikalavimai, susiję su organizacijos veiklos ypatumais, turi būti apibrėžti pradiniuose programinės įrangos kūrimo etapuose.	
Turi būti laikomasi duomenų saugą užtikrinančių programavimo standartų ir gerosios praktikos.	
Po programinės įrangos kūrimo, testavimo ir verifikacijos, pradedant sistemos įdiegimą ir eksploataciją, turi būti laikomasi pagrindinių saugos reikalavimų.	
Duomenų naikinimas / šalinimas	
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.	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.
Popierinės ir nešiojamosios duomenų laikmenos (pvz., DVD laikmenos), kuriose buvo saugomi, kaupiami asmens duomenys, turi būti naikinamos tam skirtais	Pagal BDAR 5 straipsnį asmens duomenys neturi būti saugomi, kaupiami ilgiau, negu tai yra būtina tais tikslais,

smulkintuvais arba kitomis mechaninėmis priemonėmis.	kuriais asmens duomenys yra tvarkomi. Kai kuriais atvejais duomenų subjektai turi teisę reikalauti duomenis sunaikinti anksčiau, negu yra nustatytas duomenų saugojimo, kaupimo terminas. 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.

Vertinimą atliko:
Duomenų apsaugos pareigūnas

Tomas Gagys