DUOMENŲ VALDYTOJO

Vilniaus Fabijoniškių gimnazijos

saugumo priemonių ir rizikos vertinimo ataskaita

2025 m. rugpjūčio 26 d.

I. BENDROJI INFORMACIJA

Duomenų valdytojas Vilniaus Fabijoniškių gimnazija, kodas 190003851, buveinės adresas P. Žadeikos g. 2, Vilnius, 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 APIMTIS** (kokie asmens duomenys tvarkomu nurodytu tikslu)	**DUOMENŲ SUBJEKTŲ KATEGORIJOS**	**DUOMENŲ GAVĖJŲ KATEGORIJOS** (kam perduodami asmens duomenys)	**DUOMENŲ GAVIMO ŠALTINIS**
Personalo atrankos tikslu	Vardas, pavardė, gyvenamosios vietos adresas, gimimo data, telefono numeris, parašas, elektroninio pašto adresas, gyvenimo aprašymas, duomenys apie išsilavinimą ir kvalifikaciją, asmens tapatybės dokumento kopija (jeigu toks reikalavimas taikomas), 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, bei kita informaciją pateikta kandidato,	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 valdytojas), Informatikos ir ryšių departamentas (Įtariamųjų, kaltinamųjų ir nuteistųjų registro valdytojas), teisės aktų nustatyta tvarka asmens duomenys gali būti perduoti teisėsaugos,	Duomenų subjektas, Viešojo valdymo agentūra (vykdant konkursą per VATIS), Specialiųjų tyrimų tarnyba, Lietuvos Respublikos švietimo, mokslo ir sporto ministerija (Pedagogų registras), Informatikos ir ryšių departamentas (Įtariamųjų, kaltinamųjų ir nuteistųjų registras),

	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.), konkurso atveju – konkurso eigos metu užfiksuoto pokalbio garso įrašas.		teisminėms ar ikiteisminėms institucijoms dėl jų atliekamų tyrimų.	Buvęs arba esamas kandidato darbdavys (iš buvusio darbdavio prieš tai informavęs kandidatą, o iš esamo darbdavio – tik kandidato sutikimu).
Darbo sutarties vykdymo, įskaitant visų darbo sutartyje ar teisės aktuose numatytų teisių ir pareigų įgyvendinimo tikslu:	Vardas, pavardė, asmens kodas, pilietybė, 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, diplomo kopija, duomenys apie mokymus, kvalifikacijos atestatų kopijos, nepilnamečių vaikų gimimo liudijimų kopijos (kai asmuo siekia pasinaudoti teise į papildomą poilsio dieną), 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, kita informacija, kuri patvirtina atitiktį Lietuvos Respublikos švietimo įstatymo 48 str. reikalavimams (mokytojams).	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, Vilniaus miesto savivaldybės administracija, Nacionalinė švietimo agentūra, Valstybės duomenų agentūra, Informatikos ir ryšių departamentas prie Lietuvos Respublikos vidaus reikalų ministerijos, kvalifikacijos kėlimo įstaigos, BĮ „Skaitlis“ – duomenų tvarkytojas, El. dienynas – duomenų tvarkytojas. El. paštas – duomenų tvarkytojas, Teisės aktų nustatyta tvarka asmens duomenys gali būti perduoti teisėsaugos, teisminėms ar ikiteisminėms institucijoms dėl jų atliekamų tyrimų.	Duomenų subjektas; Pedagogų registras, Įtariamųjų, kaltinamųjų ir nuteistųjų registras (gaunama informacija apie teistumą ir atitiktį nepriekaištingos reputacijos reikalavimui), darbuotojas (darbuotojo vaikų ar kitų šeimos narių duomenys).
Darbuotojų saugos, sveikatos ir tinkamų darbo sąlygų užtikrinimo tikslu	Vardas, pavardė, informaciją, susijusi su darbuotojo sveikatos būkle (nuolatinės, periodinės asmens sveikatos patikros dokumentai).	Esami ir buvę darbuotojai	Sveikatos priežiūros įstaigos, teisės aktų nustatyta tvarka asmens duomenys gali būti perduoti teisėsaugos, teisminėms ar ikiteisminėms institucijoms dėl jų atliekamų tyrimų.	Duomenų subjektas, Sveikatos priežiūros įstaigos.
Vidaus administravimo tikslu:	Vardas, pavardė, asmens kodas, adresas, parašas, telefono numeris, elektroninio pašto adresas, pareigos.	Esami darbuotojai.	El. dienynas – duomenų tvarkytojas, El. paštas – duomenų tvarkytojas, teisės aktų nustatyta tvarka asmens duomenys gali būti perduoti teisėsaugos, teisminėms ar ikiteisminėms institucijoms dėl jų atliekamų tyrimų.	Duomenų subjektas.
Vilniečio kortelių išdavimo tikslu:	Vardas, pavardė, kortelės numeris, gimimo data, parašas, bilieto išdavimo ir grąžinimo data, pareigos.	Esami darbuotojai.	Vilniaus miesto savivaldybės administracija, SĮ „Susisiekimo paslaugos“,	Duomenų subjektas.

			teisės aktų nustatyta tvarka asmens duomenys gali būti perduoti teisėsaugos, teisminėms ar ikiteisminėms institucijoms dėl jų atliekamų tyrimų.	
Sveikinimo gimimo dienos proga tikslu:	Gimimo data.	Esami darbuotojai.		Duomenų subjektas.
Studentų praktikos atlikimo tikslu:	Vardas, pavardė, gimimo data, adresas, telefono numeris, el. pašto adresas, parašas, gyvenimo aprašymas, kita informacija pateikta kandidato.	Praktikantai, studentai, pageidaujantys atlikti praktiką.	Praktikos sutarties šalis. Teisės aktų nustatyta tvarka asmens duomenys gali būti perduoti teisėsaugos, teisminėms ar ikiteisminėms institucijoms dėl jų atliekamų tyrimų.	Duomenų subjektas.
Mokymo sutarties sudarymo, joje prisiimtų įsipareigojimų ir teisių tinkamo įgyvendinimo tikslu	Vardas, pavardė, gimimo data, asmens kodas (jeigu kodo nėra – gimimo data ir lytis), telefono numeris, el. pašto 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. Įstatyminių atstovų vardai, pavardės, telefono numeriai, el. pašto adresai.	Mokiniai, mokinio tėvai (kiti atstovai).	Lietuvos Respublikos švietimo, mokslo ir sporto ministerija, Nacionalinė švietimo agentūra, Vilniaus miesto savivaldybės administracija; BĮ „Skaitilis“ – duomenų tvarkytojas, El. dienynas – duomenų tvarkytojas, Vilniaus miesto savivaldybės visuomenės sveikatos biuras – duomenų tvarkytojas.	Duomenų subjektas, Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinė sistema (E. Sveikata).
Visos dienos mokyklos grupės organizavimo tikslu	mokinio vardas, pavardė, gimimo data, klasė; tėvų (kitų atstovų) vardas, pavardė, kontaktai, parašas.	Mokiniai, mokinio tėvai (kiti atstovai).	Teisės aktų nustatyta tvarka asmens duomenys gali būti perduoti teisėsaugos, teisminėms ar ikiteisminėms institucijoms dėl jų atliekamų tyrimų.	Duomenų subjektas
Pagalbos organizavimo ir koordinavimo procedūrų užtikrinimo tikslu:	Mokinio 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).	Vilniaus pedagoginė – psichologinė tarnyba, Valstybės vaiko teisių apsaugos ir įvaikinimo tarnyba.	Duomenų subjektas, Psichologinė – pedagoginė tarnyba, Valstybės vaiko teisių apsaugos ir įvaikinimo tarnyba, Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinė sistema (E. Sveikata).
Pagalbos teikimo užtikrinimo tikslu	Mokinio 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).	Vilniaus pedagoginė – psichologinė tarnyba, Valstybės vaiko teisių apsaugos ir įvaikinimo tarnyba.	Duomenų subjektas, Psichologinė – pedagoginė tarnyba, Valstybės vaiko teisių apsaugos ir įvaikinimo tarnyba, Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinė sistema (E. Sveikata).
Mokinių, turinčių	Mokinio vardas, pavardė, gimimo data, gyvenamoji vieta, sveikatos duomenys,	Mokiniai,	Vilniaus pedagoginė – psichologinė tarnyba,	Duomenų subjektas,

ugdymosi sunkumų ar švietimo pagalbos poreikių, nustatymo tikslu	ugdymosi ir elgesio ypatumai, pirminis vaiko specialiųjų ugdymosi poreikių, kylančių ugdymo(si) procese, įvertinimas. Tėvų (kitų atstovų) vardas, pavardė, kontaktai, parašas.	mokinio tėvai (kiti atstovai	Valstybės vaiko teisių apsaugos ir įvaikinimo tarnyba.	Psichologinė – pedagoginė tarnyba, Valstybės vaiko teisių apsaugos ir įvaikinimo tarnyba, Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinė sistema (E. Sveikata).
Socialinės paramos organizavimo tikslu	Vardas, pavardė, asmens kodas, gyvenamoji vieta, telefono numeris, el. pašto adresas, Tėvų (kitų atstovų) vardai, pavardės, parašas, asmens kodai, gyvenamoji vieta ir kontaktiniai telefono numeriai; kiti teisės aktuose nustatyti dokumentai (ar/ir jų kopijos).	Mokiniai, mokinio tėvai (kiti atstovai).	Vilniaus miesto savivaldybės administracija, Lietuvos Respublikos socialinės apsaugos ir darbo ministerija.	Duomenų subjektas.
Pažymų, pažymėjimų ir atestatų išdavimo ir jų apskaitos tikslu	Vardas, pavardė, asmens kodas, mokomieji dalykai, įvertinimai ir kiti duomenys nurodyti Pažymėjimų ir brandos atestatų išdavimo tvarkos apraše.	Mokiniai	Nacionalinė švietimo agentūra, Lietuvos Respublikos švietimo, mokslo ir sporto ministerija.	Duomenų subjektas, Mokinių registras, Diplomų, atestatų ir kvalifikacijos pažymėjimų registras.
Egzaminų ir pasiekimų patikrinimų vykdymo tikslu	Vardas, pavardė, klasė, mokomoji kalba, mokymo programa ir kiti asmens duomenys, numatyti teisės aktuose.	Mokiniai	Nacionalinė švietimo agentūra, Lietuvos Respublikos švietimo, mokslo ir sporto ministerija.	Duomenų subjektas, Mokinių registras, NECIS.
Nesimokančių vaikų ir mokyklos nelankančių mokinių apskaitos tikslu	Vardas, pavardė, asmens kodas arba gimimo data, gyvenamosios vietos adresas, lytis, klasė, kurioje mokosi, tačiau jos nelanko, praleistų pamokų per mėnesį skaičius ir priežastys, pokalbių duomenys: datos, kiti asmens duomenys, kurie numatyti NEMIS nuostatuose	Mokiniai, mokinio tėvai (kiti atstovai).	Nacionalinė švietimo agentūra, Lietuvos Respublikos švietimo, mokslo ir sporto ministerija.	Duomenų subjektas.
Mokinio pažymėjimo išdavimo tikslu	Vardas, pavardė, gimimo data, nuotrauka, parašas, ugdymosi programa, mokymosi forma ir būdas ir kiti duomenys numatyti Mokinio pažymėjimo išdavimo tvarkos apraše.	Mokiniai, mokinio tėvai (kiti atstovai).	Lietuvos Respublikos švietimo, mokslo ir sporto ministerija.	Duomenų subjektas.
Prašymų, skundų ar kitų kreipimųsi nagrinėjimo tikslu	Vardas, pavardė, el. pašto adresas, telefono numeris, parašas, bei kita prašyme ar kreipimesi pateikta informacija.	Asmenys, pateikę prašymą, skundą ar kitą kreipimąsi	Valstybės institucijoms, kurios pateikė prašymą ar kitą kreipimąsi, valstybės institucijoms, kompetentingoms nagrinėti kreipimąsi (kai duomenų valdytojas nekompetentingas nagrinėti), valstybės institucijoms, kurios kreipimesi nurodytos kaip papildomi adresatai ar su kuriomis susijęs kreipimasis, Teisės aktų nustatyta tvarka asmens duomenys gali būti perduoti teisėsaugos, teisminėms ar ikiteisminėms institucijoms dėl jų atliekamų tyrimų.	Duomenų subjektas.
El. dienyno tvarkymo tikslu	Mokinių: vardas, pavardė, lytis, mokinio pažymėjimo numeris, virtualios piniginės numeris, gimimo data, asmens kodas, adresas, telefono numeris, elektroninio pašto adresas, nuotrauka, specialieji ugdymo poreikiai, nemokamas maitinimas ir kt. Mokytojų: vardas, pavardė, mokomasis dalykas, auklėjamoji klasė, adresas,	Mokiniai, mokinio tėvai (kiti atstovai) darbuotojai.	Lietuvos Respublikos švietimo, mokslo ir sporto ministerija (Mokinių registras ir Pedagogų registras), El. dienynas – duomenų tvarkytojas.	Duomenų subjektas, Mokinių registras, Pedagogų registras.

	telefono numeris, elektroninio pašto adresas, asmens kodas, išsilavinimas ir kt. Mokinių tėvų (kitų atstovų): vardas, pavardė, adresas, telefono numeris, elektroninio pašto adresas, asmens kodas ir kt.			
Finansinės apskaitos tikslu	Vardas, pavardė, gimimo data arba asmens kodas, adresas, banko sąskaitos numeris, telefono numeris, el. pašto adresas, atliktų bankinių mokėjimų išrašai, individualios veiklos ar verslo liudijimo dokumento duomenys (prekių, darbų ar paslaugų tiekėjų bei gavėjų), mokėjimų ir įsiskolinimo informacija, kiti duomenys reikalingi finansinei apskaitai tvarkyti.	Mokiniai, mokinio tėvai (kiti atstovai), darbuotojai, prekių, darbų ar paslaugų teikėjai bei gavėjai (įskaitant nuomininkus ir kitaip bendradarbiaujančius asmenis) ir jų atstovai.	Vilniaus miesto savivaldybės administracija, BĮ „Skaitlis“ – duomenų tvarkytojas,	Duomenų subjektas, antstoliai, BĮ „Skaitlis“.
Skolų išieškojimo tikslu	Vardas, pavardė, gimimo data arba asmens kodas, adresas, telefono numeris, el. pašto adresas, skolos dydis (pradelsta suma), padengtos ir mokėtinos skolos dydis, atsiskaitymo informacija, kita informacija, susijusi su skola ir/ar skolininku, kuri reikalinga skolų išieškojimo tikslais.	Skolininkai	Vilniaus miesto savivaldybės administracijai, •BĮ „Skaitlis“ – duomenų tvakytojas,	Duomenų subjektas, BĮ „Skaitlis“.
Viešųjų pirkimų vykdymo, organizavimo ir sudarytų sutarčių vykdymo tikslu	Vardas, pavardė, asmens kodas, gimimo data, individualios veiklos pažymėjimo ar verslo liudijimo numeris, išsilavinimas, adresas, telefono numeris, elektroninio pašto adresas, banko sąskaitos numeris, parašas, asmens duomenys, kurių pateikimas numatytas pirkimo dokumentuose bei kiti asmens duomenys, kuriuos pateikia pats asmuo ir (arba), kuriuos tvarkyti įpareigoja teisės aktai.	Viešųjų pirkimų dalyvių ir jų atstovų (darbuotojų duomenys).	Viešųjų pirkimų tarnybai (CVP IS), UAB Ecocost – duomenų tvarkytojas.	Duomenų subjektas, viešųjų pirkimų dalyviai.
Bendruomenės ir visuomenės informavimo apie įstaigos veiklą ir bendruomenės narių pasiekimus tikslu	Vardas, pavardė, kūrybiniai darbai, informacija apie pasiekimus, dalyvavimą renginiuose, konkursuose, nuotrauka, vaizdo bei garso medžiaga, kurioje užfiksuotas duomenų subjektas.	Mokiniai, mokinio tėvai (kiti atstovai), darbuotojai,	Socialinių tinklų valdytojai, duomenų valdytojo interneto tinklapis, el. dienynas.	Duomenų subjektas.
Apklausų vykdymo tikslu	Vardas, pavardė, el. pašto adresas.	Mokiniai, mokinio tėvai (kiti atstovai), darbuotojai,	El. paštas – duomenų tvarkytojas, El. dienynas – duomenų tvarkytojas.	Duomenų subjektas.
Turto nuomos tikslu	Vardas, pavardė, asmens kodas, gyvenamoji vieta, telefono numeris, el. pašto adresas, banko sąskaitos numeris, įsiskolinimas, parašas.	Turto nuomininkai	Vilniaus miesto savivaldybės administracija (Active Vilnius), •BĮ „Skaitlis“ – duomenų tvarkytojas.	Duomenų subjektas.
Specializuotos ir (ar) kitos reikalingos pagalbos asmeniui suteikimo tikslu	Vardas, pavardė, telefono numeris, elektroninio pašto adresas, telefono numeris, el. pašto adresas.	Mokiniai, mokinio tėvai (kiti atstovai), darbuotojai,	Policija, specializuotos kompleksinės pagalbos centras, Valstybės vaiko teisių apsaugos ir įvaikinimo tarnyba prie Socialinės apsaugos ir darbo ministerijos,	Duomenų subjektas.

			Teisės aktų nustatyta tvarka asmens duomenys gali būti perduoti teisėsaugos, teisminėms ar ikiteisminėms institucijoms dėl jų atliekamų tyrimų.	
Visos dienos mokyklos grupės organizavimo tikslu	mokinio vardas, pavardė, gimimo data, klasė; tėvų (kitų atstovų) vardas, pavardė, kontaktai, parašas.	Mokiniai, mokinio tėvai (kiti atstovai).	Teisės aktų nustatyta tvarka asmens duomenys gali būti perduoti teisėsaugos, teisminėms ar ikiteisminėms institucijoms dėl jų atliekamų tyrimų.	Duomenų subjektas
Interneto tinklapio naudojimo užtikrinimo tikslu	Tvarkomi interneto svetainės lankytojų asmens duomenys, kurie gaunami slapukų pagalba.	Įstaigos interneto svetainės lankytojai	Teisės aktų nustatyta tvarka asmens duomenys gali būti perduoti teisėsaugos, teisminėms ar ikiteisminėms institucijoms dėl jų atliekamų tyrimų.	Duomenų subjektas.
Turto bei mokinių ir mokykloje dirbančių asmenų saugumo užtikrinimo tikslu	Stebėjimo kameros: vaizdo duomenys.	Mokiniai, mokinio tėvai (kiti atstovai), darbuotojai, asmenys, kurie patenka į vaizdo stebėjimo lauką, įstaigos lankytojai, registruojami svečių registracijos žurnale.	Teisės aktų nustatyta tvarka asmens duomenys gali būti perduoti teisėsaugos, teisminėms ar ikiteisminėms institucijoms dėl jų atliekamų tyrimų.	Duomenų subjektas. vaizdo stebėjimo kameros.
Mokinių registro tvarkymo tikslu:	Asmens duomenų sąrašas nustatytas Mokinių registro nuostatų 16 p.	Mokiniai, mokinio tėvai (kiti atstovai).	Lietuvos Respublikos švietimo, mokslo ir sporto ministerija, Nacionalinė švietimo agentūra.	Duomenų subjektas, Mokinių registras.
Pedagogų registro tvarkymo tikslu:	Asmens duomenų sąrašas nustatytas Pedagogų registro nuostatų 16 p.	Pedagoginiai darbuotojai, mokytojų padėjėjai.	Lietuvos Respublikos švietimo, mokslo ir sporto ministerija, Nacionalinė švietimo agentūra.	Duomenų subjektas, Pedagogų registras.

III. 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

IV. 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

V. 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 – 4 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.

VI. 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 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.
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).	

	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 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. 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.	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.
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 įsipareigojimai susiję su organizacijoje taikoma asmens duomenų saugumo politika. Turi būti aiškiai numatytos atsakomybės bei įsipareigojimai pasibaigus darbo santykiams (pvz., konfidencialumo; asmens duomenų grąžinimo / sunaikinimo).	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.
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. 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.	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.
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. Personalas turi žinoti pranešimo apie informacijos saugumo incidentų procedūrą ir kontaktinį asmenį, kuriam reikia pranešti apie įvykusį incidentą.	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.
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. 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 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.	
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

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.	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.
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 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.
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.	
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 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. 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.
Atsarginių kopijų laikmenoms privalo būti užtikrintas tinkamas fizinis aplinkos, patalpų saugos lygis, priklausantis nuo saugomų duomenų.	
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.	
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

<table>
<tr><td></td><td>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).</td></tr>
<tr><td colspan="2">Programinės įrangos sauga</td></tr>
<tr><td>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.).

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.</td><td>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.</td></tr>
<tr><td colspan="2">Duomenų naikinimas / šalinimas</td></tr>
<tr><td>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.

Popierinės ir nešiojamosios duomenų laikmenos (pvz., DVD laikmenos), kuriose buvo saugomi, kaupiami asmens duomenys, turi būti naikinamos tam skirtais smulkintuvais arba kitomis mechaninėmis priemonėmis.</td><td>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. 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.</td></tr>
</table>

Vertinimą atliko:
Duomenų apsaugos pareigūnas Tomas Gagys