TVIRTINU:
Biudžetinės įstaigos Vilniaus miesto
Nakvynės namų direktorius
Edvardas Jablonskis

(parašas)
2018 m. spalio 31 d.

BIUDŽETINĖS ĮSTAIGOS VILNIAUS MIESTO NAKVYNĖS NAMŲ ASMENS DUOMENŲ TVARKYMO TAISYKLĖS

1. BENDROSIOS NUOSTATOS

1.1. Šių asmens duomenų tvarkymo taisyklių (toliau – Taisyklės) tikslai yra:

1.1.1. nustatyti asmens duomenų rinkimo, naudojimo ir saugojimo Biudžetinėje įstaigoje Vilniaus miesto nakvynės namuose (toliau – Įstaiga) bendruosius principus ir taisykles;

1.1.2. įgyvendinti Darbo kodekso reikalavimus priimti ir įprastais darbovietėje būdais paskelbti darbuotojų stebėsenos ir kontrolės darbo vietoje tvarką;

1.1.3. įgyvendinti Bendrojo duomenų apsaugos reglamento įtvirtintus realios asmens duomenų apsaugos ir atskaitomybės principus;

1.1.4. palengvinti tinkamą Bendrojo duomenų apsaugos reglamento, Asmens duomenų apsaugos įstatymo, Darbo kodekso, kitų Europos Sąjungos ir Lietuvos Respublikos teisės aktų asmens duomenų apsaugos srityje (toliau – ADA teisės aktai) reikalavimų įgyvendinimą;

1.1.5. sukurti tarpusavio supratimą bei teisinį aiškumą tarp Įstaigos ir jos darbuotojų dėl veiksmų, kuriais Įstaiga siekia apsaugoti savo darbuotojų ir kitų asmenų asmens duomenis;

1.1.6. padėti Įstaigos darbuotojams įgyvendinti ADA teisės aktų reikalavimus.

1.2. Jei šiose Taisyklėse ir jos prieduose aiškiai nenurodyta kitaip, pirmąja didžiąja raide rašomos sąvokos turi reikšmes, nurodytas žemiau:

ADA teisės aktai	Visi galiojantys tarptautiniai, Europos Sąjungos ir Lietuvos Respublikos teisės aktai, administraciniai sprendimai, iš teismų praktikos kylantys reikalavimai, nustatantys taisykles ir/ar reikalavimus asmens duomenų tvarkymui, įskaitant bet neapsiribojant Bendruoju duomenų apsaugos reglamentu, Darbo kodeksu, Asmens duomenų teisinės apsaugos įstatymu, Elektroninių ryšių įstatymu.
Asmuo	Žmogus (fizinis asmuo), kurio asmens duomenys renkami, naudojami ir saugojami Įstaigoje ir kurio tapatybę galima nustatyti, įskaitant bet neapsiribojant Darbuotojais. ADA teisės aktuose apibrėžiamas kaip duomenų subjektas.
Duomenys	Bet kokia informacija, susijusi su Asmeniu, renkama, naudojama ar saugoma Įstaigoje. ADA teisės aktuose apibrėžiama kaip asmens duomenys.
Asmens prašymas	Bet kuris iš žemiau nurodytų: (a) prašymas susipažinti su Duomenimis apie Asmenį; (b) prašymas ištaisyti netikslius Asmens Duomenis; (c) prašymas ištrinti Duomenis apie Asmenį; (d) prašymas apriboti Duomenų apie Asmenį naudojimą ar trynimą; (e) prašymas išeksportuoti Duomenis apie Asmenį; (f) prieštaravimas dėl Duomenų apie Asmenį rinkimo, naudojimo ir saugojimo Įstaigoje;

(g) prieštaravimas dėl bet kokio automatinio sprendimo priėmimo dėl Asmens ar Asmens profiliavimo Įstaigoje;
(h) bet kuris kitas prašymas ir (arba) skundas dėl bet kokio klausimo, susijusio su Duomenų apsauga Įstaigoje.

Asmenų prašymų valdymas — Procesas, kuriuo metu analizuojami, tiriami Įstaigoje gauti Asmens prašymai ir į juos atsakoma.

Įstaiga — Biudžetinė įstaiga Vilniaus miesto nakvynės namai, atsakinga už Duomenų rinkimą, naudojimą ir saugojimą, ADA teisės aktų laikymąsi. ADA teisės aktuose apibrėžiama kaip duomenų valdytojas.

Darbuotojas — Bet kuris Įstaigos darbuotojas, praktikantas, savanoris arba komandiruotas į Įstaigą darbuotojas, turintis tiesioginę ar netiesioginę prieigą prie Duomenų.

Duomenų apsaugos pareigūnas — Įstaigos skiriamas darbuotojas arba išorės paslaugų teikėjas (fizinis arba juridinis asmuo), padedantys Įstaigai užtikrinti teisinę atitiktį ADA teisės aktams.

Duomenų tvarkymas — Duomenų rinkimas, naudojimas, saugojimas, persiuntimas, naikinimas ar bet kuris kitas konkretus su Duomenimis atliekamas veiksmas.

IKT — Informacinės ir komunikacinės technologijos, kurias Įstaiga suteikia Darbuotojams arba kurias Darbuotojai naudoja siekdami atlikti savo pareigas Įstaigoje, įskaitant, bet neapsiribojant, kompiuteriais, planšetiniais kompiuteriais, išmaniaisiais telefonais, USB įrenginiais ar kitomis duomenų laikmenomis, nutolusiomis duomenų saugyklomis, interneto svetainėmis bei kita programine įranga.

Duomenų saugumo pažeidimas — Bet kuris iš toliau nurodytų įvykių:

(a) Įstaigos IKT, dokumentų ir (arba) kitų priemonių, kuriuose yra Duomenų praradimas, vagystė arba nesuplanuotas sunaikinimas;
(b) atsitiktinis ar tyčinis Duomenų siuntimas, įkėlimas ar dalinimasis su trečiaisiais asmenimis, neturinčiai teisės jų gauti;
(c) trečiųjų asmenų neteisėta prieiga prie Įstaigos IKT, dokumentų ir (ar) kitų priemonių, kuriose yra Duomenų;
(d) kenkėjiškos atakos prieš Įstaigos IKT ir (ar) kitas priemones, kuriose yra Duomenų;
(e) klaidos, susijusios su kuriamomis, naudojamomis ir konfigūruojamomis IKT ir (ar) kitomis priemonėmis, kurios gali kelti pavojų Duomenų saugumui;
(f) bet kokie kiti saugumo pažeidimai, lemiantys atsitiktinį ar neteisėtą Duomenų sunaikinimą, praradimą, nutekėjimą, pakeitimą, neleistiną atskleidimą arba prieigos prie Įstaigai perduodamų, saugojamų ar kitaip renkamų, naudojamų ar saugojamų Duomenų suteikimą.

Duomenų saugumo pažeidimo valdymas — Procesas, kurio metu Įstaigoje analizuojami, registruojami Duomenų saugumo pažeidimai ir, jei reikia, teikiami pranešimai Inspekcijai ar Asmenims, kurių Duomenys buvo paveikti.

Duomenų tvarkymo veiklos įrašai	Elektroninis dokumentas, išsamiai apibūdinantis Įstaigoje renkamus, naudojamus ir saugomus Duomenis.
EEE	Europos Ekonominė Erdvė (visos ES valstybės narės bei Islandija, Norvegija, Lichtenšteinas).
Inspekcija	Valstybinė duomenų apsaugos inspekcija.
Inspekcijos paklausimas	Bet kuris laiškas, pranešimas, užklausa ar kitas dokumentas, kurį pateikia Valstybinė duomenų apsaugos inspekcija, ir kuris yra adresuotas Įstaigai.
Inspekcijos paklausimų valdymas	Procesas, kurio metu nagrinėjami Inspekcijos paklausimai, renkama atsakymui reikalingai informacija ir Inspekcijai pateikiamas atsakymas.
Ypatingi duomenys	ADA teisės aktuose nurodyti duomenys, kurių tvarkymui keliami padidinti reikalavimai (pvz.: duomenys, atskleidžiantys rasinę ar etninę kilmę, politines pažiūras, religinius ar filosofinius įsitikinimus ar narystę profesinėse sąjungose, sveikatos duomenys arba duomenys apie fizinio asmens lytinį gyvenimą ir lytinę orientaciją, genetiniai, biometriniai identifikatoriai, duomenys apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas).
Paslaugų teikėjas	Konkretus paslaugos teikėjas ar kitas išorės juridinis ar fizinis asmuo, kuris turi prieigą prie Įstaigos Duomenų ir juos tvarko pagal Įstaigos nurodymus. ADA teisės aktuose apibrėžiamas kaip duomenų tvarkytojas.
Taisyklės	Šios atitikties asmens duomenų apsaugai Taisyklės.
Tretieji asmenys	Visi fiziniai arba juridiniai asmenys, išskyrus Darbuotojus.

1.3. Kitos šiose Taisyklėse neapibrėžtos sąvokos suprantamos taip, kaip jos apibrėžtos ADA teisės aktuose.

1.4. Taisyklės taikomos visiems Įstaigos Darbuotojams. Darbuotojai su šiomis Taisyklėmis yra supažindinami galiojančių Darbo tvarkos taisyklių nustatyta tvarka.

2. DUOMENŲ TVARKYMO PRINCIPAI

2.1. Įstaiga tvarkydama Duomenis vadovaujasi principais, kad asmens duomenys turi būti:

2.1.1. tvarkomi teisėtai, sąžiningai ir skaidriai;

2.1.2. renkami nustatytais, aiškiai apibrėžtais bei teisėtais tikslais ir toliau netvarkomi su tais tikslais nesuderinamu būdu;

2.1.3. adekvatūs, tokie, kurių reikia siekiant tikslų, dėl kurių jie tvarkomi;

2.1.4. tikslūs ir prireikus atnaujinami;

2.1.5. laikomi tokia forma, kad duomenų subjektų tapatybę būtų galima nustatyti ne ilgiau, nei tai yra būtina tais tikslais, kuriais asmens duomenys yra tvarkomi;

2.1.6. tvarkomi tokiu būdu, kad taikant atitinkamas technines ar organizacines priemones būtų užtikrintas tinkamas asmens duomenų saugumas.

2.2. Duomenys gali būti teisėtai tvarkomi Įstaigoje tik esant bent vienam iš šių pagrindų:

2.2.1. Sutartis: Duomenys reikalingi siekiant sudaryti ar vykdyti darbo, civilinę ar kitokią sutartį su Asmeniu, įskaitant bet neapsiribojant sutarties sąlygų vykdymą, teisės aktų atitinkamai sutarties rūšiai numatytų šalių teisių ir pareigų vykdymą ir iš sutarties esmės kylančių šalių įsipareigojimų vykdymą;

2.2.2. Teisinė prievolė: Įstaiga teisės aktais yra įpareigota tvarkyti Duomenis mokesčių, darbo, socialinės apsaugos ir kitose srityse;

2.2.3. Užduočių, vykdomų viešojo intereso labui, arba pavestų viešosios valdžios funkcijų vykdymas: Duomenys yra reikalingi socialinių paslaugų, teikiamų valstybės ir/ar vietos savivaldos pavedimu, teikimui ir/ar administravimui, jei Asmens interesai konkrečių aplinkybių kontekste nėra svarbesni.

2.2.4. Sutikimas: Asmuo galėjo laisvai pasirinkti, ar duoti sutikimą dėl jo Duomenų tvarkymo, be jokių neigiamų pasekmių Asmeniui ir tokį sutikimą davė.

2.3. Ypatingi duomenys gali būti teisėtai tvarkomi Įstaigoje:

2.3.1. Darbuotojų ypatingi asmens duomenys, įskaitant sveikatos duomenis ir narystės profesinėse sąjungose duomenis, – tik ta apimtimi, kiek yra būtina siekiant įgyvendinti teises ar pareigas darbo ir socialinės apsaugos teisės srityse arba pagal kolektyvines sutartis;

2.3.2. Socialinių paslaugų gavėjų sveikatos duomenys, taip pat duomenys apie jų rasinę ar etninę kilmę, religinius ar filosofinius įsitikinimus, lytinį gyvenimą ir lytinę orientaciją – kiek reikalinga teikiant socialines paslaugas;

2.3.3. Kitų asmenų ypatingi duomenys – tik ta apimtimi, kiek Asmuo galėjo laisvai pasirinkti, ar duoti sutikimą tvarkyti Ypatingus duomenis, be jokių neigiamų pasekmių Asmeniui bei davė tokį sutikimą raštu arba elektronine forma.

2.4. Duomenys apie Asmenų teistumą gali būti tvarkomi tik šiais atvejais:

2.4.1. Darbuotojų, dirbančių su vaikais;

2.4.2. prireikus tokių duomenų viešajame pirkime ar projekto konkurse, tačiau tokie duomenys turi būti (a) saugomi atskirai nuo kitų duomenų ir su jais nejungiami ir (b) sunaikinti pasibaigus viešojo pirkimo ar projekto konkurso procedūrai, jei specialūs teisės aktai nenumato specialios Įstaigos pareigos tam tikrą laiką saugoti tokius Duomenis;

2.4.3. kitais atvejais, kai tai numato specialūs teisės aktai – tik ta apimtimi, kiek tai reikalinga atitinkamų teisės aktų įgyvendinimui, ir tik tiek laiko, kiek reikalaujama pagal teisės aktus.

3. DUOMENŲ TVARKYMO VEIKLOS ĮRAŠAI

3.1. Siekdama užtikrinti Duomenų tvarkymo teisėtumą, Įstaiga sudaro Duomenų tvarkymo veiklos įrašus, kuriuose nurodoma:

3.1.1. Asmenų kategorijos;

3.1.2. Duomenų kategorijos pagal kiekvieną Asmenų kategoriją;

3.1.3. Duomenų tvarkymo tikslai ir teisinis pagrindas (Bendrojo duomenų apsaugos reglamento straipsnio nuorodą) pagal kiekvieną Duomenų kategoriją;

3.1.4. Duomenų gavėjų kategorijos kiekvienai Asmenų kategorijai pagal Duomenų perdavimo tikslus bei teisinį pagrindą;

3.1.5. Jei tokių yra, duomenų gavėjai, veikiantys ne EEE šalyse, ir jiems taikomos duomenų apsaugos užtikrinimo priemonės;

3.1.6. Duomenų saugojimo terminai.

3.2. Darbuotojai supažindinami su Duomenų tvarkymo veiklos įrašais Darbo tvarkos taisyklių nustatyta tvarka.

4. BENDROSIOS DARBUOTOJŲ PAREIGOS DUOMENŲ APSAUGOS SRITYJE

4.1. Kiekvienas Darbuotojas privalo:

4.1.1. tvarkydamas Duomenis, įsitikinti, kad yra laikomasi visų reikalavimų, numatytų Taisyklėse;

4.1.2. tvarkyti Duomenis tik tam, kad atliktų savo darbo funkcijas, ir tik ta apimtimi, kiek tai reikalinga jų vykdymui;

4.1.3. visais atvejais identifikuoti Duomenis, kurie yra tvarkomi Darbuotojo veikloje bei žinoti, kad veiklai, susijusiai su Duomenimis, yra taikomi šių Taisyklių ir ADA teisės aktų reikalavimai;

4.1.4. visais atvejais įsitikinti, kad tvarkoma Duomenų kategorija yra įtraukta į Duomenų tvarkymo veiklos įrašus, o tvarkymo tikslas atitinka bent vieną iš Duomenų tvarkymo veiklos įrašuose nurodytų tikslų; apie poreikį tvarkyti naujas Duomenų kategorijas ir (ar) naujais tikslais informuoti Duomenų apsaugos pareigūną;

4.1.5. visais atvejais prieš perduodant Duomenis Tretiesiems asmenims įsitikinti, kad tokia Duomenų gavėjų kategorija yra įtraukta į Duomenų tvarkymo veiklos įrašus, o jei ketinama Duomenis perduoti už EEE ribų – kad atitinkamas Duomenų gavėjas yra įtrauktas į Duomenų tvarkymo veiklos įrašus; apie poreikį perduoti Duomenis Duomenų tvarkymo veiklos įrašuose nenurodytai Duomenų gavėjų kategorijai arba už EEE ribų veikiančiam Trečiajam asmeniui, nenurodytam Duomenų tvarkymo veiklos įrašuose, informuoti Duomenų apsaugos pareigūną;

4.1.6. įsitikinti, kad kiekvienas Asmuo, su kuriuo jie susiduria pirmą sykį Įstaigoje, buvo informuotas apie jo Duomenų tvarkymą, o Duomenų tvarkymo veiklos įrašuose numatytais atvejais yra davęs sutikimą Duomenų tvarkymui; jei Asmuo nebuvo informuotas apie jo Duomenų tvarkymą ir(ar) nebuvo gautas jo sutikimas, įteikti informacinį pranešimą ir (ar) paprašyti Asmens sutikimo pagal atitinkamai Asmenų kategorijai pritaikytą formą; jei konkrečiu atveju nėra tinkama nei viena iš Įstaigos naudojamų tipinių informacinių pranešimų ar sutikimų formų, Darbuotojas apie tai turi nedelsiant informuoti Duomenų apsaugos pareigūną;

4.1.7. atsižvelgiant į atliekamų darbo funkcijų pobūdį imtis protingų pastangų, kad užtikrintų, jog visi Įstaigos valdomi Duomenys būtų tikslūs ir prireikus atnaujinami;

4.1.8. tvarkydami Duomenis, elgtis rūpestingai ir atsargiai, turėdami omenyje tai, kad Darbuotojo veiksmai, susiję su Duomenimis, kelia pavojų Įstaigai ir Asmenims;

4.1.9. įgyvendinti ir naudoti technines ir organizacines Duomenų apsaugos priemones, užtikrinančias Duomenų apsaugą nuo neleistinos prieigos, neteisėto rinkimo, naudojimo ir saugojimo, netyčinio praradimo, sunaikinimo ar sugadinimo, kaip tai nustatyta šiose Taisyklėse, darbo tvarkos taisyklėse ir kituose Įstaigos dokumentuose;

4.1.10. neatskleisti informacijos apie Įstaigos taikomas technines ir organizacines Duomenų apsaugos priemones, įskaitant bet neapsiribojant Įstaigos vidaus dokumentais, jokiems Tretiesiems asmenims, prieš tai neįsitikinus jų teise gauti tokią informaciją;

4.1.11. nesaugoti asmens duomenų jokiose Darbuotojui priklausančiose asmeninėse atmintinėse, kompiuterinėje ar programinėje įrangoje (internetinėse duomenų saugyklse, atmintinėse, kompiuteriuose, telefonuose ir pan.), nebent konkrečiu atveju Įstaiga leistų Darbuotojui naudoti konkrečias asmenines priemones darbo funkcijų vykdymui;

4.1.12. neišnešti iš Įstaigos dokumentų, kuriuose yra užfiksuoti duomenys apie socialinių paslaugų gavėjus, nebent tai yra absoliučiai būtina teikiant paslaugas;

4.1.13. nepalikti Įstaigos dokumentų ant stalo ir kitose lankytojams prieinamose vietose;

4.1.14. kai Darbuotojui leidžiama naudoti asmenines atmintines ir/ar kompiuterinę ar programinę įrangą darbo funkcijoms vykdyti, pasibaigus darbo santykiams perduoti visus Darbuotojo bet kokiose informacijos rinkmenose (asmeninėse internetinėse saugyklose, atmintinėse, asmeniniame kompiuteryje, telefone ir pan.) esančius Duomenis Įstaigai ir sunaikinti visas tokios informacijos kopijas;

4.1.15. kreiptis į Duomenų apsaugos pareigūną ir gauti jo konsultaciją:

4.1.15.1. ketinant Įstaigoje pasitelkti naują Paslaugų teikėją;

4.1.15.2. ketinant Įstaigoje sukurti, diegti ar naudoti kokybiškai naujas IKT ir (ar) kitus metodus Duomenų tvarkymui;

4.1.15.3. esant bet kokiems netikslumams, abejonėms ar klausimams, susijusiems su Taisyklių arba ADA teisės aktų taikymu, aiškinimu, pažeidimu ar atitikimu Taisyklėms arba ADA teisės aktams.

4.1.16. su Asmenų prašymais elgtis rūpestingai ir atidžiai; gavę bet kokį Asmens prašymą, susijusį su Asmens duomenimis nedelsdami, ne vėliau kaip per 1 (vieną) darbo dieną nuo Asmens prašymo gavimo:

4.1.17. gavus kitokį Asmens prašymą – pranešti apie tai Duomenų apsaugos pareigūnui;

4.1.18. nedelsiant, bet ne vėliau kaip per 12 (dvylika) valandų, sužinoję apie Duomenų saugumo pažeidimą Įstaigoje:

4.1.18.1. informuoti Duomenų apsaugos pareigūną apie Duomenų saugumo pažeidimą;

4.1.18.2. pagal savo kompetenciją imtis pagrįstų veiksmų, kad Duomenų saugumo pažeidimas būtų sustabdytas;

4.1.18.3. pagal savo kompetenciją imtis pagrįstų veiksmų, kad Duomenų saugumo pažeidimas nepasikartotų.

4.1.19. bendradarbiauti su Duomenų apsaugos pareigūnu, kitais Darbuotojais ir (ar) Paslaugų teikėjais atliekant Duomenų saugumo pažeidimo valdymą, Asmenų prašymų valdymą, Inspekcijos paklausimų valdymą ir kitas Įstaigos nustatytas su Duomenų tvarkymu susijusias procedūras;

4.1.20. per trumpiausius galimus terminus pateikti Duomenų apsaugos pareigūnui bet kokią prašomą informaciją;

4.1.21. vykdyti Duomenų apsaugos pareigūno nurodymus dėl Duomenų tvarkymo.

4.2. Nė vienam Darbuotojui neturi būti suteikta prieiga prie Duomenų, jei šie Duomenys nėra reikalingi jų darbo funkcijoms atlikti.

5. ASMENŲ TEISIŲ ĮGYVENDINIMAS

5.1. Darbuotojas, gavęs Asmens prašymą, susijusį su Asmens duomenimis nedelsdamas, ne vėliau kaip per 1 (vieną) darbo dieną nuo Asmens prašymo gavimo dienos kreipiasi į Duomenų apsaugos pareigūną.

5.2. Duomenų apsaugos pareigūnas atlieka gautų Asmenų prašymų valdymą vadovaudamasis šiomis Taisyklėmis ir ADA teisės aktais:

5.2.1. peržiūri prašymą;

5.2.2. nustato prašymą pateikusio Asmens tapatybę;

5.2.3. surenka prašymo nagrinėjimui reikalingą informaciją;

5.2.4. įvertina prašymo teisinį pagrįstumą;

5.2.5. paruošia ir pateikia Asmeniui atsakymą į prašymą; ir

5.2.6. esant reikalui duoda reikiamus pavedimus Darbuotojams dėl prašymą pateikusio Asmens Duomenų tolesnio tvarkymo.

5.3. Prašymą pateikusio Asmens tapatybė nustatoma:

5.3.1. kai prašymas susijęs su konkrečių socialinių paslaugų teikimu:

5.3.1.1. pateikiant prašymą fiziškai – pateikiant asmens dokumentą;

5.3.1.2. siunčiant prašymą paštu ar per kurjerį – pateikiant notariškai patvirtintą asmens dokumento nuorašą;

5.3.1.3.siunčiant prašymą elektroniniu paštu – pasirašant prašymą kvalifikuotu elektroniniu parašu.

5.3.2. kitais atvejais – iš kontekstinių prašymo duomenų (pareiškėjo elektroninio pašto adreso, kitų Asmens pateiktų jo identifikacinių duomenų).

5.4. Jei Duomenų apsaugos pareigūnas nustato, kad reikalinga papildoma informacija iš Darbuotojų, Trečiųjų asmenų ir (ar) Asmens, pateikusio Asmens prašymą, Duomenų apsaugos pareigūnas prašo pateikti šią informaciją, o Darbuotojai per protingą terminą Duomenų apsaugos pareigūnui pateikia bet kurią informaciją, kurios yra prašoma.

5.5. Duomenų apsaugos pareigūnas užtikrina, kad:

5.5.1. į Asmens prašymą būtų atsakyta per 1 (vieną) mėnesį nuo jo gavimo dienos; jei Asmens prašymų, pateiktų to paties Asmens, sudėtingumas ar skaičius yra didelis, Duomenų apsaugos pareigūnas turi teisę pratęsti terminą atsakymui pateikti iki 2 (dviejų) mėnesių informuodamas apie tai Asmenį ir nurodydamas termino pratęsimo priežastis;

5.5.2. Asmeniui būtų pateikta tik ta informacija, kuri yra susijusi su juo;

5.5.3. Asmeniui būtų pateikiama tik tiek informacijos, kiek reikalauja ADA teisės aktai;

5.5.4. ADA teisės aktų numatytais atvejais, kai Asmuo neturi teisės pasinaudoti savo kaip duomenų subjekto teise, Asmens prašymas nebūtų tenkinamas;

5.5.5. Asmenims nebūtų atskleista jokia Įstaigos konfidenciali informacija;

5.6. Asmens prašymą tenkinti atsisakoma, kai:

5.6.1. Asmens prašymas nesusijęs su ADA teisės aktų numatytomis teisėmis;

5.6.2. Asmens prašymas susijęs su informacija, kuri nėra Duomenys;

5.6.3. Asmens prašymas susijęs su informacija apie kitą Asmenį;

5.6.4. Asmuo neturi teisės pasinaudoti atitinkamomis duomenų subjekto teisėmis pagal ADA teisės aktų nustatytus reikalavimus bei išimtis;

5.6.5. Asmens prašymas yra akivaizdžiai neproporcingas, įskaitant bet neapsiribojant šiais atvejais:

5.6.5.1. Asmens prašymas yra pasikartojantis – tas pats Asmuo jau yra pateikęs tokį patį Prašymą per 1 (vienus) metus iki Prašymo gavimo;

5.6.5.2. Asmens prašymas susijęs su dideliu kiekiu pasikartojančių Duomenų;

5.6.5.3. aplinkybės rodo, kad vienintelis Asmens prašymo tikslas yra sutrikdyti Įstaigos veiklą.

5.7. Duomenų apsaugos pareigūnas į Asmens prašymą atsako elektroninėmis priemonėmis glausta ir Asmeniui suprantama forma, vartodamas aiškią ir suprantamą kalbą, išskyrus atvejus, kai Asmuo prašo žodinio atsakymo ar ne elektroninio atsakymo raštu.

5.8. Jei Asmens prašymą tenkinti atsisakoma visiškai arba iš dalies, atsakyme turi būti nurodomos atsisakymo priežastys ir informuojama apie galimybę pateikti skundą Inspekcijai ir (ar) imtis teisminės gynybos priemonių.

5.9. Jei Asmens prašymas tenkinamas, Duomenų apsaugos pareigūnas koordinuoja ir planuoja Asmens prašymo įgyvendinimą Įstaigoje, teikia nurodymus bei konsultacijas Darbuotojams ir Paslaugų teikėjams, kurie turi dalyvauti Asmens prašymo įgyvendinime.

6. PASLAUGŲ TEIKĖJAI

6.1. Duomenų apsaugos pareigūnas, sužinojęs apie ketinimą pasitelkti naują Paslaugų teikėją, turi:

6.1.1. patikrinti ir įsitikinti, kad Paslaugų teikėjas imasi tinkamų techninių ir organizacinių duomenų apsaugos priemonių ir atitinka kitus ADA teisės aktų reikalavimus;

6.1.2. pasirūpinti, kad Įstaiga prieš dalindamasi Duomenimis su Paslaugų teikėju sudarytų su juo Duomenų tvarkymo sutartį (arba įtrauktų atitinkamas nuostatas į esamas sutartis, įskaitant paslaugų teikimo sąlygas); (sutarties forma pridedama kaip Priedas Nr. 1).

6.2. Jei Paslaugų teikėjas pateikia Įstaigai savo Duomenų tvarkymo sutarties formą, įskaitant paslaugų teikimo sąlygas, Duomenų apsaugos pareigūnas, prieš Įstaigai sudarant tokią sutartį, turi įsitikinti, kad ji atitinka ADA teisės aktų nustatytus reikalavimus.

7. DARBUOTOJŲ STEBĖSENOS IR KONTROLĖS DARBO VIETOJE TVARKA

7.1. Vaizdo stebėjimo duomenys gali būti renkami išskirtinai siekiant apsaugoti Darbdavio turtą nuo vagysčių ir panašių nusikaltimo požymių turinčių veikų arba siekiant apsaugoti žmonių sveikatą ar gyvybę laikantis šių taisyklių:

7.1.1. Vaizdo stebėjimo kameros ir jų stebima teritorija paženklinama aiškiai matomais ir suprantamais ženklais, juose turi būti nuoroda, kur galima susipažinti su stebėjimo duomenimis ir jų tvarkymo sąlygomis;

7.1.2. Vaizdo stebėjimas organizuojamas Įstaigai patvirtinus atskirą vaizdo stebėjimo aprašą (-us) ir pasikonsultavus su Valstybine asmens duomenų apsaugos inspekcija; Toks aprašas (-ai) yra skelbiami viešai Įstaigos interneto svetainėje;

7.1.3. Vaizdo stebėjimo duomenys yra prieinami tik specialiai Darbdavio paskirtam darbuotojui (-ams) arba Įstaigai saugos paslaugas teikiančiai įmonei; nustatęs įtariamą vagystę ar panašią nusikaltimo požymių turinčią veiką, už vaizdo stebėjimą atsakingas asmuo perduoda atitinkamą vaizdo įrašo fragmentą Įstaigos vadovui ar kitam jo paskirtam Darbuotojui; kai įtariamas Darbuotojas, jis yra supažindinamas su atitinkamu vaizdo įrašo fragmentu ir jo paprašoma pateikti paaiškinimus, kitais atvejais Įstaigos vadovo sprendimu atitinkamas vaizdo įrašo fragmentas yra perduodamas teisėsaugos institucijoms;

7.1.4. Vaizdo stebėjimo duomenys saugomi keturiolika kalendorinių dienų, išskyrus atvejus, kai jų prireikia siekiant pareikšti reikalavimus ar gintis nuo reikalavimų, pareikštų teisme, baudžiamojo proceso, administracinėje ar kitokioje teisinėje procedūroje;

7.1.5. Vaizdo stebėjimo duomenys gali būti panaudoti kaip įrodymas nustatant Darbuotojo darbo pareigų pažeidimus tik ta apimtimi, kiek tokie pažeidimai turi vagystės ar panašių nusikalstamų veikų požymių arba yra susiję su pavojumi žmonių sveikatai ar gyvybei.

7.2. Įstaiga, siekdama valdyti savo IKT infrastruktūrą bei užtikrinti jos saugumą, suteikia nuotolinio prisijungimą prie savo IKT (kompiuterių, planšečių, telefonų ir pan.) jų techninę priežiūrą vykdantiems Darbuotojams arba išoriniams paslaugų teikėjams – programinės įrangos diegimui, atnaujinimui, gedimų šalinimui ir panašios techninės pagalbos darbams. Nors šiuo atveju nėra renkama įrenginyje saugoma informacija, teikiant techninę priežiūrą gali būti nustatyti Darbuotojo darbo pareigų pažeidimai (pvz., neteisėtai instaliuota programinė įranga) ir tokia informacija gali būti panaudota kaip įrodymas nustatant Darbuotojo darbo pareigų pažeidimus.

7.3. Darbuotojo susirašinėjimo su kitais Darbuotojais ir Trečiaisiais asmenimis (klientais, tiekėjais ir pan.) naudojant Įstaigos elektroninio pašto, socialinių tinklų ar panašią paskyrą duomenys yra saugomi Įstaigos ir (ar) Įstaigos pasitelkto atitinkamų elektroninių paslaugų tiekėjo informacinėse sistemose siekiant užtikrinti Įstaigos teisėtus interesus – sudarytų sutarčių vykdymą, ypač atsižvelgiant į tai, kad toks susirašinėjimas laikomas sutarčių dalimi, informacijos pateikimą kontrahentams, efektyvų darbo organizavimą, taip pat ir paties darbuotojo darbo palengvinimui. Šie Duomenys tvarkomi laikantis tokių taisyklių:

7.3.1. Įstaigos komunikacijos sistemos, įskaitant elektroninį paštą, socialinius tinklus ir pan., technologiškai yra sukurtos informacijos saugojimui, t.y. vien dėl techninių priežasčių jos saugo visą įkeltą informaciją, jei ji nėra specialiai ištrinama;

7.3.2. Darbuotojai keldami bet kokią informaciją į Įstaigos IKT, įskaitant elektroninių pranešimų siuntimą naudojant Įstaigos elektroninį paštą, socialinių tinklų ir kitas panašias paskyras, gali ir privalo suprasti, kad tokia informacija neišvengiamai bus išsaugota. Darbdavio naudojamos

technologijos neleidžia pažymėti keliamos informacijos, įskaitant elektroninio pašto žinutes, kaip asmeninės, todėl įkėlus asmeninio pobūdžio informaciją ji gali atsitiktinai tapti žinoma kitiems asmenims. Atitinkamai Darbuotojai neturi naudoti Įstaigos IKT asmeninėms reikmėms, o tą darydami prisiima riziką, kad asmeninio pobūdžio informacija atsitiktinai gali tapti žinoma kitiems asmenims.

7.3.3. Darbuotojo susirašinėjimo duomenys siekiant užtikrinti Įstaigos veiklos nepertraukiamumą ir tęstinumą yra prieinami pavaduojantiems Darbuotojams jo atostogų, nedarbingumo ar panašiais laikotarpiais, o taip pat Darbuotojui nutraukus darbo sutartį bus prieinami naujam Darbuotojui, perimsiančiam atleisto Darbuotojo darbą.

7.3.4. Laikina prieiga prie Darbuotojo susirašinėjimo duomenų gali būti suteikta kitiems Darbuotojams:

7.3.4.1. kai prireikia skubiai gauti atitinkamą informaciją, o pačio Darbuotojo nėra darbo vietoje;

7.3.4.2. kai to reikia informacijos surinkimui siekiant pareikšti arba ginantis nuo pareikštų reikalavimų teisme, administracinėse procedūrose, komerciniuose ginčuose su Darbuotoju ar Trečiaisiais asmenimis arba kitokiose teisinėse procedūrose.

7.3.5. Darbuotojo susirašinėjimo duomenys gali būti panaudoti kaip įrodymas nustatant Darbuotojo darbo pareigų pažeidimus.

7.4. Įstaiga nevykdo nuolatinio, sistemingo IKT stebėjimo, t.y. nerenka Darbuotojų Duomenų IKT, tačiau Įstaigos paskirti Darbuotojai turi teisę atlikti IKT patikrinimą, įskaitant bet neapsiribojant Darbuotojo elektroninio pašto, socialinių tinklų ir panašių paskyrų, Darbuotojo žinioje esančių kompiuterių, planšetinių kompiuterių ir kitos įrangos patikrinimą, šiais atvejais:

7.4.1. kai yra nustatoma arba tiriama nusikalstama veika, kiti rimti teisės ir (ar) darbo tvarkos taisyklių pažeidimai;

7.4.2. kai yra nustatomas arba tiriamas konfidencialios informacijos nutekėjimas, intelektinės nuosavybės pažeidimas;

7.4.3. kai vyksta bylinėjimasis;

7.4.4. kai reikia atlikti Duomenų saugumo pažeidimo valdymą;

7.4.5. kai reikia užtikrinti Įstaigos IKT saugumą.

7.5. Įstaiga tikrina IKT tais atvejais, kai nėra kitų priemonių 7.4 punkte nurodytiems tikslams pasiekti. Sprendimą dėl IKT tikrinimo priima Įstaigos vadovas (sprendimo forma pridedama kaip priedas Nr. 2).

7.6. Tikrindami IKT, Įstaigos paskirti Darbuotojai turi kiek įmanoma labiau sumažinti renkamų, naudojamų ir saugojamų Duomenų kiekį. Tikrindami IKT, Įstaigos paskirti Darbuotojai renka, naudoja ir saugo tik tokius Duomenis, kurie yra būtini IKT tikrinimui. Jei tikrinant IKT pertekliniai Duomenys buvo surinkti, Darbuotojai nedelsdami juos ištrina.

7.7. Įstaigos paskirti Darbuotojai gali pradėti tikrinti IKT po to, kai atliko žemiau išvardintus veiksmus:

7.7.1. nustatė konkrečias priežastis, įtarimus ar informaciją, dėl kurių reikia tikrinti IKT, ir konkrečius IKT tikrinimo tikslus remdamiesi šios Taisyklių 7.4 punktu;

7.7.2. nustatė, kad kitų priemonių pasiekti tikslinimo tikslams nėra arba šios priemonės yra neveiksmingos;

7.7.3. informavo Duomenų apsaugos pareigūną ir gavo jo konsultaciją dėl numatomo IKT tikrinimo;

7.7.4. reikiamais atvejais pasitelkė IKT ekspertą ir (ar) antstolį;

7.7.5. pasirūpino, kad būtų priimtas raštiškas sprendimas dėl IKT tikrinimo (sprendimo forma pridedama kaip priedas Nr. 2).

7.8. Įstaigos paskirti Darbuotojai turi informuoti konkrečius Darbuotojus, kurių IKT yra tikrinamos, ir sudaryti jiems galimybę stebėti IKT tikrinimą, nebent minėtos informacijos atskleidimas sutrukdytų pasiekti tikrinimo tikslus.

7.9. Atlikę IKT patikrinimą, Įstaigos paskirti Darbuotojai turi raštu įforminti IKT tikrinimo rezultatus.

8. DUOMENŲ SAUGUMO PAŽEIDIMŲ VALDYMAS

8.1. Darbuotojas, sužinojęs apie galimą Duomenų saugumo pažeidimą Įstaigoje, nedelsdamas, bet ne vėliau kaip per 12 (dvylika) valandų, turi apie tai informuoti Duomenų apsaugos pareigūną.

8.2. Duomenų apsaugos pareigūnas vykdo Duomenų saugumo pažeidimų valdymą vadovaudamasis šiomis Taisyklėmis ir ADA teisės aktais ir pildo duomenų saugumo pažeidimo registrą (registro įrašo forma pridedama kaip Priedas Nr. 3).

8.3. Duomenų apsaugos pareigūnas užtikrina, kad laikomasi šios Taisyklių ir ADA teisės aktų nustatytų terminų. Duomenų apsaugos pareigūnas pažeidimų registre nurodydamas pratęsimo priežastis, gali pratęsti terminus, jei tai reikalinga dėl to paties Asmens Duomenų saugumo pažeidimo sudėtingumo ar skaičiaus.

8.4. Duomenų apsaugos pareigūnas gavęs informaciją apie galimą Duomenų saugumo pažeidimą iš Darbuotojo ar pats jį pastebėjęs nedelsdamas, bet ne vėliau kaip per 12 (dvylika) valandų, atlieka pirminę Duomenų saugumo pažeidimo analizę:

8.4.1. peržiūri informaciją apie Duomenų saugumo pažeidimą;

8.4.2. nustato Duomenų saugumo pažeidimo valdymo (įskaitant reikalingos informacijos rinkimą, konsultavimąsi su Darbuotojais ir (arba) Paslaugų teikėjais) terminus;

8.4.3. nustato, ar ir kokia papildoma informacija iš Darbuotojų yra reikalinga vykdant Duomenų saugumo pažeidimo valdymą, bei paprašo šios informacijos;

8.4.4. nustato, ar ir kokie Paslaugų teikėjai, išorės Duomenų apsaugos pareigūnai, IT saugumo konsultantai ir (ar) kiti Tretieji asmenys turi būti įtraukti į Duomenų saugumo pažeidimų valdymo procesą bei prireikus prašo jų pagalbos.

8.5. Duomenų apsaugos pareigūnas, nustatęs, kad Duomenų saugumo pažeidimo valdymui reikalinga papildoma informacija, paprašo Darbuotojų ir (ar) Paslaugų teikėjų suteikti reikiamą informaciją ne vėliau kaip per 24 (dvidešimt keturias) valandas. Darbuotojai turi laiku suteikti Duomenų apsaugos pareigūnui visą prašomą informaciją.

8.6. Duomenų apsaugos pareigūnas ne vėliau kaip per 72 (septyniasdešimt dvi) valandas nuo momento, kai sužinojo apie Duomenų saugumo pažeidimą, turi užbaigti Duomenų saugumo pažeidimo valdymą, įskaitant Duomenų saugumo pažeidimo užregistravimą ir, jei reikia, pranešimų pateikimą Inspekcijai.

8.7. Duomenų apsaugos pareigūnas vykdo Duomenų saugumo pažeidimo valdymą:

8.7.1. pildydamas Duomenų saugumo pažeidimų registro įrašo formą ir joje aprašydamas kiekvieną Duomenų saugumo pažeidimą (forma pridedama kaip Priedas Nr. 3);

8.7.2. teikdamas pranešimus Inspekcijai ir Asmenims apie Duomenų saugumo pažeidimus;

8.7.3. teikdamas rekomendacijas ir nurodymus Darbuotojams dėl Duomenų saugumo pažeidimų pasekmių šalinimo ar švelninimo.

8.8. Duomenų apsaugos pareigūnas raštu praneša Inspekcijai apie kiekvieną Duomenų saugumo pažeidimą, išskyrus atvejus, kai Duomenų saugumo pažeidimų registro įrašas rodo, jog atitinkamas Duomenų saugumo pažeidimas nekelia pavojaus Asmenims (pranešimo forma pridedama kaip Priedas Nr. 4).

8.9. Jei užpildytas Duomenų saugumo pažeidimų registro įrašas rodo, jog atitinkamas Duomenų saugumo pažeidimas kelia didelį pavojų Asmenims, kurių Duomenys buvo paveikti, Duomenų apsaugos pareigūnas raštu praneša Asmenims apie Duomenų saugumo pažeidimą,

išskyrus atvejus, kai Duomenų saugumo pažeidimų registro įrašas įrodo, jog Asmenys buvo apsaugoti nuo pavojaus (pranešimo forma pridedama kaip Priedas Nr. 5).

8.10. Jei užpildytas Duomenų saugumo pažeidimų registro įrašas pagrindžia, jog Asmenų informavimas apie jų Duomenų saugumo pažeidimą pareikalautų neproporcingų pastangų, Duomenų apsaugos pareigūnas neprivalo pranešti Asmenims apie Duomenų saugumo pažeidimą. Šiuo atveju Duomenų apsaugos pareigūnas, derindamas su Įstaigos vadovu, turi imtis kitų veiksmingų priemonių, skirtų informuoti Asmenis, kurių Duomenys buvo paveikti Duomenų saugumo pažeidimo (pvz., informaciją paskelbti internete ar žiniasklaidoje), bei šias priemones nurodyti Duomenų saugumo pažeidimo registro įraše.

9. INSPEKCIJOS PAKLAUSIMAI

9.1. Darbuotojas gavęs Inspekcijos paklausimą, nedelsiant, bet ne vėliau kaip per 1 (vieną) darbo dieną, informuoja Duomenų apsaugos pareigūną apie tokį paklausimą.

9.2. Duomenų apsaugos pareigūnas vykdo Inspekcijos paklausimų valdymą vadovaudamasis šiomis Taisyklėmis ir ADA teisės aktais.

9.3. Duomenų apsaugos pareigūnas, gavęs Inspekcijos paklausimą, turi nedelsdamas atlikti pirminę Inspekcijos paklausimo analizę:

9.3.1. peržiūrėti Inspekcijos paklausimą;

9.3.2. nustatyti atsakymo į Inspekcijos paklausimą terminus (įskaitant reikalingos informacijos surinkimą, konsultacijas su Darbuotojais ir (ar) Paslaugų teikėjais). Duomenų apsaugos pareigūnas turi patikslinti šiame skyriuje nurodytus terminus, jei to reikia, kad būtų laikomasi Inspekcijos nustatytų terminų;

9.3.3. jei reikia, kreiptis į Inspekciją dėl termino pateikti atsakymą pratęsimo;

9.3.4. nustatyti, ar yra reikalinga papildoma informacija iš Darbuotojų ir, jei taip, - paprašyti tokią informaciją pateikti;

9.3.5. nustatyti, ar Paslaugų teikėjai, išoriniai Duomenų apsaugos pareigūnai, IT saugumo konsultantai ir (ar) Tretieji asmenys yra susiję su Inspekcijos paklausimu ir, jei taip, paprašyti jų pagalbos rengiant atsakymą į Inspekcijos paklausimą.

9.4. Duomenų apsaugos pareigūnas, nustatęs, kad Inspekcijos paklausimo valdymui reikalinga papildoma informacija, paprašo Darbuotojų, Paslaugų teikėjų ir (ar) Trečiųjų šalių suteikti tokią informaciją. Darbuotojai turi laiku suteikti Duomenų apsaugos pareigūnui visą jo prašomą informaciją.

9.5. Surinkęs visą atsakymui į Inspekcijos paklausimą reikalingą informaciją, tačiau jokiu būdu ne vėliau kaip per Inspekcijos nustatytą terminą, Duomenų apsaugos pareigūnas parengia ir pateikia Inspekcijai atsakymą į paklausimą.

10. DUOMENŲ APSAUGOS PAREIGŪNAS

10.1. Įstaiga paskiria Duomenų apsaugos pareigūną, kuris padeda prižiūrėti kaip Įstaigoje laikomasi ADA teisės aktų reikalavimų.

10.2. Duomenų apsaugos pareigūnas turi būti tinkamai ir laiku (kuo anksčiau) įtrauktas į visus klausimus, susijusius su Duomenų apsauga Įstaigoje.

10.3. Duomenų apsaugos pareigūno vardas bei pavardė (pavadinimas) ir kontaktiniai duomenys turi būti nurodyti Duomenų tvarkymo veiklos įrašuose.

10.4. Duomenų apsaugos pareigūnas tiesiogiai atskaitingas Įstaigos vadovybei.

10.5. Duomenų apsaugos pareigūnas neturi gauti jokių nurodymų dėl užduočių vykdymo. Įstaiga negali atleisti Duomenų apsaugos pareigūno arba bausti jo dėl jam nustatytų užduočių atlikimo.

10.6. Įstaiga padeda Duomenų apsaugos pareigūnui vykdyti nurodytas užduotis suteikdama būtinus išteklius, taip pat suteikdama galimybę susipažinti su Duomenimis, dalyvauti duomenų tvarkymo operacijose ir išlaikyti savo ekspertines žinias.

10.7. Įstaiga paskelbia Duomenų apsaugos pareigūno kontaktinius duomenis ir praneša apie juos Inspekcijai.

10.8. Duomenų apsaugos pareigūnas atlieka šias užduotis:

10.8.1. informuoja Įstaigą, jos Darbuotojus ir valdymo organų narius apie jų prievoles pagal ADA teisės aktus, taip pat apie Duomenų apsaugą Įstaigoje ir konsultuoja juos šiais klausimais;

10.8.2. stebi, kaip Įstaigoje laikomasi ADA teisės aktų;

10.8.3. rūpinasi Duomenų rinkimo, naudojimo ir saugojimo veikloje dalyvaujančių Darbuotojų sąmoningumo ugdymu bei mokymu;

10.8.4. atlieka ir (arba) koordinuoja Įstaigos atitikties ADA teisės aktams auditus;

10.8.5. koordinuoja, atlieka ir (ar) stebi poveikio Duomenų apsaugai vertinimus Įstaigoje;

10.8.6. stebi, ar Įstaiga kuria, diegia ir (ar) naudoja IKT Duomenų tvarkymui laikantis ADA teisės aktų reikalavimų;

10.8.7. atlieka kontaktinio asmens funkcijas Asmenims, kurie kreipiasi į Įstaigą su Duomenų tvarkymu susijusiais klausimais;

10.8.8. konsultuoja Įstaigą dėl Duomenų perdavimo konkretiems Paslaugų teikėjams ar kitiems subjektams, įsisteigusiems už EEE ribų.

10.8.9. rengia šias Taisykles, Duomenų tvarkymo veiklos įrašus, kitas su Duomenų apsauga susijusias vidaus taisykles, procedūras, šablonus, standartines formas ir kitus dokumentus, prižiūri jų laikymąsi ir juos peržiūri;

10.8.10. koordinuoja, kad Įstaiga su visais Paslaugų teikėjais sudarytų Duomenų tvarkymo sutartis, įskaitant sąlygas dėl paslaugų teikimo (arba sutartis su Paslaugų teikėjais atitinkamomis nuostatomis);

10.8.11. praneša apie esamus ar galimus ADA teisės aktų pažeidimus, keliančius pavojus Įstaigos veiklai, bei konsultuoja Darbuotojus, atsakingus už šiuos pažeidimus;

10.8.12. praneša Įstaigos vadovybei, kai Įstaigoje nesivadovaujama Duomenų apsaugos pareigūno nuomone;

10.8.13. atlieka Duomenų saugumo pažeidimų valdymą;

10.8.14. atlieka Asmenų teisių įgyvendinimo valdymą;

10.8.15. atlieka kontaktinio asmens funkcijas Inspekcijai kreipiantis į Įstaigą.

11. POVEIKIO DUOMENŲ APSAUGAI VERTINIMAS

11.1. Darbuotojai privalo prieš protingą terminą informuoti Duomenų apsaugos pareigūną, kai ketinama Įstaigoje kurti, diegti ar naudoti tam tikras IKT ir (ar) kitus metodus, skirtus tvarkyti Duomenis, šiais atvejais:

11.1.1. naujos rūšies informacinės technologijos, kurios pirmą kartą diegiamos Įstaigoje;

11.1.2. ypatingų duomenų bazės;

11.1.3. Asmenų automatinio vertinimo ir profiliavimo įrankiai;

11.1.4. vaizdo stebėjimo priemonės;

11.1.5. IKT tikrinimo priemonės;

11.1.6. įrankiai, skirti Asmenis sekti internete;

11.1.7. nacionalinio, regioninio ar tarptautinio pobūdžio Duomenų bazės, kuriose saugomi dideli Duomenų kiekiai;

11.1.8. vaikų arba vyresnio amžiaus žmonių Duomenų bazės;

11.1.9. debesų kompiuterijos įrankiai;

11.1.10. dirbtinio intelekto įrankiai;

11.1.11. blokų grandinės (angl. blockchain) įrankiai;
11.1.12. socialinių tinklų įrankiai;
11.1.13. įrankiai, dėl kurių naudojimo Duomenys tampa prieinami Paslaugų teikėjams, įsteigtiems už EEE ribų;
11.1.14. kitos konkrečios IKT ir (arba) kiti metodai, skirti Įstaigoje tvarkyti Duomenis, jeigu jie patenka į Inspekcijos patvirtintą poveikio duomenų apsaugai reikalaujančių operacijų sąrašą;
11.1.15. kitos konkrečios IKT ir (ar) kiti metodai, skirti Įstaigoje tvarkyti Duomenis, kurie kelia pavojų Asmenims pagal ADA teisės aktus.
11.2. Duomenų apsaugos pareigūnas, gavęs Darbuotojo pranešimą, nedelsdamas suteikia raštišką konsultaciją atsakingam (-iems) Darbuotojui (-ams) dėl to, ar atlikti poveikio Duomenų apsaugai vertinimą dėl konkrečių IKT ir (ar) kitų metodų.
11.3. Gavęs Duomenų apsaugos pareigūno konsultaciją atsakingas (-i) Darbuotojas (-ai) turi nuspręsti, ar turi būti atliktas poveikio Duomenų apsaugai vertinimas dėl konkrečių IKT ir (ar) kitų metodų, skirtų tvarkyti Duomenis Įstaigoje, bei informuoti Duomenų apsaugos pareigūną apie tokį sprendimą.
11.4. Duomenų apsaugos pareigūnas, gavęs sprendimą atlikti poveikio Duomenų apsaugai vertinimą, pagal šių Taisyklių ir ADA teisės aktų reikalavimus turi:
11.4.1. nustatyti, ar ir kokia papildoma informacija iš Darbuotojų ir (ar) Paslaugų teikėjų yra reikalinga siekiant atlikti poveikio Duomenų apsaugai vertinimą, ir paprašyti tokią informaciją pateikti;
11.4.2. nuspręsti, ar Duomenų apsaugos pareigūnas atliks poveikio Duomenų apsaugai vertinimą pats, ar paprašys Paslaugų teikėjo ar kitos kvalifikuotos trečiosios šalies atlikti tokį vertinimą bei paruošti išvadą;
11.4.3. nustatyti, ar ir kurie Paslaugų teikėjai, išorės Duomenų apsaugos pareigūnai, IT saugumo konsultantai ir (arba) kiti tretieji asmenys turi dalyvauti poveikio Duomenų apsaugai vertinime bei paprašyti šių trečiųjų asmenų įsitraukti į poveikio Duomenų apsaugai vertinimo rengimą;
11.4.4. per protingą terminą nuo visos reikiamos informacijos gavimo pagal ADA teisės aktų reikalavimus atlikti poveikio Duomenų apsaugai vertinimą ir parengti raštišką vertinimo ataskaitą dėl kiekvienos konkrečios IKT ir (ar) metodo; o tais atvejais, kai nusprendžiama poveikio Duomenų apsaugai vertinimą pavesti atlikti Paslaugų teikėjui ar kitai kvalifikuotai trečiajai šaliai, užtikrinti, kad šiuos veiksmus atliktų atitinkamas subjektas;
11.4.5. pateikti poveikio Duomenų apsaugai vertinimo išvadą atsakingam (-iems) Darbuotojui (-ams), o jei nustatoma, kad kyla didelis pavojus Asmenų Duomenų apsaugai, patarti jam (jiems) kreiptis į Inspekciją dėl išankstinės konsultacijos;
11.4.6. jei Duomenų apsaugai vertinimo išvadoje nustatoma, kad kyla didelis pavojus Asmenų Duomenų apsaugai, atsakingas (-i) Darbuotojas (-ai) privalo per 3 (tris) darbo dienas nuspręsti, ar kreiptis į Inspekciją dėl išankstinės konsultacijos, ir apie savo sprendimą informuoti Duomenų apsaugos pareigūną;
11.4.7. Duomenų apsaugos pareigūnas, gavęs atsakingo (-ų) Darbuotojo (-ų) sprendimą kreiptis į Inspekciją dėl išankstinės konsultacijos, kreipiasi į Inspekciją Įstaigos vardu;
11.4.8. Duomenų apsaugos pareigūnas dalyvauja išankstinių konsultacijų procedūroje, bendradarbiauja su Inspekcija, analizuoja ir atsako į Inspekcijos paklausimus, Inspekcijos prašymu renka informaciją, jei reikia prašo Paslaugų teikėjų ir trečiųjų asmenų pagalbos arba kreipiasi į Inspekciją su prašymu gauti raštišką konsultaciją.

12. BAIGIAMOSIOS NUOSTATOS

12.1. Šios Taisyklės įsigalioja nuo jų patvirtinimo dienos ir taikomos Darbuotojams nuo supažindinimo su Taisyklėmis dienos.

12.2. Toliau nurodyti dokumentai pridedami prie Taisyklių kaip priedai ir yra neatskiriama jų dalis:

12.2.1. Duomenų tvarkymo sutarties forma;

12.2.2. Sprendimo dėl IKT tikrinimo forma;

12.2.3. Duomenų saugumo pažeidimų registro įrašo forma;

12.2.4. Pranešimo Inspekcijai apie Duomenų saugumo pažeidimą forma;

12.2.5. Pranešimo Asmeniui apie Duomenų saugumo pažeidimą forma.