PATVIRTINTA
Kretingos socialinių paslaugų centro direktoriaus
2021 m. gegužės 17 d. įsakymu Nr. V-126
(pakeitimas 2022-11-09 įsakymu Nr. V- 495)

ASMENS DUOMENŲ APSAUGOS POLITIKA

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Šios asmens duomenų apsaugos politikos (toliau – Politika) tikslai yra:

1.1. nustatyti asmens duomenų rinkimo, naudojimo ir saugojimo Kretingos socialinių paslaugų centro (toliau – SPC, įstaiga, darbdavys ar darbovietė) bendruosius principus ir taisykles;

1.2. įgyvendinti 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 – Bendrasis duomenų apsaugos reglamentas) įtvirtintus realios asmens duomenų apsaugos ir atskaitomybės principus;

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

1.4. sukurti tarpusavio supratimą bei teisinį aiškumą tarp įstaigos ir jos darbuotojų dėl veiksmų, kuriais įstaiga siekia apsaugoti savo darbuotojų asmens duomenis;

1.5. padėti įstaigos darbuotojams įgyvendinti ADA teisės aktų reikalavimus.

2. Šioje Politikoje ir jos prieduose vartojamos sąvokos turi žemiau nurodytas reikšmes:

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, LR darbo kodeksu, Asmens duomenų teisinės apsaugos įstatymu.
Asmuo	Žmogus (fizinis asmuo), kurio asmens duomenys renkami, naudojami ir saugojami įstaigoje ir kurio tapatybę galima nustatyti, įskaitant bet neapsiribojant darbuotojais, klientais. ADA teisės aktuose apibrėžiamas kaip **duomenų subjektas**.
Asmens prašymas	Bet kuris iš žemiau nurodytų: • prašymas susipažinti su duomenimis apie asmenį; • prašymas ištaisyti netikslius asmens duomenis; • prašymas ištrinti duomenis apie asmenį („teisė būti pamirštam“); • prašymas apriboti duomenų apie asmenį tvarkymą; • prašymas išeksportuoti duomenis apie asmenį (duomenų perkeliamumas); • prieštaravimas dėl duomenų apie asmenį rinkimo, naudojimo ir saugojimo įstaigoje; • prieštaravimas dėl bet kokio automatinio sprendimo priėmimo dėl asmens

	ar asmens profiliavimo įstaigoje; • bet kuris kitas prašymas ir (arba) skundas dėl bet kokio klausimo, susijusio su duomenų apsauga įstaigoje.
Darbuotojas	Bet kuris SPC darbuotojas arba komandiruotas į įstaigą darbuotojas, turintis tiesioginę ar netiesioginę prieigą prie duomenų.
Duomenys	Bet kokia informacija, susijusi su asmeniu, renkama, naudojama ar saugoma įstaigoje. ADA teisės aktuose apibrėžiama kaip **asmens duomenys.**
Duomenų apsaugos pareigūnas	Duomenų apsaugos pareigūnu (DAP) gali būti skiriamas įstaigos darbuotojas arba išorinis paslaugų teikėjas (t. y. atlikti DAP užduotis pagal paslaugų teikimo sutartį, sudarytą su asmeniu ar kitu juridiniu asmeniu), kuris padeda įstaigai užtikrinti teisinę atitiktį ADA teisės aktams, priimantis sprendimus ir konsultuojantis darbuotojus ir kitus asmenis duomenų apsaugos srityje.
Duomenų tvarkymas	Bet kokia automatizuotomis arba neautomatizuotomis priemonėmis su asmens duomenimis ar asmens duomenų rinkiniais atliekama operacija ar operacijų seka, kaip antai rinkimas, įrašymas, rūšiavimas, sisteminimas, saugojimas, adaptavimas ar keitimas, išgava, susipažinimas, naudojimas, atskleidimas persiunčiant, platinant ar kitu būdu sudarant galimybę jais naudotis, taip pat sugretinimas ar sujungimas su kitais duomenimis, apribojimas, ištrynimas arba sunaikinimas.
Duomenų saugumo pažeidimas	Bet kuris iš toliau nurodytų įvykių: • įstaigos IKT, dokumentų ir (arba) kitų priemonių, kuriuose yra duomenų praradimas, vagystė arba nesuplanuotas sunaikinimas; • atsitiktinis ar tyčinis duomenų siuntimas, įkėlimas ar dalinimasis su trečiaisiais asmenimis, neturinčiai teisės jų gauti; • trečiųjų asmenų neteisėta prieiga prie įstaigos IKT, dokumentų ir (ar) kitų priemonių, kuriose yra duomenų; • kenkėjiškos atakos prieš įstaigos IKT ir (ar) kitas priemones, kuriose yra duomenų; • klaidos, susijusios su kuriamomis, naudojamomis ir konfigūruojamomis IKT ir (ar) kitomis priemonėmis, kurios gali kelti pavojų duomenų saugumui; • 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).

Įstaiga	Kretingos socialinių paslaugų centras (SPC), atsakingas už duomenų rinkimą, naudojimą ir saugojimą, ADA teisės aktų laikymąsi. ADA teisės aktuose apibrėžiama kaip **duomenų valdytojas arba duomenų tvarkytojas**, atsižvelgiant į konkrečių duomenų tvarkymą.
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.
Informacinių sistemų administratorius	SPC darbuotojas (-a), atsakingas (-a) už informacinių ir komunikacinių technologijų (IKT) infrastruktūrą, užtikrinant jos ir informacinių sistemų (IS) veikimą ir elektroninės informacijos saugą įstaigoje.
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.
Klientas	Asmuo (suaugęs ar vaikas), kuris naudojasi SPC teikiamomis socialinėmis paslaugomis (paslaugų gavėjas).
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**.
Saugos įgaliotinis	SPC darbuotojas (-a), atsakingas (-a) už SPC asmens duomenų apsaugos politikos ir elektroninės informacijos saugos politikos įgyvendinamą įstaigoje
Specialių kategorijų asmens 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). ADA teisės aktuose apibrėžiami kaip specialių kategorijų asmens duomenys. **Reglamento 35 pastraipa:** prie asmens sveikatos duomenų turėtų būti priskirti visi duomenys apie duomenų subjekto sveikatos būklę, kurie atskleidžia informaciją apie duomenų subjekto buvusią, esamą ar būsimą fizinę ar psichinę sveikatą. Tai apima informaciją apie fizinį asmenį, surinktą registruojantis sveikatos priežiūros paslaugoms gauti ar jas teikiant tam fiziniam asmeniui, kaip nurodyta Europos Parlamento ir Tarybos direktyvoje 2011/24/ES (9); fiziniam asmeniui priskirtą numerį, simbolį ar žymę, pagal kurią galima konkrečiai nustatyti fizinio asmens tapatybę sveikatos priežiūros tikslais; informaciją, gautą atliekant kūno dalies ar medžiagos tyrimus ar analizę, įskaitant genetinius duomenis ir biologinius mėginius; ir bet kurią informaciją apie,

pavyzdžiui, ligą, negalią, riziką susirgti, sveikatos istoriją, klinikinį gydymą arba duomenų subjekto fiziologinę ar biomedicininę būklę, neatsižvelgiant į informacijos šaltinį, pavyzdžiui, ar ji būtų gauta iš gydytojo, ar iš kito sveikatos priežiūros specialisto, ligoninės, medicinos priemonės ar in vitro diagnostinio tyrimo.

3. Kitos šioje Politikoje sąvokos suprantamos taip, kaip jos apibrėžtos ADA teisės aktuose.

II SKYRIUS
TAIKYMO SRITIS IR ADRESATAI

4. Ši Politika taikoma:

4.1. duomenų rinkimui, naudojimui ir saugojimui įstaigos vardu;

4.2. duomenų, tvarkomų įstaigoje rinkimui, naudojimui ir saugojimui;

4.3. klientų, kurie naudojasi įstaigos teikiamomis socialinėmis paslaugomis, duomenų tvarkymui;

4.4. darbuotojų darbo funkcijų tikslu vykdomam duomenų rinkimui, naudojimui ir saugojimui;

4.5. duomenų rinkimui, naudojimui ir saugojimui naudojant IKT.

5. Ši Politika privaloma visiems įstaigos darbuotojams, įskaitant vadovybę. Darbuotojai su šia Politika yra supažindinami galiojančių Darbo tvarkos taisyklių nustatyta tvarka.

6. Atskiruose Politikos skyriuose numatytos atsakomybės, aktualios tik atitinkamas pareigas einantiems darbuotojams. Politika taip pat numato pareigas ir atsakomybes, kurių turi laikytis visi darbuotojai.

7. Visi darbuotojai turi patvirtinti, kad suprato savo įsipareigojimus ir privalo jų laikytis. Duomenų apsaugos pareigūnas turi užtikrinti, kad kiekvienam darbuotojui būtų pateikta ar pasiekiama šios Politikos kopija.

III SKYRIUS
DUOMENŲ TVARKYMO PRINCIPAI

8. Įstaiga tvarkydama duomenis vadovaujasi principais, kad asmens duomenys turi būti:

8.1. tvarkomi teisėtai, sąžiningai ir skaidriai;

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

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

8.4. renkami, naudojami ir saugojami laikantis įstaigos vidaus procedūrų ir užtikrinant duomenų apsaugą nuo neleistinos prieigos, neteisėto rinkimo, naudojimo ir saugojimo, netyčinio praradimo, sunaikinimo ar sugadinimo;

8.5. tikslūs ir prireikus atnaujinami;

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

8.7. tvarkomi tokiu būdu, kad taikant atitinkamas technines ar organizacines priemones būtų užtikrintas tinkamas asmens duomenų saugumas ir konfidencialumas, įskaitant prieigos prie

duomenų suteikimą tik tiems darbuotojams, kuriems jų reikia savo tiesioginėms darbo funkcijoms atlikti.

9. Duomenys gali būti teisėtai tvarkomi įstaigoje, tik esant bent vienam iš šių pagrindų:

9.1. 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;

9.2. teisinė prievolė: įstaiga teisės aktais yra įpareigota tvarkyti duomenis mokesčių, darbo ir kitose srityse, arba valdyti sveikatos priežiūros sistemas, vadovaujantis taikytinais teisės aktais;

9.3. teisėtas interesas: duomenys yra reikalingi ginčų nagrinėjimui, incidentų tyrimui, turto, žmonių ir IKT saugumo užtikrinimui, veiklos tęstinumui ar kitiems iš anksto nustatytiems įstaigos interesams, jei asmens interesai konkrečių aplinkybių kontekste nėra svarbesni.

9.4. sutikimas: asmuo galėjo laisvai pasirinkti, ar duoti sutikimą dėl jo duomenų tvarkymo, be jokių neigiamų pasekmių asmeniui ir tokį sutikimą davė.

10. Specialių kategorijų asmens duomenys, kurie gali būti teisėtai tvarkomi įstaigoje:

10.1. klientų sveikatos duomenys teikiant socialinės priežiūros ir pagalbos paslaugas – tik ta apimtimi, kiek yra būtina siekiant valdyti socialinių paslaugų sistemas, vadovaujantis taikytinais teisės aktais;

10.2. darbuotojų sveikatos duomenys – tik ta apimtimi, kiek yra būtina siekiant įgyvendinti teises ar pareigas sveikatos, darbo ir socialinės apsaugos teisės srityse;

10.3. kitų asmenų specialių kategorijų asmens duomenys – tik ta apimtimi, kiek asmuo galėjo laisvai pasirinkti, ar duoti sutikimą tvarkyti specialių kategorijų duomenis, be jokių neigiamų pasekmių asmeniui bei davė tokį sutikimą raštu arba elektronine forma;

10.4. kitų asmenų specialių kategorijų asmens duomenis tvarkyti yra būtina ES ar nacionalinių teismų teisminių įgaliojimų vykdymui, teisėtvarkos ar priežiūros institucijų tyrimų vykdymui;

10.5. tvarkyti specialių kategorijų asmens duomenis būtina siekiant pareikšti, vykdyti arba apginti teisinius reikalavimus.

11. Duomenys apie asmenų teistumą gali būti tvarkomi tik, kai tai numato specialūs teisės aktai ir tik ta apimtimi, kiek tai reikalinga atitinkamų teisės aktų įgyvendinimui.

IV SKYRIUS
DUOMENŲ TVARKYMO VEIKLOS ĮRAŠAI

12. Siekdama užtikrinti duomenų tvarkymo teisėtumą, nuolatinę ir aktualią informaciją apie savo vykdomos duomenų tvarkymo veiklos apimtis, joje dalyvaujančius asmenis, naudojamas tvarkymo priemones įstaiga sudaro duomenų tvarkymo veiklos įrašus.

13. Duomenų tvarkymo veiklos įrašai yra tvarkomi raštu. Rašytinei formai yra prilyginama ir elektroninė forma, saugoma kompiuteryje. Tvarkant duomenų tvarkymo veiklos įrašus turi būti užtikrinamas jų pakeitimų atsekamumas, tam kad būtų galima nustatyti, kokie pakeitimai buvo daromi, kada jie buvo atlikti ir dėl kokių priežasčių.

14. Duomenų tvarkymo veiklos įrašuose turi būti nurodoma ši informacija (priedas Nr. 1):

14.1. duomenų subjektų kategorijos;

14.2. asmens duomenų kategorijos pagal kiekvieną duomenų subjekto kategoriją;

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

14.4. duomenų gavėjų kategorijos kiekvienai asmenų kategorijai pagal duomenų perdavimo tikslus bei teisinį pagrindą;

14.5. jei tokių yra, duomenų gavėjai, veikiantys ne EEE šalyse, ir jiems taikomos duomenų apsaugos užtikrinimo priemonės; šiuo metu įstaiga duomenų perdavimo už EEE ribų nevykdo;

14.6. duomenų saugojimo, ištrynimo terminai;

14.7. kita informacija;

14.8. bendras duomenų saugumo priemonių aprašymas (kai įmanoma);

14.9. duomenų įvedimo, keitimo data (-os).

15. Duomenų tvarkymo veiklos įrašai yra įstaigos vidaus dokumentai, kuriuose gali būti konfidencialios informacijos, todėl jie negali būti viešinami ir turi būti saugomi kaip ir kita įstaigos konfidenciali informacija.

16. Už duomenų tvarkymo veiklos įrašų sudarymo, keitimo ir atnaujinimo organizavimą ir centralizuotą jų tvarkymą atsakingas duomenų apsaugos pareigūnas, o įstaigos vadovas yra tiesiogiai atsakingas už informacijos, reikalingos duomenų tvarkymo veiklos įrašams sudaryti, pakeisti ar atnaujinti, surinkimą, jų projektų paruošimą bei pateikimą duomenų apsaugos pareigūnui.

17. Įstaiga turi pateikti duomenų tvarkymo veiklos įrašus Valstybinei duomenų apsaugos inspekcijai, gavę jos prašymą, pavyzdžiui, priežiūros institucijai atliekant prevencinį tyrimą ir (ar) tikrinimą, nagrinėjant duomenų subjekto prašymą ar pan.

18. Įstaigos darbuotojai atsakingi už asmens duomenų tvarkymą ar turintys prieigą prie asmens duomenų turi būti susipažinę su duomenų tvarkymo veiklos įrašais. Duomenų apsaugos pareigūnas turi užtikrinti, kad darbuotojui būtų pateikta ar pasiekiama duomenų tvarkymo veiklos įrašo kopija.

V SKYRIUS
BENDROSIOS DARBUOTOJŲ PAREIGOS DUOMENŲ APSAUGOS SRITYJE

19. Kiekvienas darbuotojas privalo:

19.1. tvarkydamas duomenis, įsitikinti, kad yra laikomasi visų reikalavimų, numatytų šioje Politikoje;

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

19.3. visais atvejais identifikuoti duomenis, kurie yra tvarkomi darbuotojo veikloje bei žinoti, kad veiklai, susijusiai su duomenimis, yra taikomi šios Politikos, duomenų tvarkymo sutarčių ir ADA teisės aktų reikalavimai.

20. Kai tvarkomi duomenys, kurių valdytojas yra įstaiga:

20.1. 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;

20.2. visais atvejais prieš perduodant duomenis trečiosioms šalims 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 veikiančiai trečiai šaliai, nenurodytam duomenų tvarkymo veiklos įrašuose, informuoti duomenų apsaugos pareigūną.

21. 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, kai pagal veiklos įrašus jis yra būtinas, 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.

22. Atsižvelgiant į atliekamų darbo funkcijų pobūdį imtis protingų pastangų, kad užtikrintų, jog visi įstaigos valdomi duomenys būtų tikslūs ir prireikus atnaujinami.

23. Tvarkydami duomenis, elgtis rūpestingai ir atsargiai, turėdami omenyje tai, kad darbuotojo veiksmai, susiję su duomenimis, kelia pavojų įstaigai ir asmenims, esant bet kokiam neaiškumui, susijusiam su duomenų tvarkymu, kreiptis į duomenų apsaugos pareigūną ir prieš atliekant duomenų tvarkymo operaciją gauti duomenų apsaugos pareigūno konsultaciją ar nurodymą.

24. 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 šioje Politikoje, darbo tvarkos taisyklėse ir kituose įstaigos norminiuose dokumentuose. Organizacinių ir techninių duomenų saugumo priemonių sąrašas pateikiamas ir pagal poreikį tikslinamas priede Nr. 2.

25. Neatskleisti informacijos apie įstaigos taikomas technines ir organizacines duomenų apsaugos priemones, įskaitant, bet neapsiribojant, įstaigos vidaus dokumentais, jokioms trečioms šalims, prieš tai neįsitikinus jų teise gauti tokią informaciją.

26. Nesaugoti asmens duomenų jokiose darbuotojui priklausančiose asmeninėse atmintinėse, kompiuterinėje ar programinėje įrangoje (internetinėse duomenų saugyklose, atmintinėse, kompiuteriuose, telefonuose ir pan.), nebent konkrečiu atveju įstaiga leistų darbuotojui naudoti konkrečias asmenines priemones darbo funkcijų vykdymui, tokiu atveju pasibaigus darbo santykiams perduoti visus darbuotojo bet kokiose informacijos rinkmenose esančius duomenis įstaigai ir sunaikinti visas tokios informacijos kopijas.

27. Kreiptis į duomenų apsaugos pareigūną ir gauti jo konsultaciją:

27.1. ketinant įstaigoje pasitelkti naują paslaugų teikėją;

27.2. ketinant įstaigoje sukurti, diegti ar naudoti naujas IKT ir (ar) kitus metodus duomenų tvarkymui;

27.3. prieš pradedant naują tiesioginės rinkodaros kampaniją ar duomenų rinkimą jos įgyvendinimui;

27.4. esant bet kokiems netikslumams, abejonėms ar klausimams, susijusiems su šios Politikos taikymu, aiškinimu, pažeidimu ar atitikimu Politikai.

28. Su asmenų prašymais elgtis rūpestingai ir atidžiai; gavę bet kokį asmens prašymą nedelsdami, ne vėliau kaip per 1 (vieną) darbo dieną nuo asmens prašymo gavimo, pranešti apie tai duomenų apsaugos pareigūnui.

29. Nedelsiant, bet ne vėliau kaip per 12 (dvylika) valandų, nuo sužinojimo apie duomenų saugumo pažeidimą įstaigoje:

29.1. informuoti duomenų apsaugos pareigūną apie duomenų saugumo pažeidimą;

29.2. pagal savo kompetenciją imtis pagrįstų veiksmų, kad duomenų saugumo pažeidimas būtų sustabdytas;

29.3. pagal savo kompetenciją imtis pagrįstų veiksmų, kad duomenų saugumo pažeidimas nepasikartotų;

29.4. 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;

29.5. per trumpiausius galimus terminus pateikti duomenų apsaugos pareigūnui bet kokią prašomą informaciją;

29.6. vykdyti duomenų apsaugos pareigūno nurodymus dėl duomenų tvarkymo.

30. Nė vienam darbuotojui neturi būti suteikta prieiga prie duomenų, jei šie duomenys nėra reikalingi jų darbo funkcijoms atlikti.

VI SKYRIUS
ASMENŲ TEISIŲ ĮGYVENDINIMAS

31. Darbuotojas, gavęs asmens prašymą, nedelsdamas, ne vėliau kaip per 1 (vieną) darbo dieną nuo asmens prašymo gavimo dienos kreipiasi į duomenų apsaugos pareigūną.

32. Duomenų apsaugos pareigūnas atlieka gautų asmenų prašymų valdymą vadovaudamasis šia Politika ir ADA teisės aktais.

33. Duomenų apsaugos pareigūnas atlieka asmenų prašymų valdymą užpildydamas asmenų prašymų registro įrašo formą atskirai kiekvienam asmens prašymui (priedas Nr. 3, pildoma elektroninė forma, saugoma kompiuteryje).

34. Gavęs prašymą, duomenų apsaugos pareigūnas:

34.1. peržiūri prašymą;

34.2. nustato prašymą pateikusio asmens tapatybę;

34.3. surenka prašymo nagrinėjimui reikalingą informaciją;

34.4. įvertina prašymo teisinį pagrįstumą;

34.5. patvirtina asmeniui, kad jo prašymas yra gautas;

34.6. nustato, ar ir kokia papildoma informacija iš darbuotojų, paslaugų teikėjų ir (ar) asmens, kuris pateikė prašymą, yra reikalinga siekiant atsakyti į asmens prašymą;

34.7. esant reikalui duoda reikiamus pavedimus darbuotojams dėl prašymą pateikusio asmens duomenų tolesnio tvarkymo;

34.8. paruošia ir pateikia asmeniui atsakymą į prašymą.

35. Duomenų apsaugos pareigūnas užtikrina, kad:

35.1. 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;

35.2. asmeniui būtų pateikta tik ta informacija, kuri yra susijusi su juo;

35.3. asmeniui būtų pateikiama tik tiek informacijos, kiek reikalauja ADA teisės aktai;

35.4. ADA teisės aktų numatytais atvejais, kai asmuo neturi teisės pasinaudoti savo kaip duomenų subjekto teise, asmens prašymas nebūtų tenkinamas;

35.5. asmenims nebūtų atskleista jokia įstaigos konfidenciali informacija, ypatingai klientų duomenys.

36. Asmens prašymą tenkinti atsisakoma, kai:

36.1. asmens prašymas nesusijęs su ADA teisės aktų numatytomis teisėmis;

36.2. asmens prašymas susijęs su informacija, kuri nėra duomenys;

36.3. asmens prašymas susijęs su informacija apie kitą asmenį;

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

36.5. asmens prašymas yra akivaizdžiai neproporcingas, įskaitant, bet neapsiribojant, šiais atvejais:

36.5.1. asmens prašymas yra pasikartojantis – tas pats asmuo jau yra pateikęs tokį patį prašymą per 1 (vienus) metus iki prašymo gavimo išskyrus atvejus, kai per šį laikotarpį asmuo gali pagrįstai tikėtis, kad pasikeitė apie asmenį tvarkomų duomenų apimtis;

36.5.2. asmens prašymas susijęs su dideliu kiekiu pasikartojančių duomenų;

36.5.3. aplinkybės rodo, kad vienintelis asmens prašymo tikslas yra sutrikdyti įstaigos veiklą ir įstaiga gali tai įrodyti.

37. 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.

38. 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.

39. 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.

VII SKYRIUS
PASLAUGŲ TEIKĖJAI

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

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

40.2. 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).

41. 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.

VIII SKYRIUS
DARBUOTOJŲ STEBĖSENOS IR KONTROLĖS DARBO VIETOJE TVARKA

42. Įstaigos teritorijoje vaizdo stebėjimo duomenys yra tvarkomi siekiant apsaugoti darbdavio turtą nuo vagysčių ir panašių nusikaltimo požymių turinčių veikų.

43. Vaizdo duomenys tvarkomi laikantis šių principų:

43.1. nustačius įtariamą vagystę ar panašią nusikaltimo požymių turinčią veiką ir tai patvirtina peržiūrėta vaizdo medžiaga, atitinkamas vaizdo įrašo fragmentas perduodamas įstaigos vadovui ar kitam jo paskirtam darbuotojui. Kai įtariamas įstaigos 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;

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

43.3. 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.

44. Įstaigoje techninėmis garso įrašymo priemonėmis (diktofonais) yra fiksuojama atvejo vadybos posėdžių eiga (duomenų subjektų pokalbiai, pareiškimai, pranešimai ir pan.). Duomenis naudoja SPC atvejo vadybininkas rengiant pagalbos šeimai planą (elektronine ir popierine forma).

45. Garso įrašymo duomenys tvarkomi laikantis šių principų:

45.1. garso duomenys iš diktofono perkeliami į SPC atvejo vadybininko darbo kompiuteryje suformuotą elektroninę laikmeną – šeimos bylą, o įrašas diktofone iškart sunaikinamas;

45.2. garso įrašai elektroninėje laikmenoje saugomi iki atvejo vadybos proceso užbaigimo. Garso įrašus darbo kompiuteryje, gavus (priėmus) sprendimą užbaigti atvejo vadybos procesą, sunaikina SPC atvejo vadybininkas;

45.3. jei garso įrašų duomenys bus naudojami kaip įrodymai nustatant darbuotojo darbo pareigų pažeidimą, civilinėje, administracinėje ar baudžiamojoje byloje ar kitais įstatymų nustatytais atvejais, garso duomenys bus saugomi tiek, kiek reikalinga šiems duomenų tvarkymo tikslams, ir bus sunaikinami nedelsiant, kai taps nebereikalingi.

46. Įstaiga, siekdama valdyti savo IKT infrastruktūrą bei užtikrinti jos saugumą, gali suteikti nuotolinio prisijungimo galimybę prie savo IKT (kompiuterių, planšečių, telefonų ir pan.) jų techninę priežiūrą vykdantiems darbuotojams, 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.

47. Darbuotojo susirašinėjimo su kitais darbuotojais ir trečiomis šalimis (valstybinėmis institucijomis, 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:

47.1. įstaigos komunikacijos sistemos, įskaitant elektroninį paštą, technologiškai yra sukurtos informacijos saugojimui, t.y. vien dėl techninių priežasčių jos saugo visą įkeltą informaciją, jei ji nėra specialiai ištrinama;

47.2. 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 ir tokia techninė įranga reikalauja neproporcingai didelių kaštų, 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;

47.3. siekiant įgyvendinti komunikacijos su paslaugų gavėjais, įstaigos klientais ir vidinės tarpusavio komunikacijos įstaigoje praktiką, užtikrinti nenutrūkstamą ūkinę komercinę veiklą, kai yra būtina, įstaigos darbuotojams gali būti suteikiama prieiga prie kitų įstaigos darbuotojų naudojamų komunikacijos kanalų (pavyzdžiui, vardinio elektroninio pašto);

47.4. 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;

47.5. laikina prieiga prie darbuotojo susirašinėjimo duomenų gali būti suteikta kitiems darbuotojams:

47.5.1. kai prireikia skubiai gauti atitinkamą informaciją, o pačio darbuotojo nėra darbo vietoje,

47.5.2. kai to reikia informacijos surinkimui siekiant pareikšti arba ginantis nuo pareikštų reikalavimų teisme, administracinėse procedūrose, komerciniuose ginčuose su darbuotoju ar trečiomis šalimis arba kitokiose teisinėse procedūrose;

47.6. darbuotojo susirašinėjimo duomenys gali būti panaudoti kaip įrodymas nustatant darbuotojo darbo pareigų pažeidimus, tik kai toks pažeidimas nustatomas šioje Politikoje nustatyta tvarka.

48. 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, išskyrus asmenines paskyras, darbuotojo žinioje esančių kompiuterių, planšetinių kompiuterių ir kitos įrangos patikrinimą, šiais atvejais:

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

48.2. kai yra nustatomas arba tiriamas klientų duomenų, įstaigos konfidencialios informacijos nutekėjimas, intelektinės nuosavybės pažeidimas ir (ar) nesąžiningos konkurencijos atvejis;

48.3. kai vyksta bylinėjimasis;

48.4. kai reikia atlikti duomenų saugumo pažeidimo valdymą;

48.5. kai reikia užtikrinti įstaigos IKT saugumą.

49. **48 punkte** numatytą IKT patikrinimą gali atlikti įstaigos darbuotojai.

50. Įstaiga tikrina IKT tais atvejais, kai nėra kitų priemonių **48 punkte** nurodytiems tikslams pasiekti. Sprendimą dėl IKT tikrinimo priima įstaigos vadovas (sprendimo forma pridedama kaip priedas Nr. 4).

51. 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.

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

52.1. nustatė konkrečias priežastis, įtarimus ar informaciją, dėl kurių reikia tikrinti IKT, ir konkrečius IKT tikrinimo tikslus remdamiesi šios Politikos **48 punktu**;

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

52.3. informavo duomenų apsaugos pareigūną ir gavo jo konsultaciją dėl numatomo IKT tikrinimo;

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

52.5. pasirūpino, kad būtų priimtas raštiškas sprendimas dėl IKT tikrinimo (priedas Nr. 4).

53. 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.

54. Atlikę IKT patikrinimą, įstaigos paskirti darbuotojai turi raštu įforminti IKT tikrinimo rezultatus.

IX SKYRIUS
DUOMENŲ SAUGUMO PAŽEIDIMŲ VALDYMAS

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

56. Duomenų apsaugos pareigūnas vykdo duomenų saugumo pažeidimų valdymą vadovaudamasis šia Politika ir ADA teisės aktais ir pildo duomenų saugumo pažeidimo registrą (priedas Nr. 5, pildoma elektroninė forma, saugoma kompiuteryje).

57. Duomenų apsaugos pareigūnas užtikrina, kad laikomasi šios Politikos 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 masto.

58. 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:

58.1. peržiūri informaciją apie duomenų saugumo pažeidimą;

58.2. nustato duomenų saugumo pažeidimo valdymo (įskaitant reikalingos informacijos rinkimą, konsultavimąsi su darbuotojais ir (arba) paslaugų teikėjais) terminus;

58.3. nustato, ar ir kokia papildoma informacija iš darbuotojų yra reikalinga vykdant duomenų saugumo pažeidimo valdymą bei paprašo šios informacijos;

58.4. nustato, ar ir kokie paslaugų teikėjai, išorės duomenų apsaugos pareigūnai, IT saugumo konsultantai ir (ar) kitos trečios šalys turi būti įtrauktos į duomenų saugumo pažeidimo valdymo procesą bei prireikus prašo jų pagalbos.

59. 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 ir paslaugų teikėjai turi laiku suteikti duomenų apsaugos pareigūnui visą prašomą informaciją.

60. 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.

61. Duomenų apsaugos pareigūnas vykdo duomenų saugumo pažeidimo valdymą:

61.1. pildydamas duomenų saugumo pažeidimų registro įrašo formą ir joje aprašydamas kiekvieną duomenų saugumo pažeidimą (priedas Nr. 5);

61.2. teikdamas pranešimus Inspekcijai ir asmenims apie duomenų saugumo pažeidimus;

61.3. teikdamas rekomendacijas ir nurodymus darbuotojams dėl duomenų saugumo pažeidimų pasekmių šalinimo ar švelninimo.

62. Duomenų apsaugos pareigūnas raštu praneša Inspekcijai apie kiekvieną duomenų saugumo pažeidimą (pranešimo forma pridedama kaip priedas Nr. 6), išskyrus atvejus, kai duomenų saugumo pažeidimų registro įrašas rodo, jog atitinkamas duomenų saugumo pažeidimas nekelia pavojaus asmenims.

63. 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. 7).

64. 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.

X SKYRIUS
INSPEKCIJOS PAKLAUSIMAI

65. Duomenų apsaugos pareigūnas vykdo Inspekcijos paklausimų valdymą vadovaudamasis šia Politika ir ADA teisės aktais.

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

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

67.1. peržiūrėti Inspekcijos paklausimą;

67.2. nustatyti atsakymo į Inspekcijos paklausimą terminus (įskaitant reikalingos informacijos surinkimą, konsultacijas su darbuotojais ir (ar) paslaugų teikėjais);

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

67.4. nustatyti, ar yra reikalinga papildoma informacija iš darbuotojų ir, jei taip – paprašyti tokią informaciją pateikti;

67.5. nustatyti, ar paslaugų teikėjai, išoriniai duomenų apsaugos pareigūnai, IT saugumo konsultantai ir (ar) trečios šalys yra susiję su Inspekcijos paklausimu ir, jei taip, paprašyti jų pagalbos rengiant atsakymą į Inspekcijos paklausimą.

68. 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.

XI SKYRIUS
DUOMENŲ APSAUGOS PAREIGŪNAS

69. Įstaiga paskiria duomenų apsaugos pareigūną (DAP), kuris padeda prižiūrėti kaip įstaigoje laikomasi ADA teisės aktų reikalavimų ir veikia kaip įstaigos atstovas su asmens duomenų apsauga susijusiais klausimais.

70. Darbuotojai darbo tvarkos taisyklių nustatyta tvarka informuojami apie paskirtą duomenų apsaugos pareigūną bei jo kontaktinius duomenis.

71. Įstaiga padeda duomenų apsaugos pareigūnas vykdyti nurodytas užduotis suteikdama būtinus išteklius, taip pat suteikdama galimybę susipažinti su duomenimis, dalyvauti duomenų tvarkymo operacijose ir išlaikyti savo ekspertines žinias.

72. Duomenų apsaugos pareigūnas atlieka šias užduotis:

72.1. informuoja įstaigą, jos darbuotojus apie jų prievoles pagal ADA teisės aktus, taip pat apie duomenų apsaugą įstaigoje ir konsultuoja juos šiais klausimais;

72.2. stebi, kaip įstaigoje laikomasi ADA teisės aktų;

72.3. rūpinasi duomenų rinkimo, naudojimo ir saugojimo veikloje dalyvaujančių darbuotojų sąmoningumo ugdymu bei mokymu;

72.4. koordinuoja, atlieka ir (ar) stebi poveikio duomenų apsaugai vertinimus įstaigoje;

72.5. stebi, ar įstaiga kuria, diegia ir (ar) naudoja IKT duomenų tvarkymui laikantis ADA teisės aktų reikalavimų;

72.6. atlieka kontaktinio asmens funkcijas asmenims, kurie kreipiasi į įstaigą su duomenų tvarkymu susijusiais klausimais;

72.7. konsultuoja darbuotojus dėl duomenų perdavimo konkretiems paslaugų teikėjams ar kitiems subjektams, įsisteigusiems už EEE ribų;

72.8. dalyvauja rengiant šią Politiką, duomenų tvarkymo veiklos įrašus, kitas su duomenų apsauga susijusias vidaus taisykles, procedūras, šablonus ir kitus dokumentus, prižiūri jų laikymąsi ir juos periodiškai peržiūri;

72.9. koordinuoja, kad įstaiga su visais paslaugų teikėjais sudarytų duomenų tvarkymo sutartis, įskaitant sąlygas dėl paslaugų teikimo (arba sutartis su paslaugų teikėjais atitinkamomis nuostatomis);

72.10. praneša apie esamus ar galimus ADA teisės aktų pažeidimus, keliančius pavojus įstaigos veiklai bei konsultuoja darbuotojus, atsakingus už šiuos pažeidimus;

72.11. atlieka duomenų saugumo pažeidimų valdymą;

72.12. atlieka asmenų teisių įgyvendinimo valdymą;

72.13. atlieka kontaktinio asmens funkcijas Inspekcijai kreipiantis į įstaigą.

XII SKYRIUS
POVEIKIO DUOMENŲ APSAUGAI VERTINIMAS

73. Darbuotojai privalo prieš protingą terminą informuoti saugos įgaliotinį, kai ketinama įstaigoje kurti, diegti ar naudoti tam tikras IKT ir (ar) kitus metodus, skirtus tvarkyti duomenis, šiais atvejais:

73.1. naujos rūšies informacines technologijas, kurios pirmą kartą diegiamos įstaigoje;

73.2. specialiųjų kategorijų duomenų bazes;

73.3. asmenų automatinio vertinimo ir profiliavimo įrankius;

73.4. vaizdo stebėjimo priemones;

73.5. IKT tikrinimo priemones;

73.6. įrankius, skirti asmenis sekti internete;

73.7. nacionalinio, regioninio ar tarptautinio pobūdžio duomenų bazes, kuriose saugomi dideli duomenų kiekiai;

73.8. vaikų arba vyresnio amžiaus žmonių duomenų bazes;

73.9. debesų kompiuterijos įrankius;

73.10. daiktų interneto įrankius (t.y., įrankiai, sujungiantys į interneto tinklą kasdieninius objektus ir leidžiantys jiems siųsti ir gauti duomenis);

73.11. socialinių tinklų įrankius;

73.12. įrankius, dėl kurių naudojimo duomenys tampa prieinami paslaugų teikėjams, įsteigtiems už EEE ribų;

73.13. kitos konkrečios IKT ir (arba) kiti metodai, skirti įstaigoje tvarkyti duomenis, jeigu jie patenka į Inspekcijos patvirtintą poveikio duomenų apsaugai reikalaujančių operacijų sąrašą;

73.14. kitos konkrečios IKT ir (ar) kiti metodai, skirti įstaigoje tvarkyti duomenis, kurie kelia pavojų asmenims pagal ADA teisės aktus.

74. Saugos įgaliotinis, gavęs darbuotojo pranešimą, jį išnagrinėjęs, konsultuojasi su duomenų apsaugos pareigūnu, ir derindamas su įstaigos vadovu, turi nuspręsti, ar turi būti atliktas poveikio duomenų apsaugai vertinimas dėl konkrečių IKT ir (ar) kitų metodų, skirtų tvarkyti duomenis įstaigoje.

75. Saugos įgaliotinis priėmęs sprendimą atlikti poveikio duomenų apsaugai vertinimą, pagal šios Politikos ir ADA teisės aktų reikalavimus turi:

75.1. 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;

75.2. nuspręsti, ar atliks poveikio duomenų apsaugai vertinimą pats, ar paprašys paslaugų teikėjo ar kitos kvalifikuotos trečiosios šalies atlikti tokį vertinimą bei paruošti išvadą;

75.3. 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;

75.4. 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 (Priedas Nr. 8); 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;

75.5. kai asmens duomenys bus tvarkomi vadovaujantis BDAR 6 straipsnio 1 dalies f punktu, saugos įgaliotinis užpildo Teisėtų interesų balanso testo formą (Priedas Nr. 9) ir ją prideda kaip Poveikio asmens duomenų apsaugai vertinimo išvados priedą;

75.6. pateikti poveikio duomenų apsaugai vertinimo ataskaitą įstaigos vadovui ir atsakingam (-iems) darbuotojui (-ams);

75.7. jei duomenų apsaugai vertinimo išvadoje nustatoma, kad kyla didelis pavojus asmenų duomenų apsaugai, saugos įgaliotinis derindamas su įstaigos vadovu nusprendžia, ar kreiptis į Inspekciją dėl išankstinės konsultacijos. Nusprendus nesikreipti į Inspekciją dėl išankstinės konsultacijos IKT priemonės ar kitos **73 punkte** nurodytos priemonės diegimo yra atsisakoma.

76. 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 šalių pagalbos arba kreipiasi į Inspekciją su prašymu gauti raštišką konsultaciją.

XIII SKYRIUS
BAIGIAMOSIOS NUOSTATOS

77. Ši Politika įsigalioja nuo jos patvirtinimo dienos ir taikoma darbuotojams nuo supažindinimo su Politika dienos.

78. Toliau nurodyti priedai pridedami prie Politikos ir yra neatskiriama jos dalis:

Priedas Nr. 1, Įstaigos duomenų tvarkymo veiklos įrašo forma, kai įstaiga yra duomenų valdytojas.

Priedas Nr. 2, Organizacinės ir techninės duomenų saugumo priemonės (sąrašas);

Priedas Nr. 3, Asmenų prašymo registro įrašo forma;

Priedas Nr. 4, Sprendimo dėl IKT tikrinimo forma;

Priedas Nr. 5, Duomenų saugumo pažeidimų registro įrašo forma;

Priedas Nr. 6, Pranešimo apie duomenų saugumo pažeidimą Inspekcijai forma;

Priedas Nr. 7, Pranešimo apie duomenų saugumo pažeidimą Asmenims forma.

Priedas Nr. 8, Poveikio duomenų apsaugai vertinimo ataskaitos forma.

Priedas Nr. 9, Teisėtų interesų balanso testo forma.
