PATVIRTINTA
Utenos socialinės globos namų direktoriaus
2022-07-21 įsakymu Nr. V-45

UTENOS SOCIALINĖS GLOBOS NAMŲ INFORMACINIŲ TECHNOLOGIJŲ SAUGUMO POLITIKA

SĄVOKOS

BDAR	reiškia 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentą (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas).
Darbuotojas	reiškia Įstaigos darbuotoją.
Įstaiga	reiškia **UTENOS SOCIALINĖS GLOBOS NAMAI** Valstybės biudžetinė įstaiga Adresas: Kupiškio g. 66, 28175 Utena Duomenys kaupiami ir saugomi Juridinių asmenų registre, kodas 190797098
Direktorius	reiškia Utenos socialinės globos namų direktorius
Įrenginys	reiškia bet kokią Darbuotojui suteiktą techninę įrangą ar įrenginį.
DAP	Duomenų apsaugos pareigūnas.
Politika	reiškia šią Informacijos saugumo politiką.

I TIKSLAS IR APIMTIS

1. Šia Politika yra siekiama nustatyti bendruosius saugumo reikalavimus Įstaigos pasitelkiamoms informacinėms technologijoms bei jų panaudojimo būdams, siekiant užtikrinti maksimalų Įstaigos ir jos gyventojų, gyventojų atstovų, taip pat darbuotojų, kontrahentų bei kitų asmenų informacijos saugumą, ir apsaugoti juos nuo neteisėtų ir žalą sukeliančių tiesioginių ar netiesioginių, tyčinių ar atsitiktinių asmenų veiksmų tvarkant jiems prieinamus asmens ar kitus duomenis, taip pat naudojant atitinkamą įrangą savo darbo funkcijoms atlikti.
2. Politikos tikslas yra apsaugoti Įstaigos gyventojus, gyventojų atstovus, darbuotojus nuo neteisėtų ir žalą sukeliančių tiesioginių ar netiesioginių, tyčinių ar atsitiktinių asmenų veiksmų tvarkant jiems prieinamus asmens ar kitus duomenis, taip pat naudojant atitinkamą įrangą savo darbo funkcijoms atlikti.
3. Ši Politika yra taikoma tvarkant bet kuriose informacinėse sistemose esančią ir bet kurioje laikmenoje saugomą Įstaigos informaciją, nepriklausomai nuo to, ar šios informacijos tvarkymas yra susijęs su Įstaigos vidaus procesais, ar su Įstaigos išorės santykiais su bet kuriais trečiaisiais asmenimis.
4. Ši Politika taip pat yra taikoma Įstaigos darbuotojams jų darbo funkcijų vykdymo metu ir (ar) naudojant jiems Įstaigos suteiktą įrangą ir įrankius.
5. Ši Politika gali būti taikoma kartu su kitomis politikomis, taisyklėmis, procedūromis ar

kitais Įstaigos vidaus dokumentais.

6. Ši Politika yra taikoma ir Įstaigos vardu informaciją tvarkantiems paslaugų teikėjams (įskaitant duomenų tvarkytojus) tiek, kiek Politikos nuostatos neprieštarauja sudarytai paslaugų teikimo, duomenų tvarkymo ar kitai sutarčiai.
7. Už Politikos nurodytų reikalavimų, susijusių su Įstaigos informacinių technologijų darbo aspektais, įgyvendinimą ir priežiūrą yra atsakingas IT specialistas arba paslaugų teikėjas, su kuriuo sudaryta duomenų tvarkymo sutartis, sutartyje numatyta apimtimi; už įgyvendinimo kontrolę – Įstaigos vadovas.
8. DAP ir IT specialistas yra paskiriami Įstaigos vadovo įsakymu.

II INFORMACIJAI TVARKYTI NAUDOJAMOS SISTEMOS

9. Bet kokios informacinės sistemos, įskaitant, bet neapsiribojant, kompiuterine, serverių įranga, bet kokia programine įranga, operacinėmis sistemomis, bet kokiomis duomenų laikmenomis, tinklo paskyromis, elektroninio pašto paskyromis, paieškos sistemomis ir bet kokia kita Įstaigos veikloje naudojama technine įranga ir įrankiais, yra laikomos Įstaigos nuosavybe.
10. Kiekvienas darbuotojas jam Įstaigos suteiktus įrenginius ir įrangą privalo naudoti atsakingai bei atidžiai, ir tik su Įstaigos veikla susijusiems tikslams. Vienintelė šios taisyklės išimtis yra atvejai, kai Įstaiga, suteikdama darbuotojui įrenginį (pavyzdžiui, mobilųjį telefoną), leidžia jį naudoti ir asmeniniais tikslais.
11. Kiekvienas darbuotojui suteikiamas įrenginys yra registruojamas.

12. IT specialistas veda IT išteklių (naudojamų asmens duomenims tvarkyti) registrą (techninės, programinės ir tinklo įrangos sąrašą) (1 priedas prie Politikos). IT išteklių registras turi apimti bent tokią informaciją: IT išteklių tipą (pvz., tarnybinę stotį, kompiuterinę darbo vietą), vietą (fizinę ar elektroninę). IT išteklių registro tvarkymas priskiriamas IT specialistui.
13. IT išteklių registras turi būti reguliariai peržiūrimas ir atnaujinamas pagal poreikį, tačiau ne rečiau kaip kartą per 3 mėnesius.

III DARBUOTOJŲ PAREIGOS

14. Bet kokia informacija, prieinama darbuotojui jo darbo funkcijų vykdymo metu, bus laikoma konfidencialia ir saugoma laikantis šios Politikos nuostatų. Informacija negali būti atskleidžiama jokiems kokioms tretiesiems asmenims, išskyrus atvejus, kai toks atskleidimas yra būtinas su Įstaigos veikla susijusiems tikslams ir ją gaunantys tretieji asmenys įsipareigoja užtikrinti tokios informacijos konfidencialumą. Darbuotojai, dirbantys su tokia informacija, turi laikytis konfidencialumo principo ir laikyti ją paslaptyje. Šios pareigos lieka galioti ir perėjus dirbti į kitas pareigas Įstaigoje, taip pat pasibaigus darbo ar kitiems sutartiniams santykiams su Įstaiga.
15. Visi fizinių asmenų prašymai, susiję su asmens duomenimis ir (ar) jų tvarkymu, kuriuos Įstaigos darbuotojas gauna vykdydamas savo darbo funkcijas, turi būti nedelsiant perduodami vadovaujantis *Utenos socialinės globos namų darbuotojų ir gyventojų asmens duomenų tvarkymo taisyklėmis*.
16. Tais atvejais, kai jungdamiesi prie Įstaigos informacinių sistemų ar prieigai kitų išteklių (pvz., jungdamiesi prie darbinio elektroninio pašto, Įstaigai priklausančių ar jos naudojamų duomenų bazių), darbuotojai naudoja asmeninius įrenginius ar įrangą, jie privalo laikytis šios Politikos nuostatų taip pat, kaip ir naudodamiesi Įstaigos suteiktais įrenginiais ar įranga. Atitinkamai draudžiama yra saugoti bet kokius su Įstaigos veikla susijusius duomenis ir informaciją savo asmeniniame įrenginyje ar įrangoje; bet koks Įstaigos

duomenų tvarkymas ir saugojimas yra galimas tik per Įstaigai priklausančiose ar jos naudojamose informacinėse sistemose ir saugyklose.

17. Kiekvienas darbuotojas privalo laikytis šios Politikos, taikytinų teisės aktų bei Įstaigos vidaus dokumentų ar lokalinių teisės aktų, kurie nustato informacijos tvarkymo ir saugumo reikalavimus.

IV PRIEIGŲ VALDYMAS IR INFORMACIJOS APSAUGA

18. Bet kokie įrenginiai bei informacija darbuotojams yra pasiekiami priklausomai nuo jų darbo funkcijų pobūdžio, turimų atsakomybių ir griežtai vadovaujantis principu „būtina žinoti“. Prieiga prie konkrečios Įstaigos informacinės sistemos nereiškia, kad darbuotojas yra įgaliotas peržiūrėti ir naudoti visą ir bet kurią toje sistemoje esančią informaciją.
19. Darbuotojai, kurių kompiuteriuose saugomi gyventojų, kitų asmenų duomenys, arba iš kurių kompiuterių galima prisijungti prie Įstaigos informacinių sistemų, kuriose yra saugomi gyventojų, kitų asmenų duomenys, savo kompiuterius turi apsaugoti slaptažodžiais; „svečio“ (angl. *guest*) tipo, t. y. neapsaugotos slaptažodžiais, vartotojų paskyros yra draudžiamos.
Šiuose kompiuteriuose taip pat turi būti nustatytas sesijos laikas (t. y. naudotojui esant neaktyviam tam tikrą laiką (pavyzdžiui, 15 min.), jo sesija turi būti nutraukta).
20. Darbuotojas yra atsakingas už visus veiksmus, atliekamus naudojantis jam priskirta paskyra. Kiekvienas darbuotojas privalo užtikrinti, kad jo paskyrų duomenys (slaptažodžiai) nebūtų prieinami jokiems tretiesiems asmenims, įskaitant kitus Įstaigos darbuotojus.
21. Prieigas prie informacinių sistemų apsaugantys slaptažodžiai turi būti sudaromi atsakingai (jie negali būti lengvai atspėjami) ir reguliariai keičiami (ne rečiau kaip kartą per 3 mėnesius). Kiekvienas darbuotojas yra asmeniškai atsakingas už savo naudojamų slaptažodžių atitiktį šios Politikos nuostatoms ir bet kokioms kitoms Įstaigos taisyklėms. Slaptažodžiams keliami šie reikalavimai:
21.1. slaptažodis turi būti sudarytas iš mažiausiai 8 simbolių, iš kurių bent vienas turi būti skaičius ir bent vienas turi būti raidė;
21.2. slaptažodis negali sutapti su darbuotojo ar jo šeimos narių asmeniniais duomenimis;
21.3. slaptažodį saugo ir jį gali žinoti tik darbuotojai, dirbantys su konkrečių kompiuterių ar sistema;
21.4. slaptažodžiai negali būti pasiekiami kitiems asmenims (pvz., užrašomi ant lapelių ir pan. lipdukami darbo vietose).
22. Darbuotojas gali susipažinti su konfidencialia informacija tik tuo atveju, jeigu jis turi atitinkamus įgaliojimus pagal darbo sutartį ir (ar) jam tokius įgaliojimus suteikė Įstaiga.
23. Darbuotojai, atliekantys asmens duomenų tvarkymą, turi užkirsti kelią bet kokiam atsitiktiniam ar neteisėtam duomenų tvarkymui, tinkamai bei atsakingai saugoti dokumentus (vengti nereikalingų dokumentų kopijų su asmens duomenimis laikymo ir kt.). Dokumentų, kuriuose yra asmens duomenų, kopijos turi būti sunaikinamos tokiu būdu, kad šių dokumentų ir jų turinio nebūtų galima atkurti.
24. Nesant būtinybės, rinkmenos su gyventojų, kitų asmenų duomenimis neturi būti dauginamos skaitmeniniu būdu, t. y. neturi būti daromos rinkmenų kopijos, saugomos kompiuterių kietuosiuose diskuose, nešiojamose laikmenose, nuotolinėse rinkmenų talpyklose ir kt.
25. Įstaigos darbuotojai privalo taip organizuoti savo darbą, kad kiek įmanoma būtų apribota galimybė kitiems asmenims (kitiems Įstaigos darbuotojams, paslaugų teikėjams ir kitiems tretiesiems asmenims) susipažinti su jų tvarkomais asmens duomenimis. Tai įgyvendinama:
25.1. naudojant dokumentų su asmens duomenimis ir įrenginių, kuriais naudojantis galima susipažinti su asmens duomenimis, be priežiūros tokiu būdu, kad juose esančią informaciją

gi ų perskaityti darbuotojai, neturintys teisės dirbti su konkrečiais asmens duomenimis, ir ti tretieji asmenys;

25.2. d mentus laikant taip, kad jų (ar jų fragmentų) negalėtų perskaityti atsitiktiniai tretieji a nys;

25.3. j dokumentai, kuriuose yra asmens duomenų, jų gavėjams perduodami per asmenis, n rinčius teisės tvarkyti tokius asmens duomenis, arba paštu ar per kurjerį, jie turi būti s čiami užklijuotame nepermatomame voke.

26. D uotojai gali perduoti dokumentus, kuriuose yra asmens duomenų, tik tiems d uotojams, kurie pagal savo pareigas ar atskirus pavedimus turi teisę susipažinti su tais a ns duomenimis.

27. D uotojo prieigos teisės prie Įstaigos informacinės sistemos ar kitų išteklių turi būti n lsiant panaikinamos, kai išnyksta pagrindas ar poreikis naudotis ta sistema ir (ar) t yti joje esančius duomenis (pvz., pasibaigus darbo santykiams arba pasikeitus d uotojo pareigoms ar darbo funkcijoms):

V TECHNINĖS SAUGUMO PRIEMONĖS

28. V ems bet kokiu būdu surinktiems ir tvarkomiems bet kokios formos (popierinės, e roninės, kt.) duomenims ir informacijai yra taikomi šios Politikos ir atitinkamų teisės a reikalavimai dėl informacijos rinkimo, tvarkymo, apsaugos ir tolesnio saugojimo; t duomenys ir informacija saugiai laikomi Įstaigos nustatytose vietose, laikantis t tinuose teisės aktuose ir Įstaigos vidaus dokumentuose nustatytų terminų.

29. A ens duomenų, esančių išorinėse duomenų laikmenose ir elektroniniame pašte, s umo kontrolė ir jų savalaikis ištrynimas užtikrinami perkeliant juos į atitinkamas i macines sistemas.

30. V duomenų pakeitimai Įstaigos informacinėse sistemose yra stebimi ir registruojami IT s ialisto.

31. K vienos informacinės sistemos, naudojamos asmens duomenų tvarkymui, atžvilgiu yra į endinama tokia kontrolė bei stebėsena:

31.1. F uojami šie techninių žurnalų įrašai apie prieigą prie asmens duomenų: asmens d nenys, prie kurių buvo prieita, su asmens duomenimis atlikti veiksmai (įvedimas, p iūra, keitimas, naikinimas ir kiti asmens duomenų tvarkymo veiksmai). Šie įrašai turi b saugomi ne trumpiau kaip 1 (vienerius metus).

31.2. T minių žurnalų įrašai 1 (vieną) kartą per metus (taip pat iškilus poreikiui) peržiūrimi ir (teikiamos jų peržiūros ataskaitos duomenų apsaugos pareigūnui ir įstaigos vadovui.

32. Į gos įrenginiai bei informacinės sistemos yra tinkamai apsaugoti techninėmis bei o nizacinėmis priemonėmis, siekiant išvengti neleistinos prieigos.

33. K prie Įstaigos informacinių sistemų yra jungiamasi internetu (per nuotolį), yra n ojami saugūs, šifruoti komunikacijos kanalai. Perduodant asmens duomenis išoriniais d menų perdavimo tinklais, yra užtikrinamas saugių protokolų ir (arba) slaptažodžių n ojimas.

34. D uotojų kompiuteriai, kuriuose saugomos rinkmenos su gyventojų, kitų fizinių asmenų d menimis, negali būti laisvai prieinami iš kitų tinklo kompiuterių.

35. J u Įstaigos duomenims pasiekti yra naudojami įvairūs nuotoliniai įrenginiai, d uotojas privalo įsitikinti, kad naudojamas interneto ryšys yra saugus ir patikimas. Į gos duomenims pasiekti negali būti naudojamas viešas, neapsaugotas interneto ryšys. M biliuosiuose įrenginiuose (nešiojamuose kompiuteriuose, planšetėse, išmaniuosiuose t fonuose ir pan.), jeigu jie naudojami ne Įstaigos vidiniame kompiuterių tinkle, esantys s cialių kategorijų asmens duomenys ir prisijungimo prie Įstaigos informacinių sistemų d menys turi būti šifruojami arba apsaugomi kitomis priemonėmis, kurios atitiktų esamas r kas.

36. Į staigos įrenginius bei įrangą gali būti diegiamos ir juose naudojamos tik Įstaigos

naudojamos informacinės sistemos ir tinkamai licencijuota programinė įranga.

37. Įstaigos įrenginiai bei įranga yra tinkamai apsaugoti antivirusine ir (ar) kitokia programine įranga, skirta apsisaugoti nuo kenkėjiškos programinės įrangos.
38. Įstaigos naudojama programinė įranga, įskaitant operacines sistemas, yra nuolat atnaujinama pagal tiekėjų rekomendacijas.
39. Visi esminiai IT sistemų keitimai turi būti stebimi ir registruojami IT specialisto.
40. Visi atvejais esminiai IT sistemų keitimai privalo būti derinami su IT specialistu.
41. IT specialistas atsakingas už IT sistemų keitimo procedūros dokumentavimą.
42. Siekiant užtikrinti įstaigos duomenų atkuriamumą, nuolat daromos informacijos atsarginės kopijos, laikantis gerųjų rinkos praktikų:
42.1. atsarginės duomenų kopijos, jei jos daromos, saugomos kitoje geografinėje vietoje, negu aktyviai naudojamos informacinės sistemos duomenys;
42.2. atsarginės kopijos, archyvuose ir išorinėse duomenų laikmenose saugomi duomenys yra šifruojami.
43. Elektroniniu paštu perduodami asmens duomenys turi būti šifruojami.
44. Kai Įstaigos saugoma informacija tampa nebereikalinga vykdant Įstaigos veiklą, tokia informacija ištrinama, visos jos kopijos sunaikinamos, o su šios informacijos tvarkymu susiję darbuotojai atitinkamai informuojami apie jų pareigą ištrinti, sunaikinti ir (ar) grąžinti Įstaigai visą informaciją, kurios jiems nebereikia vykdant darbo funkcijas (visų pirma, grąžinti Įstaigai, ištrinti arba sunaikinti duomenų kopijas tuo atveju, kai nutrūksta darbo santykiai su darbuotoju).
45. Patekimas į patalpas, kuriose laikomi Įstaigos įrenginiai bei įranga, įskaitant serverių patalpas, yra kontroliuojamas fizinėmis, elektroninėmis ar kitokiomis apsaugos priemonėmis (durų rakinimo sistema, bendra apsaugos signalizacijos sistema, kt.), kurios užtikrina, kad jokie pašaliniai, neįgalioti asmenys į tas patalpas negalėtų patekti.
46. Siekiant užtikrinti šios Politikos reikalavimų laikymąsi bei įvertinti, ar naudojamos saugumo priemonės yra pakankamos, yra atliekamas informacinėse sistemose atliekamo duomenų tvarkymo keliamos rizikos vertinimas, kuris būtų atliekamas kartą per 1 (vienerius) metus, IT specialistui bei atsakingiems Įstaigos administracijos darbuotojams užpildant „Asmens duomenų tvarkymo saugumo patikrinimo kontrolinis klausimyną“ (2 priedas prie Politikos);

VI DRAUDŽIAMI VEIKSMAI

47. Išskyrus konkrečiai nustatytas išimtis, jokiais atvejais ir jokiomis aplinkybėmis Įstaigai priklausantys įrenginiai, sistemos ir įrankiai negali būti naudojami su darbuotojų darbo funkcijomis ar Įstaigos veikla nesusijusiems tikslams.
48. Jokia šioje Politikoje nurodyta informacija negali būti siunčiama, perduodama arba bet kokiu kitu būdu atskleidžiama trečiajam asmeniui, nebent tai būtina darbuotojo darbo funkcijoms vykdyti ir tik tokia apimtimi, kokia reikalinga darbo funkcijų vykdymui. Duomenų perdavimo ar kitokio atskleidimo tretiesiems asmenims atveju turi būti užtikrinama, kad duomenys yra perduodami naudojant saugias priemones ir (ar) imamasi kitų reikiamų saugumo priemonių.
49. Darbuotojams neleidžiama savo įrenginiuose laikyti Įstaigos asmens duomenis (visų pirma, gyventojų duomenis) ar bet kokią kitą konfidencialią informaciją.
50. Žemiau nurodyti veiksmai yra griežtai draudžiami, nenumatant jokių išimčių:
50.1. bet kokių fizinio ar juridinio asmens intelektinės nuosavybės teisių pažeidimas, įskaitant, bet neapsiribojant, bet kokios nelegalios programinės įrangos, virtualių platformų ar kito Įstaigai nelicencijuoto skaitmeninio turinio įdiegimu, kopijavimu, platinimu ar saugojimu Įstaigos sistemose, įrangoje ar įrenginiuose.
50.2. Neleistėtas autorių teisėmis saugomos medžiagos kopijavimas.

50.3. Bet kurio asmens teisių pažeidimas dėl perteklinio ir nereikalingojo asmens duomenų rinkimo ir tvarkymo.

50.4. Priėjimas prie Įstaigos duomenų, serverio, sistemos, bet kokio įrenginio ar įrangos, prisijungimas ar pasinaudojimas paskyra kitais tikslais nei Įstaigos veiklos užtikrinimas ar konkretaus darbuotojo darbo funkcijų vykdymas.

50.5. Įstaigai priklausančios ir (ar) kitos konfidencialios informacijos ar duomenų eksportas, jeigu toks eksportas nėra reikalingas Įstaigos veiklai užtikrinti ar darbuotojo darbo funkcijoms vykdyti, ir (ar) atliekamas pažeidžiant taikytinus teisės aktus ar Įstaigos vidaus dokumentus.

50.6. Darbuotojo paskyros slaptažodžio atskleidimas kitam asmeniui ir (ar) leidimas kitam asmeniui naudotis tokia darbuotojo paskyra (įskaitant, bet neapsiribojant, darbuotojo šeimos nariais).

50.7. Apgaulingi ir (ar) neteisėti produktų ar paslaugų pasiūlymai, naudojantis Įstaigos suteikta paskyra, sistema ar įrenginiais.

50.8. Saugumo pažeidimai arba tinklo sutrikdymas. Tokie saugumo pažeidimai apima, bet neapsiriboja, prieiga prie duomenų, kurie nėra skirti darbuotojui, arba prisijungimu prie serverio ar paskyros, darbuotojui neturint atitinkamų įgaliojimų (nebent prieigos teisės darbuotojui būtų suteiktos dėl jo dalyvavimo konkrečiame Įstaigos projekte).

50.9. Visais atvejais griežtai draudžiama naudotis viešais prieigos įrenginiais (pavyzdžiui, bibliotekose, kt.). Jeigu suteiktomis darbo priemonėmis naudojamasi viešose vietose, darbuotojai privalo dėti pastangas, kad jų įrenginio ekranas nebūtų matomas, stebimas ar įrašinėjamas pašalinių asmenų, taip pat nebūtų jungiamasi, naudojamasi viešu, nesaugiu, belaidžiu interneto ryšiu (*Wi-Fi*).

VII PRANEŠIMAS APIE SAUGUMO INCIDENTUS

51. Apie visus informacijos saugumo incidentus turi būti nedelsiant pranešta IT specialistui, DAP ir (ar) Įstaigos vadovui, kurie atitinkamai imasi priemonių galimai žalai išvengti, kilusiai žalai pašalinti ir buvusiai saugumo būklei atkurti.

52. Visi su asmens duomenimis susiję saugumo incidentai yra valdomi vadovaujantis Utenos socialinės globos namų Asmens duomenų saugumo pažeidimų valdymo politika.

53. Kai tai yra būtina, Įstaigos vadovas privalo užtikrinti, kad apie informacijos saugumo pažeidimus būtų pranešta kompetentingoms valdžios institucijoms ir (ar) kitiems asmenims, kaip tai numatyta taikytinuose teisės aktuose ir (ar) Įstaigos vidaus dokumentuose.

54. Už visų šioje Politikoje nurodytų saugumo priemonių įgyvendinimą yra atsakingi Įstaigos darbuotojai pagal kompetenciją ir (ar), kai taikytina, jos pasitelkti paslaugų teikėjai.

VIII KITOS NUOSTATOS

55. DAP organizuoja darbuotojų, kuriems suteikti įgaliojimai tvarkyti asmens duomenis, mokymus. Už tokių mokymų vykdymo kontrolę yra atsakingas Įstaigos vadovas.

56. Už Politikos laikymosi priežiūrą ir jos nuostatų įgyvendinimo kontrolę, Politikos nuostatų peržiūrą ne rečiau kaip kartą per 2 metus, taip pat, esant poreikiui, Politikos atnaujinimą yra atsakingas IT specialistas.

1 priedas

Utenos socialinės globos namų IT išteklių registras

Įrangos tipas	Inventorinis Nr.	Įrangos pavadinimas	Eksploatacijos pradžia	Kur pastatyta	Naudotojas	Kiekis	Kaina	Programinė įranga

2 priedas

ASMENS DUOMENŲ TVARKYMO SAUGUMO PATIKRINIMO KONTROLINIS KLAUSIMYNAS

20 m. _____ d.
(klausimyno pildymo data)

I. BENDROJI DALIS

Duomenų valdytojo pavadinimas	
Buveinės adresas	
Kontaktai (el. pašto adresas, telefono ryšio Nr.)	
Duomenų valdytojo veiklos pobūdis	

II. SPECIALIOJI DALIS

Organizacinės saugumo priemonės
(Atitinkamas grafas pildo Įstaigos administracijos darbuotojas pagal kompetenciją)

Asmens duomenų saugumo politika ir procedūros		
1.	Ar asmens duomenų ir jų tvarkymo saugumas Įstaigoje yra dokumentuotas kaip informacijos saugumo politikos dalis?	
2.	Ar saugumo politika peržiūrima ir prireikus atnaujinama? Kokiu dažnumu tai daroma?	
Vaidmenys ir atsakomybės		
3.	Ar su asmens duomenų tvarkymu susiję vaidmenys ir atsakomybės aiškiai apibrėžti ir paskirstyti pagal saugumo politiką?	
4.	Ar Įstaigoje numatytas ir aiškiai apibrėžtas darbuotojų teisių ir pareigų atšaukimas taikant atitinkamas vaidmenų ir atsakomybių perdavimo procedūras (vidaus organizacijos pertvarkymo ar darbuotojų atleidimo, funkcijų pasikeitimo metu)?	
Prieigos valdymo politika		
5.	Ar Įstaigoje kiekvienam vaidmeniui, susijusiam su asmens duomenų tvarkymu, yra priskiriamos konkrečios prieigos kontrolės teisės, vadovaujantis principu „būtinybė žinoti“ (angl. need to know)? Kokiame dokumente ar informacinių techno-logijų (IT) sistemoje tai numatyta?	
Išteklių ir turto valdymas		

6.	Ar Įstaiga turi IT išteklių, naudojamų asmens duomenims tvarkyti, registrą (techninės, programinės ir tinklo įrangos)? Ar registro tvarkymas priskirtas konkrečiam asmeniui, pvz., IT specialistui?	
7.	Ar IT išteklių registro tvarkymas priskirtas konkrečiam asmeniui, pvz., IT specialistui?	
8.	Ar IT išteklių registras reguliariai peržiūrimas ir atnaujinamas? Kokiu dažnumu?	
Pakeitimų valdymas		
9.	Ar visi Įstaigos IT sistemų pakeitimai stebimi ir registruojami konkretaus asmens (pvz., IT specialisto)?	
10.	Ar Įstaigoje naudojamos programinės įrangos kūrimas atliekamas specialioje aplinkoje, kuri nėra prijungta prie IT sistemų, naudojamų tvarkant asmens duomenis. Ar testuojant sistemas naudojami testiniai (ne realūs) duomenys?	
Duomenų tvarkytojai		
11.	Ar su Įstaigos tvarkomų duomenų tvarkytojais apibrėžtos, dokumentuotos ir suderintos formalios gairės ir procedūros, taikomos duomenų tvarkytojams (rangovams / užsakomųjų paslaugų teikėjams) dėl asmens duomenų tvarkymo? Ar šios gairės ir procedūros nustato tokį patį asmens duomenų saugumo lygį, koks yra numatytas Įstaigos saugumo politikoje?	
12.	Ar sutartyse su duomenų tvarkytojas numatyta prievolė nepagrįstai nedelsiant pranešti duomenų valdytojui apie nustatytus asmens duomenų saugumo pažeidimus?	
13.	Ar duomenų tvarkytojai yra pateikę dokumentais pagrįstus įrodymus dėl atitikties keliamiems reikalavimams?	
Asmens duomenų saugumo pažeidimai ir incidentai		
14.	Ar Įstaigoje yra parengta išsami reagavimo į incidentus ir jų padarinių likvidavimo tvarka (reagavimo į incidentus planas), užtikrinanti veiksmingą incidentų, susijusių su asmens duomenų saugumo pažeidimais, valdymą?	

15.	Ar Įstaigoje nustatyta pranešimo apie asmens duomenų saugumo pažeidimus kompetentingoms institucijoms ir duomenų subjektams tvarka, vadovaujantis Bendrojo duomenų apsaugos reglamento (BDAR) 33 ir 34 straipsniais?	
Veiklos tęstinumas		
16.	Ar Įstaiga nusistačiusi pagrindines procedūras, kurių reikia laikytis incidento / asmens duomenų saugumo pažeidimo atveju, kad būtų užtikrintas reikiamas asmens duomenų tvarkymo IT sistemomis tęstinumas ir prieinamumas?	
Personalo konfidencialumas		
17.	Ar Įstaigoje vaidmenys ir atsakomybės aiškiai išdėstyti darbuotojui prieš pradedant vykdyti jam paskirtas funkcijas ir darbus?	
Mokymai		
18.	Ar Įstaiga užtikrina, kad visi darbuotojai būtų tinkamai informuoti apie IT sistemų saugumo reikalavimus, susijusius su jų kasdieniu darbu?	
19.	Ar darbuotojai, susiję su asmens duomenų tvarkymu, mokomi apie atitinkamų duomenų apsaugos reikalavimus ir atsakomybę, rengiant reguliarius mokymus, informavimo renginius/instruktažus? Kokiu dažnumu vyksta mokymai?	

Techninės saugumo priemonės

Prieigų kontrolė ir autentifikavimas		
20.	Ar Įstaigoje įdiegta / įgyvendinta Prieigų kontrolės sistema, kuri taikoma visiems IT sistemos naudotojams? (Prieigų kontrolės sistema turi leisti kurti, patvirtinti, peržiūrėti ir panaikinti naudotojų paskyras)	
21.	Ar Įstaigoje naudojamos bendros naudotojų paskyros? Jeigu taip, ar visi bendros paskyros naudotojai turi tokias pačias teises ir pareigas?	
22.	Ar Įstaigoje yra veikiantis autentifikavimo mechanizmas, leidžiantis prieigas prie IT sistemų (paremtas Prieigų kontrolės politika)? Ar Įstaiga užtikrina minimalų reikalavimą naudotojui prisijungti prie	

	IT sistemos naudotojo prisijungimo vardu ir slaptažodžiu? Ar slaptažodžiai sudaromi atsižvelgiant į tam tikrą kompleksiškumo lygį? Kokios slaptažodžio taisyklės?	
23.	Ar Prieigų kontrolės sistema turi galimybę aptikti ir neleisti naudoti slaptažodžių, kurie neatitinka tam tikro kompleksiškumo lygio?	
Techninių žurnalų įrašai ir stebėsena		
24.	Ar techninių žurnalų įrašai įgyvendinti kiekvienai IT sistemai / taikomajai programai, naudojamai asmens duomenų apdorojimui? Ar techniniuose žurnaluose matomi bent šie prieigų prie asmens duomenų įrašų tipai: data, laikas, peržiūrėjimas, keitimas, panaikinimas? Koks šių įrašų saugojimo terminas?	
25.	Ar techninių žurnalų įrašai turi laiko žymas ir ar jie apsaugoti nuo galimo sugadinimo, suklastojimo ar neautorizuotos prieigos? Ar IT sistemose naudojami laiko apskaitos mechanizmai sinchronizuoti pagal bendrą laiko atskaitos šaltinį?	
Tarnybinių stočių / duomenų bazių apsauga		
26.	Ar Įstaigos duomenų bazės ir taikomųjų programų tarnybinės stotys sukonfigūruotos taip, kad veiktų korektiškai ir naudotų atskirą paskyrą su priskirtomis žemiausiomis operacinės sistemos privilegijomis?	
27.	Ar duomenų bazės ir taikomųjų programų tarnybinės stotys apdoroja tik tuos asmens duomenis, kurie yra reikalingi darbui, atitinkančiam duomenų tvarkymo tikslus?	
Darbo stočių apsauga		
28.	Ar Įstaigoje užtikrinta, kad naudotojai neturėtų galimybės išjungti ar apeiti / išvengti saugos nustatymų?	
29.	Kokios antivirusinės taikomosios programos naudojamos Įstaigos darbo vietose? Kaip dažnai atnaujinamos šių programų virusų duomenų bazės?	
30.	Ar darbo vietose užtikrinta, kad naudotojai neturėtų privilegijų diegti, šalinti, administruoti neautorizuotos programinės įrangos?	
31.	Ar IT sistemose (įskaitant darbo vietų operacines sistemas) nustatytas sesijos	

	laikas (naudotojui esant neaktyviam sistemoje nustatytą laiką, jo sesija nutraukiama)? Jeigu taip, koks nustatytas neaktyvios sesijos laikas?	
32.	Ar kritiniai operacinių sistemų saugos atnaujinimai diegiami reguliariai ir nedelsiant?	
	Tinklo / komunikacijos sauga	
33.	Kai prieiga prie naudojamų IT sistemų yra vykdoma internetu ar naudojami šifruoti komunikacijos kanalai, t. y. kriptografiniai protokolai (pvz., TLS/SSL)?	
	Atsarginės kopijos	
34.	Ar Įstaigos atsarginės kopijos ir duomenų atstatymo procedūros apibrėžtos, dokumentuotos ir aiškiai susaistytos su vaidmenimis ir pareigomis?	
35.	Ar atsarginių kopijų laikmenoms užtikrintas tinkamas fizinis aplinkos / patalpų saugos lygis?	
36.	Ar atsarginių kopijų darymo procesas stebimas, siekiant užtikrinti užbaigtumą / išsamumą?	
37.	Ar pilnos atsarginės duomenų kopijos daromos reguliariai? Jei taip, tai kokiu dažnumu daromos pilnos ir/ar pridedamosios kopijos?	
	Mobilūs / nešiojami įrenginiai	
38.	Ar Įstaigoje nustatytos ir dokumentuotos mobilių ir nešiojamų įrenginių administravimo procedūros, aiškiai aprašant tinkamą tokių įrenginių naudojimąsi?	
39.	Ar mobilūs / nešiojami įrenginiai, kuriais naudojamasi darbui su informacinėmis sistemomis, prieš naudojimąsi užregistruojami ir autorizuojami?	
40.	Ar mobilūs įrenginiai yra pakankamame prieigos kontrolės procedūrų lygyje kaip ir kita naudojama įranga asmens duomenų tvarkymui?	
	Programinės įrangos sauga	
41.	Ar informacinėse sistemose naudojama programinė įranga (asmens duomenims tvarkyti) atitinka programinės įrangos saugos gerąsias praktikas, programinės įrangos kūrime taikomas saugos gerąsias praktikas, programinės įrangos kūrimo struktūras (angl. *frameworks*),	

	standartus?	
42.	Ar specifiniai saugos reikalavimai buvo apibrėžti pradiniuose programinės įrangos kūrimo etapuose?	
43.	Ar Įstaigoje laikomasi duomenų saugą užtikrinančių programavimo standartų ir gerųjų praktikų? Jei taip, tai kokių?	
44.	Ar programinės įrangos kūrimo, testavimo ir verifikacijos etapai vyksta atsižvelgiant į pagrindinius saugos reikalavimus?	
Duomenų naikinimas / šalinimas		
45.	Ar Įstaigoje prieš pašalinant bet kokią duomenų laikmeną visi joje esantys duomenys sunaikinami naudojant tam skirtą programinę įrangą, kuri palaiko patikimus duomenų naikinimo algoritmus? Tais atvejais, kai tai padaryti neįmanoma (pvz., CD/DVD diskai, ir pan.) ar vykdomas fizinis duomenų laikmenos sunaikinimas be galimybės atstatyti?	
46.	Ar popierius ir nešiojamos duomenų laikmenos, kuriuose buvo saugomi / kaupiami asmens duomenys, naikinami tam skirtais smulkintuvais?	
Fizinė sauga		
47.	Ar Įstaigoje įgyvendinta fizinė aplinkos / patalpų, kuriose yra IT sistemų infrastruktūra, apsauga nuo neautorizuotos prieigos?	

Patvirtinu, kad visa šiame klausimyne pateikta informacija yra tiksli ir teisinga:

_____ _____ _____

(pareigos) *(parašas)* *(vardas, pavardė)*

IT specialistas

_____ _____

(parašas) *(vardas, pavardė)*

Duomenų apsaugos pareigūnas

_____ _____

(parašas) *(vardas, pavardė)*