PATVIRTINTA
VšĮ Utenos verslo informacijos centro
Direktoriaus 2022-02-04 Įsakymu Nr. V1-143

ASMENS DUOMENŲ TVARKYMO POLITIKA

1. BENDROSIOS NUOSTATOS

1.1. Asmens duomenų tvarkymo politika (toliau – *Politika*) reglamentuoja *VšĮ Utenos verslo informacijos centro*, juridinio asmens kodas 300056112 (toliau – Įstaiga), asmens duomenų tvarkymą užtikrinant 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 (Bendrasis duomenų apsaugos reglamentas), Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo (toliau – ADTAĮ) ir kitų teisės aktų, nustatančių asmens duomenų tvarkymą ir apsaugą, nuostatų laikymąsi ir įgyvendinimą.

1.2. Politikos paskirtis – numatyti pagrindines asmens duomenų tvarkymo ir asmens duomenų saugos organizacines ir technines priemones.

1.3. Politikos privalo laikytis visi Įstaigos darbuotojai, dirbantys pagal darbo sutartis, praktikantai, atliekantys praktiką Įstaigoje (toliau – darbuotojas), taip pat kiti asmenys, kurie, tvarkydami asmens duomenis Įstaigoje eidami savo pareigas, sužino asmens duomenis arba turi bet kokio pobūdžio prieigą prie asmens duomenų.

1.4. Įstaigos vadovo paskirtas darbuotojas yra atsakingas už Politikos įgyvendinimo priežiūrą. Asmens, atsakingo už Politikos įgyvendinimo priežiūrą, paskyrimas nepanaikina kiekvieno darbuotojo, kuris tvarko asmens duomenis, eidamas savo pareigas, juos sužino arba turi bet kokio pobūdžio prieigą prie asmens duomenų, pareigos ir atsakomybės už Politikos laikymąsi ir įgyvendinimą bei asmens duomenų tvarkymo teisėtumą.

2. TAIKYMO SRITIS IR ADRESAI

2.1. Ši politika taikoma:

2.1.1. Duomenų rinkimui, naudojimui ir saugojimui *Įstaigos* vardu.

2.1.2. Duomenų tvarkomų Įstaigoje rinkimui, naudojimui ir saugojimui.

2.1.3. Darbuotojų darbo funkcijų tikslu vykdomam Duomenų rinkimui, naudojimui ir saugojimui.

2.1.4. Duomenų rinkimui, naudojimui ir saugojimui naudojant informacines ir komunikacines technologijas.

2.1.5 Politika skirta visiems Įstaigos darbuotojams. Atskiruose Politikos skyriuose numatytos atsakomybės, aktualios tik tam tikras pareigas einantiems Darbuotojams.

2.1.6. Įstaiga įsipareigoja su šiomis taisyklėmis supažindinti visus darbuotojus, užtikrinti, kad Darbuotojas susipažino ir suprato savo įsipareigojimus. Pasirašydamas šią Politiką patvirtina, kad laikysis jose nustatytų, jam keliamų įpareigojimų.

3. SĄVOKOS

3.1. Jei, šioje Politikoje ir jos prieduose aiškiai nenurodyta kitaip, pirmąja, didžiąja raide rašomos sąvokos turi reikšmes, nurodytas žemiau:

Duomenys – bet kokia informacija apie fizinį asmenį, kurio tapatybė nustatyta arba kurio tapatybę galima nustatyti.

Ypatingi duomenys – Asmens duomenų apsaugos aktuose nurodyti duomenys, kurių tvarkymui keliami padidinti reikalavimai (pvz. duomenys atskleidžiantys rasinę ar etninę kilmę, politines pažiūras, religinius, filosofinius įsitikinimus ar narystę profesinėje sąjungoje, sveikatos duomenys arba duomenys apie fizinio asmens lytinį gyvenimą ir lytinę orientaciją, genetiniai, biometriniai identifikatoriai, duomenys apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas).

Asmuo - Duomenų subjektas, kurio asmens duomenys renkami, naudojami ir saugomi Įstaigoje ir kurio tapatybę galima nustatyti, įskaitant, bet neapsiribojant darbuotojais.

Įstaiga – VšĮ Utenos verslo informacijos centras, juridinio asmens kodas 300056112, atsakinga už Duomenų rinkimą, naudojimą ir saugojimą, asmens duomenų apsaugos teisės aktų laikymąsi, kuriuose apibrėžiama kaip duomenų valdytojas arba duomenų tvarkytojas, atsižvelgiant į konkrečių Duomenų tvarkymą savo arba savo klientų interesais.

Darbuotojas – bet kuris Įstaigos darbuotojas, turintis tiesioginę ar netiesioginę prieigą prie duomenų.

Įgaliotas asmuo – Įstaigos skiriamas duomenų apsaugos pareigūnas (DAP), padedantis užtikrinti teisinę atitiktį, asmens duomenų apsaugos teisės aktams, priimanti sprendimus ir konsultuojantis duomenų apsaugos srityje, o jei toks nepaskirtas, vadovybė.

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

Duomenų saugumo pažeidimas – (1) Įstaigos informacinių, komunikacinių technologijų, Dokumentų ir (arba) kitų priemonių, kuriose yra Duomenys, praradimas, vagystė arba neplanuotas sunaikinimas. (2) Atsitiktinis ar tyčinis Dokumentų siuntimas, įkėlimas ar dalinimasis su trečiaisiais asmenimis, neturinčiais teisės jų gauti. (3) Trečiųjų asmenų neteisėta prieiga prie Įstaigos informacinių, komunikacinių technologijų, dokumentų ir (ar) kitų priemonių , kuriose yra

Duomenų. (4) Klaidos, susijusios su kuriamomis, naudojamomis ir konfigūruojamomis informacinėmis, komunikacinėmis technologijomis ir (ar) kitomis priemonėmis, kurios gali kelti pavojų duomenų saugumui. (5) Bet kokie kiti saugumo pažeidimai, lemiantys atsitiktinį ar neteisėtą Duomenų sunaikinimą, praradimą, nutekinimą, pakeitimą, neleistiną atskleidimą arba prieigos prie Įstaigaiį perduodamų, saugojamų ar kitaip, renkamų, naudojamų ar saugojamų Duomenų suteikimą.

Paslaugų teikėjas – Konkretus paslaugos teikėjas ar kitas išorės juridinis ar fizinis asmuo, kuris turi prieigą prie Įstaigos duomenų ir juos tvarko pagal Įstaigos nurodymus.

Politika – Ši, atitikties asmens duomenų apsaugos politika.

3.2. Kitos, šioje Politikoje neapibrėžtos sąvokos suprantamos taip, kaip jos apibrėžtos asmens duomenų apsaugos aktuose.

4. DUOMENŲ TVARKYMO PRINCIPAI

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

4.1.1. tvarkomi teisėtai, sąžiningai ir skaidriai;

4.1.2. renkami nustatytais, aiškiai apibrėžtais tikslais;

4.1.3. adekvatūs, tokie, kokių reikia siekiant tikslų, dėl kurių jei tvarkomi.

4.1.4. renkami, naudojami ir saugomi užtikrinant Duomenų apsaugą nuo neteisėtos prieigos, neteisėto rinkimo, naudojimo ir saugojimo, netyčinio praradimo, sunaikinimo ar sugadinimo;

4.1.5. tikslūs, esant poreikiui atnaujinami;

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

4.1.7. tvarkomi tokiu būdu, kad taikant atitinkamas technines ir organizacines priemones, būtų užtikrintas tinkamas asmens duomenų saugumas ir konfidencialumas, įskaitant prieigos prie Duomenų suteikimą tik tiems darbuotojams, kuriems jos reikia, tiesioginėms darbo funkcijoms vykdyti.

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

4.2.1. 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.

4.2.2. Teisinė prievolė. Įstaiga teisės aktais yra įpareigota tvarkyti Duomenis.

4.2.3. Teisėtas interesas. Duomenys yra reikalingi ginčų nagrinėjimui, incidentų tyrimui, turto, žmonių, informacinių, komunikacinių technologijų saugumui užtikrinti, veiklos tęstinumui ar kitiems, iš anksto nustatytiems Įstaigos interesams, jei Asmens interesai, konkrečių aplinkybių kontekste nėra svarbesni.

4.2.4. Sutikimas. Kai Asmuo davė sutikimą, kad jo duomenys būtų tvarkomi vienu ar keliais konkrečiais veiksmais.

4.2.5. Siekiant atlikti užduotį. Kai tvarkyti duomenis būtina siekiant atlikti užduotį, vykdomą viešojo intereso labui arba vykdant duomenų valdytojui pavestas viešosios valdžios funkcijas.

4.3. Asmens ypatingi duomenys, įskaitant sveikatos duomenis Įstaigoje gali būti tvarkomi tik ta apimtimi, kiek yra būtina, siekiant pareikšti, vykdyti arba apginti teisinius reikalavimus.

4.4. Duomenys apie Asmens teistumą gali būti tvarkomi tik kai tai numato specialūs teisės aktai ir tik ta apimtimi, kiek tai reikalinga atitinkamų teisės aktų įgyvendinimui, pvz., prireikus tokių duomenų viešajame pirkime ar projekto konkurse, tačiau tokie duomenys turi būti saugomi atskirai nuo kitų duomenų ir su jais nesujungiami ir sunaikinami pasibaigus viešojo pirkimo ar projekto konkurso procedūrai, jei specialūs teisės aktai nenumato specialios pareigos, tam tikrą laiką saugoti tokius Duomenis.

4.5. Neatsižvelgiant į aukščiau nurodytus Duomenų tvarkymo teisinius pagrindus, visais atvejais Duomenys tvarkomi teisėtai, kai tai daroma duomenų tvarkymo sutarties pagrindu, teikiant duomenų tvarkymo paslaugas klientams, o Duomenys yra tvarkomi kliento vardu ir interesais bei laikantis Kliento nurodymų.

5. DUOMENŲ TVARKYMO TIKSLAI

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

5.1.1. Duomenų kategorijos pagal kiekvieną duomenų kategoriją;

5.1.2. Duomenų tvarkymo tikslai ir teisinis pagrindas (Bendrojo duomenų apsaugos reglamento straipsnio nuoroda) pagal kiekvieną Duomenų kategoriją.

5.1.3. Duomenų gavėjų kategorijos kiekvienai Asmenų kategorijai pagal Duomenų perdavimo tipą bei teisinį pagrindą (Duomenų tvarkymo lentelė, duomenų teikimas);

5.2. Duomenų saugojimo terminai.

5.2.1. Sudaromi atskiri duomenų tvarkymo veiklos įrašai, Įstaigos, kaip duomenų tvarkytojo veikloms. Šiuose įrašuose nurodoma:

(1) duomenų valdytojų, kurių duomenis tvarko Įstaiga pavadinimas, kontaktiniais duomenys, jei yra, jų duomenų apsaugos pareigūnų duomenys

5.3. Darbuotojai, prieš pradėdami tvarkyti Įstaigos klientų pagal duomenų tvarkymo sutartį perduotus Duomenis, privalo kreiptis į Įgaliotą darbuotoją, gauti bei susipažinti su atitinkamo kliento ar klientų sudarytą duomenų tvarkymo sutartimi, išsiaiškinti duomenų tvarkymo tikslus, Asmenų bei Duomenų kategorijas. Priedas Nr. 1 *Duomenų veiklos tvarkymo įrašai.*

5.4. Duomenų perdavimas į trečiąsias šalis

5.4.1. Darbuotojas gali perduoti Asmens duomenis konkretiems paslaugų teikėjams ar kitiems subjektams įsteigtiems už EEE ribų, tik tais atvejais, kai tokie paslaugų tiekėjai ar kiti subjektai yra įtraukti į Įstaigos Duomenų tvarkymo veiklos įrašus.

6. BENDROSIOS DARBUOTOJŲ PAREIGOS DUOMENŲ APSAUGOS SRITYJE

6.1. Kiekvienas darbuotojas privalo:

6.1.1. pradėdamas tvarkyti duomenis įsitikinti, ar yra laikomasi visų reikalavimų, numatytų Politikoje;

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

Kai tvarkomi Duomenys, kurių valdytojas yra Įstaiga:

6.1.3. visais atvejais identifikuoti Duomenis, kurie yra tvarkomi Darbuotojo veikloje bei žinoti, kad veiklai susijusiai su Duomenų tvarkymu, yra taikomi šios Politikos, asmens duomenų apsaugos teisės aktų reikalavimai;

6.1.4. 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 o apie poreikį tvarkyti naujas Duomenų kategorijas ir (ar) naujais tikslai, informuoti Įgaliotą asmenį;

6.1.5. visais atvejais, prieš perduodamas 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 tvarkymo veiklos įrašuose nenurodytai Duomenų gavėjų kategorijai arba už EEE ribų veikiančiam trečiajam asmeniui, nenurodytam Duomenų tvarkymo veiklos įrašuose, informuoti įgaliotą asmenį.

6.1.6. kreiptis į įgaliotą asmenį ir gauti jo informaciją:

(a) ketinant sudaryti paslaugų sutartį su nauju klientu, kurio perduoti duomenys bus tvarkomi Įstaigoje kliento vardu ir interesais;

(b) ketinant Įstaigoje pasitelkti naują Paslaugų teikėją;

(c) ketinant Įstaigoje sukurti, diegti ar naudoti naujas informacines technologijas ar kitus metodus duomenų tvarkymui.

(d) prieš pradedant naują tiesioginės rinkodaros kampaniją ar Duomenų rinkimą jos įgyvendinimui;

(e) esant bet kokiems netikslumams, abejonėms ar klausimams, susijusiems su Politikos taikymu, aiškinimu, pažeidimu ar atitikimu Politikai.

6.1.7. 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 Įgaliotam asmeniui.

6.1.8. nedelsiant, bet ne vėliau kaip per 12 (dvylika) valandų, nuo sužinojimo apie Duomenų saugumo pažeidimą Įstaigoje:

(a) informuoti įgaliotą darbuotoją apie Duomenų saugumo pažeidimą;

(b) pagal savo kompetenciją imtis pagrįstų veiksmų, kad duomenų saugumo pažeidimas būtų sustabdytas;

(c) pagal savo kompetenciją imtis pagrįstų veiksmų, kad Duomenų saugumo pažeidimas nepasikartotų.

6.1.9. Bendradarbiauti su Įgaliotu asmeniu, kitais Darbuotojais ir (ar) Paslaugų teikėjais atliekant Duomenų saugumo pažeidimo valdymą, Asmenų prašymų valdymą, Asmens duomenų apsaugos inspekcijos paklausimų valdymą ir kitas Įstaigos nustatytas, su Duomenų tvarkymu, susijusias procedūras.

6.1.10. Per trumpiausią terminą, pateikti Įgaliotam asmeniui jo prašomą informaciją, susijusią su asmens duomenų apsauga.

6.1.11. Vykdyti Įgalioto asmens nurodymus dėl Duomenų tvarkymo.

6.1.12. Užtikrinti, kad tiesioginės rinkodaros pranešimai Asmenims ir (ar) juridiniams asmenims, būtų siunčiami tik tuomet kai asmuo yra davęs sutikimą tiesioginei rinkodarai.

7. ASMENS DUOMENŲ SUBJEKTO TEISIŲ ĮGYVENDINIMAS

7.1. Darbuotojas, gavęs Asmens prašymą, nedelsdamas, ne vėliau, kaip per 1 (vieną) darbo dieną nuo Asmens prašymo gavimo dienos kreipiasi į Įgaliotą asmenį.

7.2. Įgaliotas asmuo, gavęs Asmens prašymą atlieka Asmenų prašymų valdymą, užpildydamas Asmenų prašymų registro įrašo formą.

7.3. Gavęs prašymą Įgaliotas asmuo:

7.3.1. peržiūri prašymą;

7.3.2. nustato prašymą pateikusio Asmens tapatybę;

7.3.3. surenka prašymo nagrinėjimui reikalingą informaciją;

7.3.4. įvertina prašymo teisinį pagrįstumą;

7.3.5. patvirtina Asmeniui, kad jo prašymas gautas;

7.3.6. nustato ar, ir kokia papildoma informacija iš Darbuotojų, Paslaugų teikėjų ir (ar) Asmens, kuris pateikė prašymą, yra reikalinga, siekiant atsakyti į Asmens prašymą;

7.3.7. esant būtinumui, duoda reikiamus pavedimus Darbuotojams dėl prašymą pateikusio Asmens Duomenų tolimesnio tvarkymo;

7.3.8. paruošia ir pateikia asmeniui atsakymą į prašymą.

7.4. Nustatęs, kad gautas Asmens prašymas yra susiję su Įstaigos kliento, pagal duomenų tvarkymo sutartį perduotais duomenimis, persiunčia tokį prašymą atitinkamam klientui ir informuoja apie tai prašymą pateikusį asmenį; šiuo atveju atsakymą į prašymą rengia Įstaigos klientas, o Įgaliotas darbuotojas suteikia klientui visą informaciją, reikalingą prašymo nagrinėjimui ir atsakymo parengimui.

7.5. Įgaliotas asmuo užtikrina, kad:

7.5.1. į Asmens prašymą turi būti atsakytas per 1 (vieną) mėnesį nuo jo gavimo dienos. Jei, Asmens prašymų, pateiktų to paties Asmens, sudėtingumas ar skaičius yra didelis, Įgaliotas asmuo turi teisę pratęsti terminą atsakymui pateikti, iki 2 (dviejų) mėnesių, informuodamas apie tai Asmenį ir nurodydamas termino pratęsimo priežastis;

7.5.2. Asmeniui būtų pateikta tik ta ir ta apimtimi informacija, kiek tai yra susiję su juo pačiu ir tik tiek, kiek reikalauja asmens duomenų apsaugos įstatymas ir kiti norminiai aktai;

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

7.6. Asmens prašymą tenkinti atsisakoma kai:

7.6.1. Asmens prašymas nesusijęs su Asmens duomenų apsaugos teisės aktų numatytomis teisėmis;

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

7.6.3. Asmens prašymas susijęs su informacija apie kitą asmenį (išskyrus atvejus, kai tai leidžiama teisės aktais).

7.6.4. Asmuo neturi teisės pasinaudoti atitinkamomis duomenų subjekto teisėmis pagal asmens duomens duomenų apsaugos teisės aktų nustatytus reikalavimus bei išimtis;

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

(a) 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 pagrįstai gali tikėtis, kad pasikeitė apie Asmenį tvarkomų duomenų apimtis.

(b) Asmens prašymas susijęs su dideliu kiekiu pasikartojančių Duomenų;

(c) aplinkybės rodo, kad vienintelis Asmens prašymo tikslas yra sutrikdyti Įstaigos veiklą ir Įstaiga gali tai įrodyti;

7.7. Įgaliotas darbuotojas į Asmens prašymą atsako elektroninėmis priemonėmis glausta ir Asmeniui suprantama forma, vartodamas aiškią ir suprantamą kalbą.

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

7.9. Jei asmens prašymas tenkinamas, Įgaliotas darbuotojas koordinuoja ir planuoja Asmens prašymo įgyvendinimą Įstaigoje, teikia nurodymus bei konsultacijas Darbuotojams ir Paslaugų teikėjams, kurie turi dalyvauti Asmens prašymo įgyvendinime.

8. DUOMENŲ SUNAIKINIMAS

8.1. Asmens duomenys, nebereikalingi jų tvarkymo tikslams pasiekti, yra sunaikinami, išskyrus tuos, kurie teisės aktų nustatytais atvejais turi būti perduodami į tam tikrą archyvą.

8.2. Sunaikinimas apibrėžiamas kaip fizinis ar techninis veiksmas, kuriuo dokumente esantys duomenys padaromi neatkuriamais įprastinėmis komerciškai prieinamomis priemonėmis.

8.3. Elektronine forma saugomi asmens duomenys sunaikinami juos ištrinant be galimybės atkurti.

8.4. Popieriniai dokumentai, kuriuose yra asmens duomenų, susmulkinami, o likučiai saugiu būdu sunaikinami.

9. DUOMENŲ SAUGUMO PAŽEIDIMŲ VALDYMAS

9.1. Darbuotojas, sužinojęs apie galimą Duomenų saugumo pažeidimą Įstaigoje, nedelsdamas, bet ne vėliau kaip per 12 (dvylika) valandų, turi apie etai informuoti Įgaliotą asmenį, o jei toks nepaskirtas, vadovybę.

9.2. Įgaliotas asmuo vykdo Duomenų saugumo pažeidimų valdymą vadovaudamasis šia Politika ir asmens duomenų apsaugos teisės aktais ir pildo duomenų apsaugos pažeidimo registrą.

9.3. Įgaliotas asmuo užtikrina, kad laikomasi šios Politikos ir asmens duomenų apsaugos teisės aktų nustatytų terminų. Įgaliotas asmuo, pažeidimų registre, nurodydamas pratęsimo priežastis, gali pratęsti terminus, jei tai reikalinga dėl to paties Asmens Duomenų saugumo pažeidimo sudėtingumo ar masto.

9.4. Įgaliotas asmuo, 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 analizę ir užpildo Asmens duomenų pažeidimo ataskaitą:

9.4.1. peržiūri informaciją apie Duomenų saugumo pažeidimą;

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

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

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

9.5. vykdomas pažeidimų dokumentavimas, registruojant pažeidimą Asmens duomenų saugumo pažeidimų žurnale (toliau – Žurnalas).

9.6. Tyrimo rezultatai įforminami, vykdoma pažeidimų analizės ir prevencijos priemonių įgyvendinimo kontrolė.

9.7. Įgaliotas asmuo, nustatęs, kad Duomenų saugumo pažeidimo valdymui reikalinga papildoma informacija, prašo Darbuotojo ir (ar) Paslaugų teikėjų, suteikti reikiamą informaciją ne vėliau kaip per 24 (dvidešimt keturias) valandas. Darbuotojai ir paslaugų teikėjai turi laiku suteikti Įgaliotam darbuotojui visą prašomą informaciją.

9.8. Įgaliotas asmuo 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.

9.9. Įgaliotas asmuo, sužinojęs apie galimą Pažeidimą, kaip įmanoma greičiau atlieka pirminį tyrimą, išsiaiškina ir nustato, ar Pažeidimas iš tikrųjų įvyko, bei kokios galimos pasekmės asmenims (t. y. įvertinti riziką).

9.10. Galimi Pažeidimo tipai:

9.10.1. „Konfidencialumo Pažeidimas" – kai yra be leidimo ar neteisėtai atskleidžiami asmens duomenys arba gaunama prieiga prie jų;

9.10.2. „Prieinamumo Pažeidimas" – kai netyčia arba neteisėtai prarandama prieiga prie arba sunaikinami asmens duomenys;

9.10.3. „Vientisumo Pažeidimas" – kai asmens duomenys pakeičiami be leidimo ar netyčia.

Priklausomai nuo aplinkybių, Pažeidimas tuo pat metu gali sietis su asmens duomenų konfidencialumu, prieinamumu ir vientisumu, taip pat su kuriuo nors jų deriniu.

9.11. Priklausomai nuo Pažeidimo pobūdžio (tipo), atliekant pirminį tyrimą ir siekiant nustatyti, ar Pažeidimas iš tikrųjų įvyko, turėtų būti išsaugomi esamos situacijos įrodymai bei vėliau naudojamos visos tinkamos techninės ir organizacinės priemonės, pvz., duomenų srauto ir prisijungimų analizės įrankiai bei kt.

9.12. Vertinant riziką, kuri gali atsirasti dėl Pažeidimo, turėtų būti atsižvelgiama į konkrečias Pažeidimo aplinkybes, pavojaus duomenų subjekto teisėms ir laisvėms atsiradimo tikimybę ir rimtumą. Rizika turėtų būti vertinama remiantis objektyviu įvertinimu ir atsižvelgiant į šiuos kriterijus:

9.12.1. Pažeidimo tipą;

9.12.2. Asmens duomenų pobūdį, apimtis (pvz., specialių kategorijų asmens duomenys);

9.12.3. Kaip lengvai identifikuojamas fizinis asmuo;

9.12.4. Pasekmių rimtumą fiziniams asmenims;

9.12.5. Specialias fizinio asmens savybes (pvz., duomenys susiję su vaikais ar kitais pažeidžiamais asmenimis);

9.12.6. Nukentėjusiųjų fizinių asmenų skaičių;

9.12.7. Specialias duomenų valdytojo savybes (pvz., veiklos pobūdį).

9.13. Vertinant riziką, laikoma, kad Pažeidimas, galintis kelti pavojų asmenų teisėms ir laisvėms yra toks, dėl kurio, laiku nesiėmus tinkamų priemonių, fiziniai asmenys gali patirti kūno sužalojimą, materialinę ar nematerialinę žalą, pvz., prarasti savo asmens duomenų kontrolę, patirti teisių apribojimą, diskriminaciją, gali būti pavogta ar suklastota jo asmens tapatybė, jam padaryta finansinių nuostolių, neleistinai panaikinti pseudonimai, gali būti pakenkta jo reputacijai, prarastas asmens duomenų, kurie saugomi profesine paslaptimi, konfidencialumas arba padaryta kita ekonominė ar socialinė žala atitinkamam fiziniam asmeniui.

9.14. Įvertinus riziką nustatoma, kad yra:

9.14.1. Žema rizikos tikimybė;

9.14.2. Vidutinė rizikos tikimybė;

9.14.3. Didelė (aukšta) rizikos tikimybė.

9.15. Išvadą dėl Pažeidimo buvimo ir rizikos fizinių asmenų teisėms bei laisvėms įvertinimo Įgaliotas asmuo pateikia vadovybei. Vadovybė priimą sprendimą dėl tolimesnių veiksmų, susijusių su Pažeidimu.

9.16. Įgaliotas asmuo visų pirma imasi visų tinkamų techninių ir organizacinių priemonių, kad Pažeidimas būtų išsamiai ištirtas ir pašalintas (sustabdytas, ištaisytas) bei ateityje nepasikartotų ir tuomet pateikia Pranešimą VDAI.

9.17. Nustačius, kad Pažeidimas buvo ir, kad yra didelė rizika fizinių asmenų teisėms ir laisvėms, Įgaliotas asmuo nedelsdamas (rekomenduojama per 72 val.) apie tai praneša duomenų subjektui, kurio teisėms ir laisvėms dėl šio Pažeidimo gali kilti didelis pavojus.

9.18. Pranešime duomenų subjektui aiškia ir paprasta kalba turėtų būti pateikiama:

9.18.1. Pažeidimo pobūdžio aprašymas;

9.18.2. Duomenų apsaugos pareigūno arba kito kontaktinio asmens vardas, pavardė (pavadinimas) ir kontaktiniai duomenys;

9.18.3. Tikėtinų Pažeidimo pasekmių aprašymas;

9.18.4. Priemonių, kurių ėmėsi arba pasiūlė imtis duomenų valdytojas, kad būtų pašalintas Pažeidimas, įskaitant (kai tinkama) priemonių galimoms neigiamoms jo pasekmėms sumažinti, aprašymas (pvz., kad apie Pažeidimą yra informuota VDAI ir, kad yra gautas patarimas dėl Pažeidimo tvarkymo ir jo poveikio sumažinimo; siūlymas duomenų subjektui pasikeisti slaptažodžius ir kt.);

9.18.5. Kita reikšminga informacija, susijusi su Pažeidimu, kuri, duomenų valdytojo manymu, turėtų būti pateikta duomenų subjektui.

9.19. Duomenų subjektai apie Pažeidimą informuojamas tiesiogiai, pvz., siunčiant jiems pranešimą el. paštu, SMS, paštu ar pan. Šis pranešimas turėtų būti atskirtas nuo kitos siunčiamos informacijos, tokios kaip nuolatiniai atnaujinimai, naujienlaiškiai ar standartiniai pranešimai.

9.20. Galimi pasirinkti keli pranešimo duomenų subjektui apie Pažeidimą būdai:

9.21. Esant Pažeidimui, pranešimo duomenų subjektui teikti nereikia, jeigu:

9.21.1. Įstaiga įgyvendino tinkamas technines ir organizacines apsaugos priemones ir tos priemonės taikytos asmens duomenims, kuriems Pažeidimas turėjo poveikio;

9.21.2. Iš karto po Pažeidimo Įstaiga ėmėsi priemonių, kuriomis užtikrinama, kad nebegalėtų kilti didelis pavojus asmenų teisėms ir laisvėms;

9.21.3. Tai reikalauja neproporcingai daug pastangų susisiekti su asmenimis (pvz., kai jų kontaktiniai duomenys buvo prarasti dėl Pažeidimo arba pirma nežinomi). Tokiu atveju vietoj to apie Pažeidimą paskelbiama viešai arba taikoma panaši priemonė, kuria duomenų subjektai būtų informuojami taip pat efektyviai.

9.22. Jeigu tiriant Pažeidimą pradžioje nustatoma, kad nėra pavojaus fizinių asmenų teisėms ir laisvėms, tačiau detalesnio Pažeidimo tyrimo metu nustatoma, kad toks pavojus gali kilti, Įstaiga rizikos vertinimą atlieka iš naujo.

10. VALSTYBINĖS DUOMENŲ APSAUGOS INSPEKCIJOS PAKLAUSIMAI

10.1. Įgaliotas darbuotojas vykdo Valstybinės duomenų inspekcijos paklausimų valdymą, vadovaudamasi asmens duomenų apsaugos teisės aktais.

10.2. Darbuotojas gavęs Valstybinės duomenų inspekcijos paklausimą, nedelsiant bet ne vėliau kaip per 1 (vieną) darbo dieną, informuoja Įgaliotą asmenį arba vadovybę apie tokį paklausimą.

10.3. Įgaliotas asmuo, gavęs Valstybinės duomenų inspekcijos paklausimą, turi nedelsiant atlikti pirminę Valstybinės duomenų inspekcijos paklausimo analizę:

10.3.1. susipažinti su Valstybinės duomenų inspekcijos paklausimu;

10.3.2. nustatyti atsakymo į Valstybinės duomenų inspekcijos paklausimą terminus (įskaitant reikalingos informacijos surinkimą, konsultacijas su Darbuotojais ar Paslaugų teikėjais;

10.3.3. jei reikia, kreiptis į Valstybinės duomenų inspekciją dėl termino patekti atsakymą pratęsimo arba paklausimo patikslinimą.

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

10.3.5. nustatyti, ar Paslaugų teikėjai, išoriniai Duomenų apsaugos pareigūnai, IT saugumo konsultantai ar tretieji asmenys yra susiję su Valstybinės duomenų inspekcijos paklausimu ir jei taip, kreiptis į juos dėl informacijos būtinos atsakymui į Valstybinės duomenų inspekcijos paklausimą.

10.4. Surinkę visą, į Valstybinės duomenų inspekcijos paklausimą būtiną informaciją, tačiau ne vėliau, kaip į Valstybinės duomenų inspekcijos nustatytą terminą, Įgaliotas asmuo parengia ir pateikia Valstybinės duomenų inspekcijai atsakymą į paklausimą.

11. ĮGALIOTAS ASMUO

11.1. Įstaiga paskiria Įgaliotą asmenį, kuris padeda prižiūrėti kaip Įstaigoje laikomasi asmens duomenų apsaugos teisės aktų reikalavimų ir veikia kaip Įstaigos atstovas su asmens duomenų

apsauga susijusiais klausimais. Jei tokio asmens nėra galimybės paskirti pačioje Įstaigoje, tokiu atveju gali būti paskirtas Asmuo iš išorės, pagal paslaugų teikimo sutartį arba pačias Įgalioto asmens funkcijas vykdyti Įstaigos vadovas.

11.2. Darbuotojai, darbo tvarkos taisyklių nustatyta tvarka informuojami apie paskirtą Įgaliotą asmenį, pranešami jo kontaktiniai duomenys.

11.3. Įgaliotas darbuotojas atlieka šias funkcijas:

11.3.1. informuoja Įstaigą, juos Darbuotojus ir vadovybę apie jo prievoles pagal asmens duomenų apsaugos teisės aktus, taip pat apie Duomenų apsaugą Įstaigoje ir konsultuoja juos šiais klausimais;

11.3.2. stebi ir kontroliuoja, kaip Įstaigoje laikomasi asmens duomenų apsaugos teisės aktų laikymosi;

11.3.3. rūpinasi Duomenų rinkimo, naudojimo ir saugojimo vykdant Įstaigos tiesioginę veiklą;

11.3.4. koordinuoja, atlieka ir stebi poveikio Duomenų apsaugai vertinimus Įstaigoje;

11.3.5. stebi, ar Įstaiga kurdama, diegdama ir (ar) naudodama IT Duomenų tvarkymui, laikosi asmens duomenų apsaugos teisės aktų reikalavimų;

11.3.6. atlieka kontaktinio asmens funkcijas Asmenims, kurie kreipiasi į Įstaigą kaip duomenų valdytoją ar tvarkytoją, su Duomenų tvarkymu susijusiais klausimais;

11.3.7. konsultuoja Darbuotojus dėl Duomenų perdavimo konkretiems Paslaugų teikėjams ar kitiems tretiesiems asmenims;

11.3.8. peržiūri, esant poreikiui papildo ar pakeičia šią politiką, Duomenų tvarkymo veiklos įrašus, kitas su Duomenų apsauga susijusias vidaus taisykles, procedūras, dokumentų šablonus, prižiūri ir kontroliuoja jų laikymąsi;

11.3.9. koordinuoja, kad Įstaiga su visais Paslaugų teikėjais ir klientais, kurių perduoti duomenys bus tvarkomi to kliento vardu ir interesais, sudarytų Duomenų tvarkymo sutartis, įskaitant sąlygas dėl paslaugų teikimo (arba sutartis su Paslaugų teikėjais atitinkamomis nuostatomis);

11.3.10. praneša apie esamus ar galimus asmens duomenų apsaugos teisės aktų pažeidimus, keliančius pavojų Įstaigos veiklai bei konsultuoja Darbuotojus, susijusius su šiais pažeidimais;

11.3.11. atlieka Duomenų saugumo pažeidimų valdymą;

11.3.12. atlieka Asmenų teisių įgyvendinimo valdymą;

11.3.13. atlieka kontaktinio asmens funkcijas Valstybinės duomenų inspekcijai kreipiantis į Įstaigą, atstovauja Įstaigos interesu.

11.4. Tuo atveju, jei Įstaigai taptų būtina arba būtų nuspręsta paskirti Asmens domenų apsaugos pareigūną, jis atliktų visas, šioje politikoje apibrėžtas Įgalioto asmens funkcijas.

12. TECHNINĖS IR ORGANIZACINĖS ASMENS DUOMENŲ SAUGUMO PRIEMONĖS

12.1. Įstaiga įgyvendinama organizacinės ir techninės duomenų saugumo priemonės užtikrina tokį saugumo lygį, kuris atitinka duomenų valdytojo valdomų duomenų pobūdį ir jų tvarkymo keliamą riziką.

12.2. Įstaiga užtikrina patalpų, kuriose saugomi asmens duomenys, saugumą.

12.3. Į patalpas, kuriose saugomi archyviniai dokumentai, gali patekti tik atsakingi už archyvo tvarkymą ir dokumentų valdymą asmenys.

12.4. Prieiga prie duomenų bei teisė atlikti duomenų tvarkymo veiksmus suteikiama tik tiems Darbuotojams, kuriems prieiga prie asmens duomenų reikalinga pagal užimamas pareigas ir atliekamas darbines funkcijas;

12.5. Užtikrinama tvarkomų asmens duomenų apsauga nuo neteisėto prisijungimo prie vidinio kompiuterinio tinklo elektroninių ryšių priemonėmis;

12.6. Užtikrinamas saugių protokolų ir slaptažodžių naudojimas, kai asmens duomenys perduodami išoriniais duomenų perdavimo tinklais;

12.7. Užtikrinama kompiuterinės įrangos apsauga nuo kenksmingos programinės įrangos (antivirusinių programų įdiegimas, atnaujinimas ir pan.);

12.8. Kompiuterinė įranga ir duomenų perdavimo tinklas prižiūrimi pagal gamintojo rekomendacijas, priežiūrą ir gedimų šalinimą atlieka kvalifikuoti specialistai, o duomenų perdavimo tinklo bei svarbiausios kompiuterinės įrangos techninė būklė nuolat stebima.

12.9. Įstaigos darbuotojams nustatomos su asmens duomenų sauga susijusios tokios pareigos:

12.9.1. Įstaigos darbuotojai turi laikytis konfidencialumo principo ir laikyti paslaptyje bet kokią su asmens duomenimis susijusią informaciją, su kuria jie susipažino vykdydami savo pareigas, nebent tokia informacija būtų vieša pagal galiojančių įstatymų ar kitų teisės aktų nuostatas. Įstaigos darbuotojai, kurie vykdydami savo tiesiogines pareigas tvarko asmens duomenis, prieš pradėdami vykdyti pareigas pasirašo pasižadėjimą dėl asmens duomenų apsaugos. Konfidencialumo principo Įstaigos darbuotojai turi laikytis ir pasibaigus darbo ar tarnybos santykiams.

12.9.2. Įstaigos darbuotojai pasirašytinai supažindinami su šiomis Taisyklėmis ir įsipareigoja saugoti asmens duomenų paslaptį, jei jų tvarkomi asmens duomenys neskirti skelbti viešai.

12.9.3. Asmens duomenų tvarkymo funkcijas vykdantys darbuotojai, siekdami užkirsti kelią atsitiktiniam ar neteisėtam asmens duomenų sunaikinimui, pakeitimui, atskleidimui, taip pat bet kokiam kitam neteisėtam tvarkymui, turi saugoti dokumentus bei duomenų rinkmenas tinkamai ir

saugiai bei vengti nereikalingų kopijų darymo. Įstaigos dokumentų kopijos, kuriose nurodomi asmens duomenys, turi būti saugiai sunaikinamos.

12.9.4. Įstaiga įgyvendina tinkamas technines ir organizacines priemones, kuriomis užtikrina, kad standartizuotai būtų tvarkomi tik tie asmens duomenys, kurie yra būtini kiekvienam konkrečiam duomenų tvarkymo tikslui. Ta prievolė taikoma surinktų asmens duomenų kiekiui, jų tvarkymo apimčiai, jų saugojimo laikotarpiui ir jų prieinamumui.

12.9.5. Įstaiga imasi reikiamų atsargumo priemonių išsaugoti duomenų subjektų asmens duomenų vientisumą ir neleisti, kad šie duomenys būtų sugadinti ar prarasti, įskaitant rūpinimąsi reikiamu duomenų atstatymu.

13. DARBUOTOJŲ MOKYMAS

13.1. Įstaiga, esant poreikiui, vykdo tinkamus mokymus Darbuotojams, turintiems teisę nuolat ar reguliariai susipažinti su asmens duomenimis.

13.2. Mokymai turi atitikti darbuotojų veiklos realijas ir apmokymą tinkamai dirbti su asmens duomenų tvarkymo sistemomis, registrais ir duomenų bazėmis.

13.3. Mokymų turinys turi padėti darbuotojams vykdyti savo darbines pareigas laikantis BDAR ir kituose asmens duomenų apsaugą reglamentuojančiuose teisės aktuose nustatytų reikalavimų.

13. BAIGIAMOSIOS NUOSTATOS

13.1. Ši politika peržiūrima ir atnaujinama ne račiau kaip kartą per metus arba pasikeitus teisės aktams, kurie reglamentuoja asmens duomenų tvarkymą.

13.2. Darbuotojai ir kiti atsakingi asmenys su šia politika yra supažindinami pasirašytinai arba elektroninėmis priemonėmis ir privalo laikytis joje nustatytų įpareigojimų bei atlikdami savo darbo funkcijas vadovautis šioje politikoje nustatytais principais.

13.3. Įstaigos darbuotojams, tvarkantiems asmens duomenis, už šios Politikos ar kitų teisės aktų nuostatų pažeidimus gali būti taikoma teisinė atsakomybė.

13.4. Darbuotojo asmens duomenų teisinę apaugą ir teisės į privatų gyvenimą įgyvendinimo ypatumus nustato ir kitos darbo teisės normos. Įstaigos darbuotojo duomenims ir jų apsaugai taikomos bendros asmens duomenų apsaugos ir privatumo nuostatos.