PATVIRTINTA

 Tauragės lopšelis-darželis „Kodėlčius“

 direktoriaus 2023 m. gruodžio 7 d.

 įsakymu Nr. V- 108

**TVARKOMŲ ASMENS DUOMENŲ APSAUGOS PAŽEIDIMŲ RIZIKOS ANALIZĖ**

**I SKYRIUS**

**BENDROSIOS NUOSTATOS**

1. Asmens duomenų apsaugos pažeidimas – tai veiksmai ar neveikimas, kurie gali sukelti ar sukelia nepageidaujamus padarinius, taip pat prieštarauja imperatyvioms įstatymų, reglamentuojančių asmens duomenų apsaugą, normoms. Asmens duomenų apsaugos pažeidimo poveikio laipsnį, žalą ir padarinius kiekvienu konkrečiu atveju nustato įstaigos vadovo ar jo įgalioto asmens sudaryta komisija. Rizikos vertinimas gali būti atliekamas įvairiais būdais, tačiau bet kuriuo atveju reikėtų įvertinti tokius faktorius ir nustatyti jų poveikį asmens duomenų konfidencialumui, saugumui, integralumui ir pasiekiamumui.

2. Duomenys įstaigoje tvarkomi rankiniu būdu susistemintuose rinkmenose ir automatiniu būdu t. y. įvairiomis elektroninėmis priemonėmis: elektroninis dienynas, Pedagogų ir Mokinių registrai, dokumentų valdymo sistema „Kontora“, buhalterinės programos ir kt. Tauragės lopšelio-darželio „Kodėlčius“ (toliau – Įstaiga) tvarkomi asmens duomenys gali būti perduodami.

3. Asmens duomenų įstaiga neatskleidžia tretiesiems asmenims, išskyrus LR įstatymuose numatytus atvejus, kai to reikalauja valstybės institucijos arba jei tai atlikti Įstaigą įpareigoja Duomenų teikėjas. Įstaiga asmens duomenis gali perduoti tik tikrinimus atliekančioms valstybinėms institucijoms.

**II SKYRIUS**

**ASMENS DUOMENŲ APSAUGOS PAŽEIDIMŲ RIZIKOS VEIKSNIAI**

**IR ASMENS DUOMENŲ APSAUGOS ĮGYVENDINIMO PRIEMONĖS**

4. Asmens duomenų apsaugos pažeidimo veiksniai skirstomi į:

4.1. netyčiniai asmens duomenų apsaugos pažeidimo veiksniai, kai asmens duomenų apsauga pažeidžiama dėl atsitiktinių priežasčių (duomenų tvarkymo klaidos, informacijos laikmenų, duomenų įrašų ištrynimo, sunaikinimo, neteisingų adresų perduodant duomenis nustatymo ir pan., ar sistemų sutrikimai dėl elektros tiekimo nutrūkimo, kompiuterinio viruso ir pan., vidaus taisyklių pažeidimo, sistemos priežiūros trūkumo ir kt.);

4.2. tyčiniai asmens duomenų apsaugos pažeidimo veiksniai, kai asmens duomenų apsauga pažeidžiama sąmoningai (neteisėtas įsibrovimas į įstaigos patalpas, asmens duomenų laikmenų saugyklas, informacines sistemas, kompiuterių tinklą, piktybinis nustatytų taisyklių tvarkant asmens duomenis pažeidimas, sąmoningas kompiuterio viruso platinimas, asmens duomenų vagystė, neteisėtas naudojimasis kito darbuotojo teisėmis ir kt.);

4.3. netikėti atsitiktiniai asmens duomenų apsaugos pažeidimo veiksniai (žaibas, gaisras, potvynis, elektros instaliacijos gedimas ir kiti nenugalimi ir/ar nekontroliuojami veiksniai).

5. Siekdama užtikrinti asmens duomenų apsaugą, įstaiga įgyvendina šias duomenų apsaugos priemones:

5.1. administracines;

5.2. technines ir programinės įrangos apsaugos;

5.3. komunikacijų ir kompiuterių tinklų apsaugos.

6. Asmens duomenų apsaugos pažeidimų rizikos ir asmens duomenų apsaugos įgyvendinimo priemonės.

|  |  |  |
| --- | --- | --- |
| **Eil. Nr.** | **Asmens duomenų apsaugos pažeidimų rizikos** | **Asmens duomenų apsaugos įgyvendinimo priemonės** |
| 1. | Neteisėta fizinė prieiga prie kompiuterinės įrangos. | Patalpos rakinamos ir saugomos signalizacija. |
| 2. | Neteisėti programinės įrangos vartotojai. | Nustatytas vartotojų prisijungimas, nustatyta slaptažodžių sudarymo ir atnaujinimo tvarka, valdoma vartotojų teisė naudotis programine įranga. |
| 3. | Neteisėtas vartotojų prisijungimas prie tinklo. | Vidinis tinklas apsaugotas ugnies sienomis, kontroliuojamas trečiųjų šalių vartotojų prisijungimas. |
| 4. | Neteisėtas saugomų laikmenų naudojimas. | Popieriniai dokumentai ar reikalingos jų kopijos saugomos rakinamose įstaigos patalpose segtuvuose. |
| 5.  | Vagystė. | Apribota fizinė prieiga prie programinės įrangos ir informacija laikmenose saugoma archyvo tikslais. |
| 6. | Duomenų perdavimo tinklo piktavališkas panaudojimas. | Veikia duomenų perdavimo tinklo valdymo programos. |
| 7. | Programinės įrangos klaidos. | Naudojama sertifikuota programinė įranga ir ji atnaujinama laikanti nustatytos tvarkos. |
| 8.  | Piktavališkos programos. | Kompiuteriuose įdiegtos antivirusinės programos. |
| 9.  | Neteisėtos programinės įrangos naudojimas. | Naudojama tik teisėta programinė įranga ir darbuotojams nesuteikta teisė patiems diegti programinę įrangą. |
| 10.  | Vartotojų klaidos. | Darbuotojai mokomi dirbti su programine įranga. |
| 11.  | Duomenų perdavimo tinklo įrangos gedimai. | Įranga prižiūrima pagal gamintojo rekomendacijas, o priežiūrą ir gedimų šalinimą atlieka kvalifikuoti specialistai. |

7. Visi vartotojai turi prieigą tik prie tų duomenų, kurie jiems yra būtini funkcijoms atlikti, ir būtų identifikuojami rizikos lygį atitinkančiomis priemonėmis. Patartina naudoti tokias prieigos teisių suteikimo priemones, kurios leistų bendro identifikavimo būdu gauti visus tai funkcijai atlikti priklausančius išteklius. Įgaliotas direktoriaus pavaduotojas ugdymui administruoja elektroninį dienyną ir internetinę įstaigos svetainę. Pedagoginis personalas prieina prie elektroninio dienyno duomenų, kurių jiems reikia jų darbo funkcijoms atlikti, įveda savo ugdytinių duomenis. Meninio ugdymo mokytojas mato elektroniniame dienyne vaikų duomenis ir pildo vaikų pasiekimus. Prie Pedagogų registro, Centralizuotos vaiko priėmimo sistemos (CVPS) ir Gyventojų registro prieigas turi direktorius. Sekretorius turi prieigas prie Centralizuotos vaiko priėmimo sistemos (CVPS), Mokinių registro, STEKAS „Personalo darbo laiko apskaitos ir atostogų“ posistemės ir Gyventojų registro. Vyr. buhalteris turi prieigas prie STEKAS, NAVISION, FINNET, Registrų centro, Valstybinio socialinio draudimo ir Valstybinės mokesčių inspekcijos sistemų, bankų ir VSAKIS. Prie dokumentų valdymo sistemos „Kontora“ prieigas turi visi įstaigos darbuotojai. Kiekvienas darbuotojas įgaliotas dirbti su asmens duomenimis žino savo prieigos ir tvarkomų duomenų apimtis ir yra pasirašę konfidencialumo pasižadėjimą.

8. Prieigos teisių užsakymas yra griežtai kontroliuojamas ir vyksta pagal numatytą procedūrą. Prisijungimo prie informacinių sistemų DVS „Kontora“ ir Elektroninis dienynas identifikavimas vyksta naudojant slaptažodžius ir jie yra administruojami pagal nustatytas taisykles: sudėtingumo (ne mažiaus nei 8 simboliai, susidedantys ne tik iš raidžių, bet ir bent vieno skaičiaus ir bent vieno simbolio), keitimo dažnumo (kas 3 mėnesiai), naikinimo, priminimo, saugojimo. Vartotojui būnant neaktyviam nustatytą laiką, informacinė sistema turi automatinio išjungimo funkciją iš sistemos, kurią aktyvavus, iš naujo įvedamas slaptažodis. Sistemos slaptažodžių keitimo tvarką vykdo patys sistemos administratoriai. Kiekvienas darbuotojas, kuris turi prieigą prie asmens duomenų yra atsakingas už slaptažodžio konfidencialumą ir įsipareigoja jo neatskleisti tretiesiems asmenims.

9. Pasikeitus darbuotojui dirbusiam su asmens duomenimis, prieigos slaptažodžiai prie duomenų bazės iš karto pakeičiami.

10. Asmens duomenis, siunčiamu elektroniniu paštu apsaugoti labai sunku. Įstaiga informacinėmis technologijomis naudojasi kai asmens duomenų siuntimas elektroniniu paštu yra būtinas ir neišvengiamas. Beveik visa elektroniniu paštu perduodama informacija yra siunčiama tarp valstybinių institucijų arba įkeliama ir perduodama per bendrai naudojamas programas. Jei asmens duomenys yra gaunami elektroniniu paštu, jų skaitmeninės arba popierinės kopijos pagal reikalavimus archyvuojamos arba naikinamos, o elektroniniame pašte gauti duomenys yra ištrinami.

11. Visi Įstaigos darbuotojai naudoja dokumentų valdymo sistemą „Kontora“, kurioje naudotojo prisijungimo duomenys (naudotojo vardas ir slaptažodis), vienareikšmiškai identifikuojantys konkretų darbuotoją laikomi elektroniniu parašu ir turi tokią pačią juridinę galią kaip ir parašas įstaigos rašytiniuose vidaus dokumentuose. Naudojami valstybiniai registrai yra prieinami tik įgaliotiems darbuotojams prisijungti su savo prisijungimų duomenimis iš bet kurio kompiuterio, prieš tai pasirašius konfidencialumo pasižadėjimus registrus prižiūrinčioms įstaigoms.

12. Įstaigos internetinę svetainę ir socialinę paskyrą prižiūri direktoriaus pavaduotojas ugdymui. Į internetinę svetainę yra keliama visa būtina informacija ir renginių nuotraukos, prieš tai gavus ugdytinių tėvų ar kitų teisėtų atstovų sutikimus dėl vaizdo duomenų naudojimo.

13. Komunikacijai naudojamose susirašinėjimo programose, esant galimybei, rekomenduojama aktyvuoti ištisinio šifravimo nuostatas. BDAR 32 straipsnis numato, kad atsižvelgdamas į techninių galimybių išsivystymo lygį, įgyvendinimo sąnaudas bei duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus, taip pat duomenų tvarkymo keliamus įvairios tikimybės ir rimtumo pavojus fizinių asmenų teisėms ir laisvėms, duomenų valdytojas ir duomenų tvarkytojas įgyvendina tinkamas technines ir organizacines priemones, kad būtų užtikrintas pavojų atitinkančio lygio saugumas, įskaitant, inter alia, jei reikia:

13.1. pseudonimų suteikimą asmens duomenims ir jų šifravimą;

13.2. gebėjimą užtikrinti nuolatinį duomenų tvarkymo sistemų ir paslaugų konfidencialumą, vientisumą, prieinamumą ir atsparumą;

13.3. gebėjimą laiku atkurti sąlygas ir galimybes naudotis asmens duomenimis fizinio ar techninio incidento atveju;

13.4. reguliarų techninių ir organizacinių priemonių, kuriomis užtikrinamas duomenų tvarkymo saugumas, tikrinimo, vertinimo ir veiksmingumo vertinimo procesą.

14. Kaip viena iš duomenų saugos priemonių kompiuterių tinkluose gali būti naudojamas kompiuterių tinklų, tinkle teikiamų paslaugų ir sistemų bei naudotojų atskyrimas. Tinklo atskyrimas gali būti atliekamas naudojant fiziškai atskirus tinklus arba skirtingus loginius tinklus. Darbuotojų, įgaliotų dirbti su asmens duomenimis, kompiuteriai nėra sujungti į vidinį tinklą, kompiuteriai yra apsaugoti skirtingais slaptažodžiais.

15. Įstaigoje belaidžiais tinklais turėtų naudotis tik personalas. Dėl sunkai apibrėžiamų tinklų ribų, belaidžiams tinklams reikalinga speciali saugos politika. Kai tvarkomi asmens duomenys, prieš suteikiant prieigą prie vidaus sistemų, reikėtų apsvarstyti galimybę visus belaidės prieigos bandymus laikyti išoriniu prisijungimu ir šią prieigą atskirti nuo vidaus tinklų, kol prieigos bandymą praleis saugiai sukonfigūruota tinklo ugniagesė. Siekiant už tikrinti, kad asmens duomenys nebūtų atskleisti, naudojant mobiliuosius įtaisus reikėtų laikytis ypatingo atsargumo.

16. Mobilieji įrenginiai gali išplėsti paslaugas, tačiau padidina riziką juose esančių duomenų nutekėjimui. Mobiliuosius įrenginius, tokius kaip planšetės ar išmanieji telefonai naudotojai gali panaudoti savo reikmėms, todėl reikia užtikrinti, kad naudotojų asmeniniai duomenys ir įstaigoje administruojami asmens duomenys nebūtų atskleisti. Mobiliuosiuose įrenginiuose turėtų veikti apsauga, leidžianti išvengti neteisėtos prieigos prie duomenų saugomų ir apdorojamų šiais įtaisais (PIN, slaptažodžiai, kriptografiniai raktai).

17. Atsarginių kopijų sistema yra esminis veiksnys, užtikrinantis įstaigos darbo ir procesų atstatymą įvykus duomenų praradimui ar sugadinimui. Domenų kopijų darymo dažnumas ir poreikis priklauso nuo Įstaigos ir joje apdorojamų duomenų.

18. Asmens duomenys keliami į valstybinius registrus, elektroninį dienyną, dokumentų valdymo sistemą yra ten saugomi pagal programos nustatymus. Direktoriaus pavaduotojas ugdymui metų gale užsako archyvą iš elektroninio dienyno, išsaugo į išorinę atminties laikmeną ir perduoda saugoti sekretoriui (saugoma 2 metus po programos baigimo).

19. Fizinės apsaugos priemonės turėtų būti numatytos ir naudojamos, siekiant apsaugoti vietas, kuriose laikomi konfidencialūs duomenys ar duomenų saugojimo bei apdorojimo priemonės. Pastatai ar vietos, kuriose yra duomenų apdorojimo priemonės, yra fiziškai patikimos, tų vietų išorinis stogas, sienos ir grindys yra iš vientisų konstrukcijų ir visos išorinės durys yra tinkamai apsaugotos nuo neteisėto patekimo valdymo mechanizmais (signalizacijomis ir spynomis). Kai nėra žmonių, durys ir langai yra užrakinti. Įstaigos valdomos duomenų apdorojimo priemonės yra fiziškai atskirtos nuo trečių šalių valdomos įrangos.

20. Saugumo zonos apsaugotos tinkamomis valdymo priemonėmis, kurios užtikrina nuolatinį personalo buvimą patalpose ir pašalinių asmenų nepatekimą į patalpas be personalo žinios. Nesant personalo, Įstaigos patalpos rakinamos ir saugomos signalizacija (sudaryta sutartis su saugos tarnyba).

21. Elektros maitinimo ir telekomunikacijų kabeliai, kuriais perduodami duomenys arba teikiamos paslaugos, yra apsaugoti nuo slapto prisijungimo, trukdžių ar pažeidimo. Siekiant išvengti trukdžių, elektros maitinimo kabeliai yra atskirti nuo ryšių (kompiuterių tinklo) kabelių. Be atitinkamo leidimo įranga, asmens duomenys arba programinė įranga negali būti išnešama iš įstaigos patalpų. Jeigu leidimas iš vadovo yra gautas, atsižvelgiant į rizikos įvertinimo rezultatus, įrangoje turi būti įdiegtos apsaugos priemonės. Asmens duomenų saugojimas išorinėse atminties laikmenose yra praktikuojamas archyvų išsaugojimui, papildomam informacijos išsaugojimui ar reikalingų dokumentų naudojimui kitose fizinėse vietose. Asmens duomenų kopijavimas yra griežtai reglamentuotas: reikalui esant saugoti atsargines asmens duomenų kopijas USB laikmenoje galima tik papildomai saugant informaciją ir laikmeną saugiai laikyti rakinamose patalpose.

22. Prieš sunaikinant ar pakartotinai naudojant IT įrangą, visi jo elementai, kuriose yra atminties, yra patikrinami, siekiant užtikrinti, kad visi konfidencialūs duomenys būtų sunaikinti arba saugiai perrašyti. Jei reikalinga, atmintinė su konfidencialia informacija turi būti fiziškai sunaikinta arba joje esanti informacija turi būti sunaikinta, ištrinta arba perrašyta naudojant būdus, skirtus pirminę informaciją paversti neatkuriama, o ne naudojant standartinę ištrynimo arba formavimo funkciją. Konfidencialių duomenų atskleidimo riziką galima sumažinti ne tik saugiuoju disko trynimu, bet ir viso disko šifravimu, jei šifravimo procesas yra pakankamai patikimas ir apima visą diską, o patys šifravimo raktai laikomi konfidencialiai (nesaugomi tame pačiame diske) ir yra pakankamai ilgi, kad atlaikytų bandymus juos „nulaužti“. Visas personalas yra informuojamas apie saugumo reikalavimus ir procedūras, taikomas be priežiūros paliekamai įrangai, ir apie jų atsakomybę už tokios paslaugos įgyvendinimą. Vartotojai turi atsijungti nuo taikomųjų programų ar tinklo paslaugų, kai jų nebereikia, apsaugoti kompiuterius ar mobiliuosius įrenginius nuo neleistino naudojimo, panaudojant prieigos slaptažodžius arba kitas tapatybės nustatymo priemones.

23. Popieriniams dokumentams ir keičiamosioms duomenų laikmenoms (USB atmintinėms, išoriniams standiesiems diskams, DVD laikmenoms) yra taikoma švaraus stalo politika. Taikant šią politiką, sumažėja neteisėtos prieigos prie duomenų, jų praradimo ir sugadinimo įprastu darbo laiku ir po jo rizikos. Svarbu nelaikyti dokumentų su asmens duomenimis pašaliniams asmenims pasiekiamoje vietoje.

24. Įstaigoje asmens duomenys saugomi Lietuvos vyriausiojo archyvaro rekomenduojamais dokumentų saugojimo terminais (Lietuvos vyriausiojo archyvaro 2011 m. kovo 9 d. įsakymas Nr. V-100 „Dėl bendrųjų dokumentų saugojimo terminų rodyklės patvirtinimo“). Suėjus duomenų tvarkymo terminui jie Įstaigoje sunaikinami Įstaigos direktoriaus įgalioto asmens arba įstatymų nustatyta tvarka perduodami į archyvą.

**III SKYRIUS**

**BAIGIAMOSIOS NUOSTATOS**

25. Asmens duomenų apsaugos įgyvendinimo priemonių įdiegimą įstaigoje kontroliuoja direktoriaus paskirtas darbuotojas.

26. Įstaigos vadovo įgalioti asmenys, kuriems suteikta teisė tvarkyti asmens duomenis, yra apmokyti tvarkyti asmens duomenis prieš asmens duomenų tvarkymą, turi darbo kompiuteriu įgūdžių, yra susipažinę su asmens duomenų saugą reglamentuojančiais teisės aktais, yra pasirašę konfidencialumo pasižadėjimus.

27. Už darbuotojų , kuriems suteikta teisė tvarkyti asmens duomenis, supažindinimą ir kitais asmens duomenų saugą įgyvendinančiais teisės aktais bei atsakomybe už šių reikalavimų nesilaikymą yra atsakingas Duomenų valdytojas.

28. Įstaigoje nėra vykdoma darbuotojų ryšių stebėsena. Svarstant incidentų rezultatus, būtina atsižvelgti į darbuotojų nuomonę, jų teikiamus pasiūlymus asmens duomenų apsaugai Įstaigoje, užtikrinti.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_