PATVIRTINTA
Kelmės rajono Kražių Žygimanto Liauksmino
pagrindinės mokyklos
2025 m. gruodžio 1 d.
direktoriaus įsakymu Nr. V1-154

KELMĖS RAJONO KRAŽIŲ ŽYGIMANTO LIAUKSMINO PAGRINDINĖS MOKYKLOS ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ NUSTATYMO, SUSTABDYMO (PAŠALINIMO), TYRIMO, PRANEŠIMO APIE JUOS IR DOKUMENTAVIMO TAISYKLĖS

1. BENDROSIOS NUOSTATOS

1.1. Kelmės rajono savivaldybės biudžetinės įstaigos, Kelmės rajono Kražių Žygimanto Liauksmino pagrindinės mokyklos administracija *(toliau – Įstaiga arba Duomenų valdytoja)* vadovaujantis Bendruoju Duomenų Apsaugos Reglamentu (ES) 2016/679 *(toliau - BDAR)*, Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu *(toliau - ADTAĮ)* ir kitais Europos sąjungos ir Lietuvos Respublikos teisės aktais, reguliuojančiais duomenų apsaugą ir tvarkymą, siekiant tinkamai įgyvendinti BDAR reikalavimus, šiose taisyklėse *(toliau – Taisyklės)* nustato asmens duomenų saugumo pažeidimų nustatymo, sustabdymo (pašalinimo), tyrimo, pranešimo apie juos ir dokumentavimo tvarką.

1.2. Taisyklių tikslas – reglamentuoti Įstaigoje atliekamų asmens duomenų saugumo pažeidimų nustatymo, sustabdymo (pašalinimo), tyrimo, pranešimo apie juos ir dokumentavimo tvarką, nustatyti ir aprašyti pagrindinius Įstaigos administracijos veiksmus asmens duomenų saugumo pažeidimo atveju.

1.3. Taisyklėse nustatoma ir aprašoma:

a) kas yra asmens duomenų saugumo pažeidimai;

b) kokiems asmenims privaloma pranešti apie galimą asmens duomenų saugumo pažeidimą;

c) kaip turi vykti asmens duomenų saugumo pažeidimo tyrimas;

d) pareiga pateikti pranešimą Valstybinei asmens duomenų apsaugos inspekcijai (priežiūros institucijai) ne vėliau kaip per 72 val. nuo sužinojimo apie pažeidimą;

e) kokiais atvejais pranešimas turi būti pateikiamas ir fiziniam asmeniui (duomenų subjektui), kurio asmens duomenys yra susiję su incidentu (pažeidimu);

f) asmens duomenų saugumo pažeidimų dokumentavimo pareiga.

2. TAISYKLĖSE VARTOJAMOS PAGRINDINĖS SĄVOKOS

2.1. Šiose Taisyklėse vartojamos sąvokos suprantamos taip, kaip jos yra apibrėžtos BDAR , ADTAĮ ir kituose Europos Sąjungos ir Lietuvos Respublikos teisės aktuose.

2.2. **Privatumo ir asmens duomenų apsaugos politika** – Privatumo ir asmens duomenų apsaugos politikos nuostatos, kurių Įstaigos administracija, kaip Duomenų valdytoja, laikosi.

2.3. **Duomenų valdytoja** – Kelmės rajono savivaldybės biudžetinė įstaiga, Kelmės rajono Kražių Žygimanto Liauksmino pagrindinė mokykla, įmonės kodas 190093592, buveinės ir korespondencijos adresas: Dariaus ir S. Girėno g. 2 Kražiai, LT-86285, Kelmės raj., tel. Nr.: +370 427 60020, Mob. tel. Nr.: +370 616 25774, el. paštas: kraziai@zlmokykla.lt, kuri šiose taisyklėse nustato asmens duomenų saugumo pažeidimų nustatymo, tyrimo, dokumentavimo, asmens duomenų saugumo pažeidimų sustabdymo (pašalinimo), pranešimo apie asmens duomenų saugumo pažeidimą ir Įstaigos administracijos veiksmus asmens duomenų saugumo pažeidimo atveju.

2.4. **Asmens duomenys** – bet kokią informaciją apie gyvą fizinį asmenį (Duomenų subjektą), kurio tapatybė Įstaigos administracijai yra žinoma arba gali būti tiesiogiai ar netiesiogiai nustatyta pasinaudojant tokiais Duomenų subjekto duomenimis kaip vardas, pavardė, gimimo data, asmens kodas, gyvenamosios vietos adresas, asmens tapatybės kortelės ar paso numeris, banko kortelės numeris, duomenys apie sveikatą, veido atvaizdas, vaizdo įrašas, asmeninio telefono numeris, asmeninio elektroninio pašto adresas, interneto protokolo (IP) adresas, asmeninio automobilio numeris arba kitais tik fiziniam asmeniui (Duomenų subjektui) būdingais požymiais.

2.5. **Duomenų subjektas** – gyvas fizinis asmuo, kurio tapatybė Įstaigos administracijai yra žinoma arba gali būti tiesiogiai ar netiesiogiai nustatyta ir kurio asmens duomenis Įstaigos administracija, kaip Duomenų valdytoja, valdo ir tvarko konkrečiai nustatytais tikslais.

2.6. **Už asmens duomenų tvarkymą atsakingas Įstaigos darbuotojas** – Įstaigos darbuotojas, kuris pagal darbo sutartį, užimamas pareigas, darbo pobūdį ir jam suteiktus įgaliojimus turi teisę vykdyti konkrečias su Duomenų subjektų asmens duomenų tvarkymu susijusias funkcijas Įstaigos vardu.

2.7. **Duomenų tvarkymas** – bet kuris automatizuotomis arba neautomatizuotomis priemonėmis su Duomenų subjektų asmens duomenimis atliekamas veiksmas: rinkimas, užrašymas, kaupimas, saugojimas, keitimas (papildymas ar taisymas), teikimas, naudojimas, naikinimas ar kitoks veiksmas arba veiksmų rinkinys.

2.8. **Duomenų tvarkytojas** – fizinis arba juridinis asmuo, valdžios institucija, agentūra ar kita įstaiga, kuri pagal sutartį Įstaigos (Duomenų valdytojo) vardu tvarko Duomenų subjektų asmens duomenis ir/ar padeda Įstaigos administracijai pagal jam suteiktus įgaliojimus įgyvendinti asmens duomenų tvarkymui nustatytus tikslus.

2.9. **Internetinė svetainė** – Įstaigos internetine svetainė esanti adresu: https://www.mokyklazl.lt, kurioje Įstaigos internetinės svetainės lankytojas, Įstaigos mokinio (vaiko) tėvai bei globėjai, Įstaigos darbuotojas, klientas ar kitas Duomenų subjektas bet kuriuo metu gali susipažinti su Įstaigos asmens duomenų tvarkymo taisyklėmis ir kitais Įstaigos lokaliniais teisės aktais, pateikti Įstaigos administracijai prašymą, užklausą, užsakymą arba duoti Įstaigos administracijai savo sutikimą tvarkyti asmens duomenis sutarties sudarymo, vykdymo, apskaitos ir kitais konkrečiai nustatytais tikslais.

2.10. **Susistemintas rinkinys** – Įstaigos bet kuris susistemintas pagal specialius kriterijus prieinamų asmens duomenų rinkinys, kuris gali būti centralizuotas, decentralizuotas arba suskirstytas funkciniu ar geografiniu pagrindu.

2.11. **Duomenų subjekto sutikimas** – bet koks laisva valia Įstaigos administracijai duotas, konkretus, nedviprasmiškas ir tinkamai informuoto Duomenų subjekto valios išreiškimas pareiškimu arba vienareikšmiais veiksmais, kuriais jis sutinka, kad Įstaigoje būtų tvarkomi su juo susiję asmens duomenys konkrečiai nustatytais tikslais.

2.12. **Duomenų gavėjas** – fizinis arba juridinis asmuo, valdžios institucija, agentūra ar kita įstaiga, kuriai atskleidžiami Duomenų subjektų asmens duomenys, nesvarbu, ar tai trečioji šalis, ar ne.

2.13. **Valdžios institucijos ir įstaigos** – Lietuvos Respublikos valstybės ir savivaldybių institucijos ir įstaigos, įmonės ir viešosios įstaigos, finansuojamos iš valstybės ar savivaldybių biudžetų bei valstybės pinigų fondų ir Lietuvos Respublikos viešojo administravimo įstatymo nustatyta tvarka įgaliotos atlikti viešąjį administravimą arba teikiančios asmenims viešąsias ar administracines paslaugas ar vykdančios kitas viešąsias funkcijas.

2.14. **Trečioji šalis** – fizinis arba juridinis asmuo, valdžios institucija, agentūra ar kita įstaiga kuri nėra kokios nors sutarties, susitarimo su Įstaigos administracija šalis ar ginčo su Įstaigos administracija dalyvis ir kuriems tiesioginiu Įstaigos direktoriaus įgaliojimu leidžiama susipažinti su Įstaigoje tvarkomais Duomenų subjektų asmens duomenimis.

2.15. **Skundas** – Duomenų subjekto rašytinis kreipimasis į Įstaigos administraciją, kuriame nurodoma, kad yra pažeistos Duomenų subjekto teisės ar teisėti interesai ir prašoma juos apginti.

2.16. **Ginčas** – Duomenų subjekto ir Įstaigos administracijos konfliktas, kuris grindžiamas pažeistais Duomenų subjekto ar Įstaigos teisiniais interesais.

2.17. **Priežiūros institucija** – Valstybinė asmens duomenų apsaugos inspekcija (toliau – VDAI). Įstaigos kontaktai: L. Sapiegos g. 17, 10312 Vilnius (Įėjimas iš kairės pusės) Tel. (0 5) 271 28 04, (0 5) 2791445. Faks. (0 5) 261 94 94. El. paštas: ada@ada.lt, E. pristatymo dėžutė: 188607912.

3. ASMENS DUOMENŲ SAUGUMO PAŽEIDIMAS

3.1. Asmens duomenų saugumo pažeidimas - Duomenų subjektų asmens duomenų saugumo pažeidimas, dėl kurio netyčia arba neteisėtai Duomenų subjektų asmens duomenys Įstaigoje sunaikinami, prarandami, be Įstaigos direktoriaus leidimo pakeičiami, atskleidžiami, buvo persiųsti kitiems asmenims arba Duomenų subjektų asmens duomenys Įstaigoje saugomi ir tvarkomi kitaip nei nustatyta BDAR, ADTAĮ ir kituose Europos Sąjungos ir Lietuvos Respublikos teisės aktuose, Įstaigos taisyklėse ir/ar prie jų be Įstaigos direktoriaus leidimo buvo suteikta prieiga.

3.2. Asmens duomenų saugumo pažeidimas pagal savo pobūdį gali būti konfidencialumo, vientisumo ir prieinamumo pažeidimas.

3.3. Konfidencialumo pažeidimas – neleistinas arba netyčinis Duomenų subjektų asmens duomenų atskleidimas arba prieigos prie asmens duomenų suteikimas.

3.4. Vientisumo pažeidimas – neleistinas arba netyčinis Duomenų subjektų asmens duomenų pakeitimas.

3.5. Prieinamumo pažeidimas – netyčinis arba neleistinas prieigos prie Duomenų subjektų asmens duomenų praradimas arba asmens duomenų sunaikinimas.

3.6. Priklausomai nuo aplinkybių, asmens duomenų saugumo pažeidimas tuo pat metu gali sietis su asmens duomenų konfidencialumu, prieinamumu ir vientisumu ar su kuriuo nors jų deriniu.

3.7. Įstaigos administracija ir Įstaigos darbuotojai, tvarkantys Duomenų subjektų asmens duomenis Įstaigos vardu, sužinojęs apie asmens duomenų saugumo pažeidimą, nedelsiant organizuoja pažeidimo tyrimą, kad būtų nustatytas pažeidimo pobūdis, tipas, aplinkybės, apytikslis asmens duomenų kuriu saugumas pažeistas, skaičius, asmens duomenų kategorijos ir apimtis, tikėtinos asmens duomenų saugumo pažeidimo pasekmės, pavojus Duomenų subjektų teisėms ir laisvėms ir imasi priemonių pažeidimui pašalinti ir neigiamoms pažeidimo pasekmėms sumažinti.

4. ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ DOKUMENTAVIMAS IR TYRIMAS

4.1. Siekiant tinkamai įgyvendinti BDAR, ADTAĮ ir kituose Europos sąjungos ir Lietuvos Respublikos teisės aktuose nustatytus reikalavimus ir atsižvelgiant į Įstaigoje atliekamus asmens duomenų tvarkymo tikslus ir veiksmus, Įstaigos direktorius savo įsakymu paskiria Įstaigos darbuotoją, atsakingą už asmens duomenų saugumo pažeidimų valdymą, tyrimą, pranešimų VDAI ir Duomenų subjektams teikimą, prevencinių priemonių įdiegimo kontrolę Įstaigoje *(toliau – Atsakingas asmuo)* ir nustato, kas ir kaip registruoja asmens duomenų saugumo pažeidimus, kur ir kokia forma asmens duomenų saugumo pažeidimų žurnalas ar registras Įstaigoje pildomas, kiek laiko saugomas ir kokia informacija turėtų būti jame įrašyta.

4.2. Įstaigos direktorius ir Įstaigos skyrių ir/ar padalinių vadovai privalo informuoti ir instruktuoti visus Įstaigos darbuotojus tvarkančius Duomenų subjektų asmens duomenis Įstaigos vardu, apie jų pareigą per 24 val. pranešti apie visus galimus pažeidimus tiesiogiai Įstaigos direktorių ir supažindinti Įstaigos darbuotojus su BDAR, ADTAĮ ir Įstaigos taisyklių reikalavimais ir jose nustatyta pranešimų apie asmens duomenų saugumo pažeidimus pateikimo tvarka.

4.3. Įstaigos direktorius, Įstaigos skyrių ir/ar padalinių vadovai ir darbuotojai privalo apie asmens duomenų saugumo pažeidimą taip pat informuoti ir Įstaigos duomenų apsaugos pareigūną *(jeigu toks yra paskirtas)* bei laiku ir tinkamai suteikti jam visą informaciją, susijusią su galimu asmens duomenų saugumo pažeidimu. Reikalui esant konsultuojasi su duomenų apsaugos pareigūnu *(jeigu toks yra paskirtas)* dėl tolimesnių veiksmų, susijusių su pažeidimu.

4.4. Įstaigos darbuotojai, tvarkantis Duomenų subjektų asmens duomenis Įstaigos vardu, nustatęs galimą asmens duomenų saugumo pažeidimą arba sužinojęs apie galimą asmens duomenų saugumo pažeidimą iš duomenų tvarkytojo, žiniasklaidos ar kito šaltinio, privalo nedelsdamas (bet

ne ilgiau kaip per 24 val.) apie tai pranešti Įstaigos direktoriui žodžiu, raštu ar elektroninėmis priemonėmis ir informuoti Įstaigos duomenų apsaugos pareigūną *(jeigu toks yra paskirtas).*

4.5. Už asmens duomenų saugumo pažeidimų valdymą ir tyrimą Įstaigoje paskirtas atsakingas darbuotojas, visus su Duomenų subjektų asmens duomenų saugumo pažeidimu susijusius faktus, jų poveikį, taisomuosius veiksmus, kurių buvo imtasi, registruoja Įstaigos asmens duomenų saugumo pažeidimų registracijos žurnale arba registre nepriklausomai nuo to, ar apie juos buvo pranešta VDAI ir Duomenų subjektui ar ne.

4.6. Už Duomenų subjektų asmens duomenų saugumo pažeidimų valdymą ir tyrimą Įstaigoje atsakingas darbuotojas, sužinojęs apie galimą pažeidimą, nedelsiant (bet ne ilgiau kaip per 5 darbo dienas) įrašo į Įstaigos asmens duomenų saugumo pažeidimų registracijos žurnalą (registrą) asmens duomenų saugumo pažeidimo faktą ir kaip įmanoma greičiau atlieka pirminį tyrimą, išsiaiškina ir nustato, ar asmens duomenų saugumo pažeidimas iš tikrųjų įvyko, įvertina galimą riziką ir kokios galimos pasekmės Duomenų subjektui (Duomenų subjektams) ir apie asmens duomenų saugumo pažeidimo faktą praneša Įstaigos direktoriui ir informuoja Įstaigos duomenų apsaugos pareigūną *(jei toks yra paskirtas)*. Reikalui esant konsultuojasi su duomenų apsaugos pareigūnu *(jeigu toks yra paskirtas)* dėl tolimesnių veiksmų, susijusių su pažeidimu.

4.7. Įstaigos asmens duomenų saugumo pažeidimų registracijos žurnale arba registre nurodoma:

a) pažeidimo data ir vieta;
b) kas pranešė apie pažeidimą;
c) kas konkrečiai įvyko;
d) kieno ir kokie asmens duomenys pažeisti;
e) kokie yra su pažeidimu susiję faktai;
f) kokia pažeidimo priežastis, poveikis ir pasekmės;
g) kokie veiksmai yra atlikti pažeidimui pašalinti ar kurių buvo imtasi;
h) ar buvo pranešta apie pažeidimą VDAI;
i) ar buvo pranešta apie pažeidimą Duomenų subjektui;
j) kas priėmė sprendimą nepranešti apie pažeidimą VDAI ir Duomenų subjektui ir kodėl; (Pvz., Pažeidimas negali sukelti pavojaus fizinių asmenų teisėms ir laisvėms, arba kokią sąlygą įvykdė, kuomet pranešti apie pažeidimą duomenų subjektui nereikia.)
k) jeigu pranešimą vėluojama pateikti VDAI ar pranešimas teikiamas etapais nurodyti pranešimo VDAI pateikimo vėlavimo priežastį;
l) kur ir kiek laiko saugoma asmens duomenų saugumo pažeidimo tyrimo medžiaga;
m) įrašoma kita reikšminga informacija susijusi su asmens duomenų saugumo pažeidimu.

4.8. Įstaigos asmens duomenų saugumo pažeidimų registracijos žurnalas arba registras tvarkomas raštu, įskaitant elektronine formą ir saugomas pagal Įstaigoje patvirtintą dokumentų saugojimo tvarką. Esant būtinybei, Įstaigos asmens duomenų saugumo pažeidimų žurnale arba registre esanti informacija papildoma ir/ar koreguojama.

4.9. Už Duomenų subjektų asmens duomenų saugumo pažeidimų valdymą ir tyrimą atsakingas Įstaigos darbuotojas privalo periodiškai peržiūrėti Įstaigos asmens duomenų saugumo pažeidimų registracijos žurnale ar registre esančius įrašus ir numatyti, kokios prevencijos priemonės yra ar turėtų būti įgyvendintos, kad ateityje analogiški pažeidimai nesikartotų Įstaigoje ir kontroliuoti prevencijos priemonių įdiegimą.

4.10. Remdamasi Įstaigos asmens duomenų saugumo pažeidimų registracijos žurnale arba registre pateikta informacija, VDAI pareigūnai ar Įstaigos duomenų apsaugos pareigūnas *(jei toks yra paskirtas)* turi galėti patikrinti, kaip buvo įgyvendinama Įstaigos (Duomenų valdytojo) prievolė pranešti apie asmens duomenų saugumo pažeidimus VDAI ir Duomenų subjektams.

4.11. Už Duomenų subjektų asmens duomenų saugumo pažeidimų valdymą ir tyrimą atsakingas Įstaigos darbuotojas, privalo imtis visų tinkamų techninių ir organizacinių priemonių, kad asmens duomenų saugumo pažeidimas Įstaigoje būtų išsamiai ištirtas ir pašalintas (sustabdytas,

ištaisytas) bei ateityje nepasikartotų. Už Duomenų subjektų asmens duomenų saugumo pažeidimų valdymą ir tyrimą atsakingas Įstaigos darbuotojas, atliekant pirminį tyrimą ir siekiant nustatyti, ar asmens duomenų saugumo pažeidimas Įstaigoje iš tikrųjų įvyko, dokumentuoja visus su asmens duomenų saugumo pažeidimu susijusius faktus, jo poveikį ir taisomuosius veiksmus, kurių buvo imtasi.

4.12. Už Duomenų subjektų asmens duomenų saugumo pažeidimų valdymą ir tyrimą atsakingas Įstaigos darbuotojas vertinant riziką, kuri gali atsirasti dėl asmens duomenų saugumo pažeidimo, turi atsižvelgti į konkrečias asmens duomenų saugumo pažeidimo aplinkybes, pavojaus Duomenų subjektų teisėms ir laisvėms atsiradimo tikimybę ir rimtumą. Rizika turėtų būti vertinama objektyviai atsižvelgiant į šiuos kriterijus:

a) į pažeidimo tipą;
b) asmens duomenų pobūdį ir apimtį;
c) kaip lengvai identifikuojamas fizinis asmuo (Duomenų subjektas);
d) pasekmių rimtumą fiziniams asmenims (Duomenų subjektams);
e) ar pažeidimas gali sukelti pavojų fizinių asmenų (Duomenų subjektų) teisėms ir laisvėms;
f) ar fiziniai asmenys (Duomenų subjektai) gali patirti materialinę ar nematerialinę žalą;
g) ar fiziniai asmenys (Duomenų subjektai) gali prarasti savo asmens duomenų kontrolę;
h) ar fiziniai asmenys (Duomenų subjektai) gali patirti teisių apribojimą ar diskriminaciją;
i) ar gali būti pavogta ar suklastota fizinių asmenų (Duomenų subjektų) tapatybė;
j) ar gali būti pakenkta fizinių asmenų (Duomenų subjektų) reputacijai;
k) ar pažeidimas gali sukelti pavojų fizinio asmens (Duomenų subjekto) savybes pakeitimui;
l) nukentėjusiųjų fizinių asmenų(Duomenų subjektų) skaičių.

Vertinant galimas rizikas, turėtų būti laikoma, kad asmens duomenų saugumo pažeidimas, galintis kelti pavojų Duomenų subjektų teisėms ir laisvėms yra toks, dėl kurio, laiku nesiėmus tinkamų priemonių, Duomenų subjektai gali patirti materialinę ar nematerialinę žalą, prarasti savo asmens duomenų kontrolę, patirti teisių apribojimą, diskriminaciją, gali būti pavogta ar suklastota jų asmens tapatybė, pakenkta jų reputacijai, prarastas asmens duomenų, kurie Įstaigoje saugomi, konfidencialumas arba padaryta kita ekonominė ar socialinė žala atitinkamam Duomenų subjektui.

4.13. Objektyviai įvertinęs asmens duomenų saugumo pažeidimo aplinkybės ir rizikos Duomenų subjektų teisėms bei laisvėms turi būti aiškiai nustatyta, kad yra:

a) žema rizikos tikimybė;
b) vidutinė rizikos tikimybė;
c) didelė (aukšta) rizikos tikimybė.

4.14. Už asmens duomenų saugumo pažeidimų valdymą ir tyrimą atsakingas Įstaigos darbuotojas, įvertinęs asmens duomenų saugumo pažeidimo aplinkybės ir rizikos Duomenų subjektų teisėms bei laisvėms, išvadą ir pasiūlymus dėl tolimesnių veiksmų, susijusių su asmens duomenų saugumo pažeidimu, nedelsdamas pateikia Įstaigos direktoriui.

4.15. Įstaigos direktorius įvertinęs pateiktą išvadą ir pasiūlymus, priima galutinį sprendimą dėl tolimesnių veiksmų, susijusių su asmens duomenų saugumo pažeidimu, kad pažeidimas būtų išsamiai ištirtas ir kuo greičiau būtų pašalintas bei ateityje Įstaigoje nepasikartotų. Reikalui esant Įstaigos direktorius konsultuojasi su Įstaigos duomenų apsaugos pareigūnu *(jei toks yra paskirtas)* arba su VDAI pareigūnų dėl tolimesnių veiksmų, susijusių su asmens duomenų saugumo pažeidimu, kad pažeidimas būtų išsamiai ištirtas ir pašalintas.

4.16. Jeigu tiriant asmens duomenų saugumo pažeidimą pradžioje nustatoma, kad nėra pavojaus Duomenų subjektų teisėms ir laisvėms, tačiau detalesnio pažeidimo tyrimo metu nustatoma,

kad toks pavojus gali jiems kilti, už asmens duomenų saugumo pažeidimų valdymą ir tyrimą Įstaigoje atsakingas darbuotojas privalo tokia riziką vertinti iš naujo ir Įstaigos direktoriui pateikti galutinę išvadą ir pasiūlymą dėl tolimesnių veiksmų, susijusių su asmens duomenų saugumo pažeidimu, kad toks pažeidimas būtų išsamiai ištirtas ir pašalintas bei ateityje Įstaigoje nepasikartotų. Reikalui esant už asmens duomenų saugumo pažeidimų valdymą ir tyrimą atsakingas Įstaigos darbuotojas konsultuojasi su duomenų apsaugos pareigūnu *(jei toks yra paskirtas)* arba su VDAI pareigūnų dėl tolimesnių veiksmų, susijusių su asmens duomenų saugumo pažeidimu, kad pažeidimas būtų tinkamai ir išsamiai ištirtas ir pašalintas.

5. PRANEŠIMAI APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMUS PRIEŽIŪROS INSTITUCIJAI

5.1. Pranešimai apie Duomenų subjektų asmens duomenų saugumo pažeidimus Lietuvos Respublikos Valstybinei duomenų apsaugos inspekcijai *(toliau – VDAI)* ir Duomenų subjektams, teikiami vadovaujantis BDAR 33 ir 34 straipsniais.

5.2. Nustačius, kad asmens duomenų saugumo pažeidimas Įstaigoje buvo ir, kad yra rizika Duomenų subjektų (fizinių asmenų) teisėms ir laisvėms, už asmens duomenų saugumo pažeidimų valdymą ir tyrimą atsakingas Įstaigos darbuotojas atlikus pirminį tyrimą, įvertinęs asmens duomenų saugumo pažeidimo aplinkybės ir rizikos Duomenų subjektų teisėms bei laisvėms ir gavus Įstaigos direktoriaus galutinį sprendimą nedelsdamas, ne vėliau kaip per 72 val., apie asmens duomenų saugumo pažeidimą praneša VDAI pagal nustatytą pranešimo formą *(Priedas Nr.1)*

5.3. Jeigu, priklausomai nuo asmens duomenų saugumo pažeidimo pobūdžio, būtina atlikti išsamesnį tyrimą ir nustatyti visus svarbius faktus, susijusius su asmens duomenų saugumo pažeidimu, ir per 72 val. nuo sužinojimo asmens duomenų saugumo pažeidimą dėl objektyvių aplinkybių to padaryti neįmanoma, pranešimas VDAI bei reikalingą informaciją gali būti teikiama etapais. Apie informacijos teikimą etapais, atlikus pirminį tyrimą ir gavus Įstaigos direktoriaus sprendimą už asmens duomenų saugumo pažeidimų valdymą ir tyrimą atsakingas Įstaigos darbuotojas apie tai informuoja VDAI teikiant pirminį pranešimą apie asmens duomenų saugumo pažeidimą Įstaigoje.

5.4. Jeigu po pranešimo VDAI pateikimo, atlikus tolesnį tyrimą, yra nustatoma, kad asmens duomenų saugumo pažeidimas Įstaigoje buvo sustabdytas arba faktiškai Įstaigoje nebuvo jokio asmens duomenų saugumo pažeidimo, už asmens duomenų saugumo pažeidimų valdymą ir tyrimą atsakingas Įstaigos darbuotojas išvadą pateikia Įstaigos direktoriui ir gavus Įstaigos direktoriaus galutinį sprendimą nedelsiant informuoja apie tai VDAI ir padaro įrašą Įstaigos asmens duomenų saugumo pažeidimų registracijos žurnale arba registre.

5.5. Jeigu Įstaigoje įvykusio asmens duomenų saugumo pažeidimas paveikia Duomenų subjektų (fizinių asmenų) asmens duomenis daugiau negu vienoje Europos Sąjungos valstybėje, tuomet Įstaigos direktorius apie asmens duomenų saugumo pažeidimą Įstaigoje privalo pranešti VDAI bei nurodyti, kad asmens duomenų saugumo pažeidimas apima ir kitose Europos Sąjungos valstybėse esančius Duomenų subjektų asmens duomenų saugumą. Už asmens duomenų saugumo pažeidimų valdymą ir tyrimą atsakingas Įstaigos darbuotojas apie tokį VDAI informavimą padaro įrašą Įstaigos asmens duomenų saugumo pažeidimų registracijos žurnale arba registre. Šiuo atveju VDAI informavimas apie asmens duomenų saugumo pažeidimą neatleidžia Įstaigos administracija nuo pareigos informuoti apie asmens duomenų saugumo pažeidimą ir Duomenų subjektus.

6. PRANEŠIMAI APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMUS DUOMENŲ SUBJEKTUI

6.1 Nustačius, kad asmens duomenų saugumo pažeidimas Įstaigoje buvo ir, kad yra didelė rizika Duomenų subjektų (fizinių asmenų) teisėms ir laisvėms, už asmens duomenų saugumo pažeidimų valdymą ir tyrimą atsakingas Įstaigos darbuotojas gavęs Įstaigos direktoriaus galutinį sprendimą nedelsdamas, ne vėliau kaip per 72 val. apie asmens duomenų saugumo pažeidimą

Įstaigoje praneša Duomenų subjektui (fiziniam asmeniui), kurio teisėms ir laisvėms dėl šio asmens duomenų saugumo pažeidimo gali kilti didelis pavojus.

6.2. Pranešime Duomenų subjektui (fiziniam asmeniui) aiškia ir paprasta kalba turėtų būti pateikiama:

a) asmens duomenų saugumo pažeidimo pobūdžio aprašymas;

b) tikėtinų asmens duomenų saugumo pažeidimo pasekmių Duomenų subjektui aprašymas;

c) priemonių, kurių Įstaigos administracija ėmėsi arba pasiūlė imtis, kad būtų pašalintas asmens duomenų saugumo pažeidimas, aprašymas;

d) kita reikšminga informacija, susijusi su asmens duomenų saugumo pažeidimu, kuri turėtų būti pateikta Duomenų subjektui (fiziniam asmeniui);

e) už asmens duomenų saugumo pažeidimų valdymą ir tyrimą atsakingo Įstaigos darbuotojo ir Įstaigos duomenų apsaugos pareigūno (jei toks yra paskirtas) kontaktiniai duomenys.

6.3. Duomenų subjektai apie jų asmens duomenų saugumo pažeidimą informuojami tiesiogiai, siunčiant jiems pranešimą el. paštu, SMS, paštu ar pan. Toks pranešimas turėtų būti atskirtas nuo kitos jiems siunčiamos informacijos ar standartiniu pranešimu.

6.4. Kai tiesioginio pranešimo Duomenų subjektui pateikimas pareikalautų neproporcingai daug Įstaigos administracijos pastangų apie įvykusį asmens duomenų saugumo pažeidimą gali būti paskelbiama viešai arba taikoma panaši priemonė, kuria Duomenų subjektai būtų informuojami taip pat efektyviai. *(Pvz., pranešimas Duomenų subjekto interneto svetainėje, SMS, el. paštu, žiniasklaidoje ar pan.)*

6.5. Už asmens duomenų saugumo pažeidimų valdymą ir tyrimą atsakingas Įstaigos darbuotojas turi pasirinkti tokius pranešimo Duomenų subjektui (fiziniam asmeniui) būdus, kurie maksimaliai didintų galimybę tinkamai pranešti apie asmens duomenų saugumo pažeidimą Įstaigoje arba gali pasirinkti kelis tokio pranešimo būdus.

6.6. Pranešimo Duomenų subjektui teikti nereikia, jeigu:

a) Įstaigos administracija jau įgyvendino tinkamas technines ir organizacines apsaugos priemones ir tokios priemonės taikytos ir Duomenų subjektų asmens duomenims, kuriems asmens duomenų saugumo pažeidimas Įstaigoje turėjo poveikio;

b) iš karto po asmens duomenų saugumo pažeidimo Įstaigos administracija ėmėsi tokiu priemonių, kuriomis užtikrinama, kad nebegalėtų kilti didelis pavojus Duomenų subjektų (fizinių asmenų) teisėms ir laisvėms;

c) arba toks pranešimas apie asmens duomenų saugumo pažeidimą, pareikalautų neproporcingai daug Įstaigos administracijos pastangų susisiekti su Duomenų subjektais. (Pvz., kai jų kontaktiniai duomenys buvo prarasti dėl pažeidimo arba nežinomi) Tokiu atveju apie asmens duomenų saugumo pažeidimą paskelbiama viešai arba taikoma panaši priemonė, kuria Duomenų subjektai būtų informuojami taip pat efektyviai.

6.7. Įstaigos administracija ir už asmens duomenų saugumo pažeidimų valdymą ir tyrimą atsakingas Įstaigos darbuotojas atliekant asmens duomenų saugumo pažeidimų tyrimą, privalo ne tik imtis veiksmų asmens duomenų saugumo pažeidimams pašalinti, bet ir tinkamai apie tai informuoti VDAI, Duomenų subjektus ir gebėti įrodyti, kad įvykdė duomenų saugumo pažeidimų dokumentavimo pareigą.

7. BAIGIAMOSIOS NUOSTATOS

7.1. Šios Taisyklės įsigalioja ir yra taikomos nuo Įstaigos direktoriaus įsakymo patvirtinimo datos ir galioja tol, kol nėra pakeistos ar atšauktos.

7.2. Už asmens duomenų saugumo pažeidimų valdymą ir tyrimą Įstaigos direktoriaus įsakymu paskirtas Įstaigos darbuotojas (-ai) su Taisyklėmis susipažindinamas pasirašytinai.

7.3. Už Taisyklių nuostatų laikymosi priežiūrą, jų vykdymo kontrolę bei periodišką peržiūrėjimą, ne rečiau kaip kartą per 2 metus, atsakingas Įstaigos direktoriaus įsakymu paskirtas Įstaigos administracijos darbuotojas, kuris, įvertinęs Taisyklių taikymo praktiką, esant poreikiui arba pasikeitus duomenų tvarkymą reglamentuojantiems teisės aktams, inicijuoja Taisyklių atnaujinimą.

_____