Klaipėdos rajono savivaldybės

asmens duomenų apsaugos politikos

5 priedas

|  |
| --- |
| **REAGAVIMO Į ASMENS DUOMENŲ SAUGUMO PAŽEIDIMUS PROCEDŪRA** |
|  |  |
| 1. **SĄVOKOS** |
| * 1. **Asmens duomenų saugumo pažeidimas** reiškia pažeidimą, dėl kurio netyčia arba neteisėtai sunaikinami, prarandami, pakeičiami, be leidimo atskleidžiami tvarkomi asmens duomenys arba prie jų be leidimo gaunama prieiga. |
| * 1. **Administracija** – Klaipėdos rajono savivaldybės administracija, juridinio asmens kodas: 188773688, buveinės adresas: Klaipėdos g. 2, Gargždai, kaip duomenų valdytojas. |
| * 1. **Savivaldybė -** Klaipėdos rajono savivaldybės administracija, Savivaldybės tarybos ir mero sekretoriatas, bei jose dirbantys valstybės tarnautojai ar darbuotojai, dirbantys pagal darbo sutartis, Meras, Mero pavaduotojai. |
| * 1. **Už duomenų saugą atsakingas asmuo** – Administracijos direktoriaus paskirtas darbuotojas, atsakingas už asmens duomenų saugumo pažeidimo procedūros vykdymą . |
| * 1. **Priežiūros institucija** reiškia valstybės narės pagal BDAR 51 straipsnį įsteigtą nepriklausomą valdžios instituciją. Lietuvos Respublikos atveju tokia institucija yra Valstybinė duomenų apsaugos inspekcija. |
| * 1. **Procedūra** reiškia šią Reagavimo į asmens duomenų saugumo pažeidimus procedūrą. |
|  |
| 1. **APIMTIS** |
| * 1. Ši procedūra taikoma įvykus asmens duomenų saugumo pažeidimui pagal BDAR 33 ir 34 straipsnius. |
| * 1. Šiame dokumente išdėstyta procedūra turėtų būti vadovaujamasi reaguojant į asmens duomenų saugumo pažeidimą, atsižvelgiant į konkrečios situacijos faktines aplinkybes. |
| 1. **ATSAKOMYBĖ** |
| * 1. Visi asmenys, turintys prieigą prie Savivaldybės tvarkomų asmens duomenų privalo žinoti ir vadovautis šia Procedūra duomenų saugumo pažeidimo atveju. |

|  |
| --- |
| 1. **PROCEDŪRA – DUOMENŲ SAUGUMO PAŽEIDIMO NUSTATYMAS IR ANALIZĖ** |
| * 1. Kaip ir galima spręsti iš Procedūros 1 punkte nurodyto asmens duomenų saugumo pažeidimo apibrėžimo, saugumo pažeidimu laikomas toks saugumo incidentas, dėl kurio įvyksta (konkretus pažeidimas gali patekti į daugiau nei vieną kategoriją): |
| * + 1. konfidencialumo pažeidimas – netyčia ar neteisėtai atskleidžiami asmens duomenys arba prie asmens duomenų suteikiama prieiga tam teisės neturintiems asmenims. Tokio pobūdžio pažeidimo pavyzdžiais galėtų būti asmens duomenų kopijos išsiuntimas trečiajam asmeniui, neturinčiam teisinio pagrindo juos gauti, prisijungimo prie duomenų bazės slaptažodžio paviešinimas ir pan.; |
| * + 1. pasiekiamumo pažeidimas – netyčia ar neteisėtai prarandama prieiga prie asmens duomenų arba duomenys yra sunaikinami. Tokio pobūdžio pažeidimu galėtų būti duomenų bazės ištrynimas nesant atsarginės kopijos, iš kurios būtų galima atkurti prarastus duomenis. Pasiekiamumo pažeidimu, kuris turėtų būti aprašytas, būtų ir laikinas įprastinę Savivaldybės veiklą sutrikdęs prieigos prie asmens duomenų praradimas; |
| * + 1. vientisumo pažeidimas – netyčia ar neteisėtai atliekami asmens duomenų pakeitimai. Tai galėtų būti trečiojo asmens, įgijusio neteisėtą prisijungimą prie duomenų bazės, įvykdyti joje esančių įrašų pakeitimai. |
| * 1. Kai yra nustatomas asmens duomenų saugumo pažeidimas, jį nustatęs Darbuotojas turi kuo skubiau informuoti už asmens duomenų saugą atsakingą asmenį asmeniškai, el. paštu, telefonu, ir / arba kitomis komunikacijos priemonėmis. |
| * 1. Už asmens duomenų saugą atsakingas asmuo atlieka pradinį vertinimą tam, kad nuspręstų dėl tinkamo veiksmų plano. Šis vertinimas turėtų apimti šiuos pagrindinius veiksnius: |
| * + 1. poveikio informacinių technologijų (toliau – IT) infrastruktūrai apimtis; |
| * + 1. informaciniai ištekliai, kuriems gali kilti arba yra kilęs pavojus (kokios duomenų bazės yra arba gali būti paveiktos); |
| * + 1. tikėtina asmens duomenų saugumo pažeidimo trukmė (kada prasidėjo ir kada buvo sustabdytas pažeidimas arba kaip skubiai tikėtina galima būtų tai padaryti); |
| * + 1. paveikti duomenų subjektai ir poveikio jiems apimtis (ar paveikti tik konkrečios duomenų subjektų grupės asmens duomenys, kokia konkrečios grupės dalis yra paveikta ir pan.); |
| * + 1. pradiniai asmens duomenų saugumo pažeidimo pasekmių požymiai (tai galėtų būti prieigos prie asmens duomenų praradimas, nustatyti neteisėti asmens duomenų pakeitimai, rasti paviešinti asmens duomenys ir pan.). |
| * 1. Aukščiau nurodyta informacija turėtų būti fiksuojama tokiu būdu, kad atliekant vėlesnę peržiūrą būtų galima susidaryti aiškų chronologišką suvokimą apie situacijos eigą ir priemones, kurių buvo imtasi. |
| * 1. Atsižvelgdamas į aukščiau aprašytą pradinę analizę, už asmens duomenų saugą atsakingas asmuo pagal Procedūros 12 punkte nurodytus kriterijus įvertina, ar asmens duomenų saugumo pažeidimo apimtis ir faktinis ar galimas poveikis lemia Reagavimo į asmens duomenų saugumo pažeidimus procedūros pradėjimą.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   * 1. Asmens duomenų saugumo pažeidimo nustatymo ir analizės schema:   **Asmens duomenų saugumo pažeidimo nustatymas ir analizė**  **Ar pradėti reagavimo į asmensduomenų saugumo pažeidimą procedūrą?**  **Apribojimas, likvidavimas ir atkūrimas**  **Pranešimas**  **Pranešimas duomenų valdytojui nuo duomenų tvarkytojo (Valdytojo procedūra)**  **Pranešimas duomenų subjektams**  **Pranešimas atsakingoms institucijoms**  **Ne**  **Taip**  **Procedūros užbaigimas**  **Asmens duomenų saugumo pažeidimo dokumentavimas**  **Duomenų saugumo pažeidimo dokumentavimas** |
| 1. **PROCEDŪRA – REAGAVIMO Į ASMENS DUOMENŲ SAUGUMO PAŽEIDIMUS PROCEDŪROS PRADĖJIMAS** |
| * 1. Formalus reagavimas į asmens duomenų saugumo pažeidimą visais atvejais turėtų būti pradėtas tada, jei nustatytos bet kurios iš toliau nurodytų aplinkybių: |
| * + 1. prarastas arba gali būti prarastas reikšmingas kiekis asmens duomenų; |
| * + 1. duomenų pažeidimas tikėtinai gali kelti didelį pavojų fizinių asmenų teisėms ir laisvėms; |
| * + 1. daromas poveikis dideliam duomenų subjektų skaičiui; |
| * + 1. bet kokia kita situacija, kuri gali sukelti reikšmingą poveikį Savivaldybei ir / arba duomenų subjektams. |
| * 1. Jei nusprendžiama nepradėti Procedūros, tada Procedūros 12 punkte aprašytas vertinimas turi būti tinkamai dokumentuotas už asmens duomenų saugą atsakingo asmens ir ši Procedūra užbaigta. |
| 1. **PROCEDŪRA – ASMENS DUOMENŲ SAUGUMO PAŽEIDIMO APRIBOJIMAS, LIKVIDAVIMAS IR ATKŪRIMAS** |
| * 1. Pirmasis žingsnis sprendžiant asmens duomenų saugumo pažeidimo klausimą yra jo apribojimas. Konkretūs veiksmai, atliktini norint tai pasiekti priklauso nuo konkretaus pažeidimo aplinkybių, bet tai galėtų būti tokie veiksmai kaip: |
| * + 1. Asmens duomenų ištrynimas nuotoliniu būdu iš pamesto ar pavogto įrenginio; |
| * + 1. kuo skubesnis kreipimasis į asmenį, kuriam per klaidą buvo išsiųsti asmens duomenys, su prašymu neatidarinėti nusiųstų duomenų ir juos ištrinti be galimybės atkurti; |
| * + 1. atskleisto tretiesiems asmenims prisijungimo prie duomenų bazės slaptažodžio pakeitimas; |
| * + 1. prarastų asmens duomenų atkūrimas iš turimos atsarginės kopijos. |
| * 1. Vykdant šią procedūrą reikia imtis atsargumo priemonių tam, kad būtų užtikrinta, jog būtų surinkti kiek įmanoma tikslesni duomenys bei įrodymai apie įvykusį asmens duomenų saugumo pažeidimą (pavyzdžiui, užfiksuojama, kas, kada ir iš kokio įrenginio jungėsi prie duomenų bazės, kam konkrečiai buvo per klaidą išsiųsti asmens duomenys, kokiomis aplinkybėmis buvo prarastas įrenginys su asmens duomenimis). |
| * 1. Veiksmai, skirti atitaisyti žalą, sukeltą asmens duomenų saugumo pažeidimo, turėtų būti nukreipti ne vien į esamo pažeidimo priežasties pašalinimą, bet ir skirti neleisti asmens duomenų saugumo pažeidimui pasikartoti. Turėtų būti nustatytas bet koks pažeidžiamumas, kuris gali būti išnaudotas siekiant įvykdyti pažeidimą. |
| * 1. Prireikus gali būti pasitelkiama IT specialistų ar teisininkų pagalba. |
| * 1. Atkūrimo stadijoje sistemos turėtų būti pagal galimybes atstatytos į ankstesnę būklę, tačiau turėtų būti imamasi būtinų veiksmų tam, kad būtų atsižvelgta į trūkumus ir asmens duomenų tvarkymo silpnąsias vietas, kurios buvo išnaudotos įvykdant asmens duomenų saugumo pažeidimą. |
| 1. **PROCEDŪRA – DUOMENŲ VALDYTOJO PRANEŠIMAS PRIEŽIŪROS INSTITUCIJAI APIE DUOMENŲ SAUGUMO PAŽEIDIMĄ** |
| * 1. Administracija, kaip duomenų valdytojas, nedelsdama privalo informuoti Priežiūros instituciją apie asmens duomenų saugumo pažeidimą tada, jei už asmens duomenų saugą atsakingas asmuo nustato, kad asmens duomenų saugumo pažeidimas tikėtinai gali kelti pavojų duomenų subjektų, paveiktų asmens duomenų saugumo pažeidimo, teisėms ir laisvėms. Pavojų keliančiu laikytinas toks pažeidimas, dėl kurio duomenų subjektas galėtų patirti kūno sužalojimą, materialinę ar nematerialinę žalą, teisių apribojimą, diskriminaciją, galėtų būti pavogta ar suklastota asmens tapatybė, jam padaryta finansinių nuostolių, neleistinai panaikinti pseudonimai, pakenkta jo reputacijai, prarastas asmens duomenų, kurie saugomi profesine paslaptimi, konfidencialumas arba padaryta kita ekonominė ar socialinė žala. |
| * 1. Jei asmens duomenų saugumo pažeidimas kelia pavojų duomenų subjektų teisėms ir laisvėms, asmuo atsakingas už asmens duomenų saugumo pažeidimo procedūros vykdymą ne vėliau kaip per 72 valandas nuo Administracijos, kaip duomenų valdytojo, sužinojimo apie pažeidimą Priežiūros institucijai pateikia tokią informaciją: |
| * + 1. asmens duomenų saugumo pažeidimo pobūdį, įskaitant, jeigu įmanoma, atitinkamai paveiktų duomenų subjektų kategorijas ir apytikslį skaičių, taip pat atitinkamų asmens duomenų įrašų kategorijas ir apytikslį skaičių; |
| * + 1. kontaktinio asmens, galinčio suteikti daugiau informacijos, vardą, pavardę ir kontaktinius duomenis; |
| * + 1. tikėtinų asmens duomenų saugumo pažeidimo pasekmių aprašymą; |
| * + 1. priemones, kurių ėmėsi arba planuoja imtis Administracija, kaip duomenų valdytojas, tam, kad būtų pašalintas asmens duomenų saugumo pažeidimas, įskaitant, kai tinkama, priemones galimoms neigiamoms jo pasekmėms sumažinti. |
| * 1. Jeigu visos informacijos neįmanoma pateikti tuo pačiu metu, tolesnė informacija nepagrįstai nedelsiant gali būti teikiama etapais. |
| 1. **PROCEDŪRA – DUOMENŲ VALDYTOJO PRANEŠIMAS DUOMENŲ SUBJEKTUI APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ** |
| * 1. Kai dėl asmens duomenų saugumo pažeidimo gali kilti didelis pavojus duomenų fizinių asmenų teisėms ir laisvėms, Administracija, kaip duomenų valdytojas, nepagrįstai nedelsdama praneša apie asmens duomenų saugumo pažeidimą duomenų subjektams. Didelį pavojų keliančiu gali būti laikytinas bet kuris 23 punkte nurodytų pasekmių riziką keliantis pažeidimas tada, jei tokios pažeidimo pasekmės yra labai tikėtinos, tvarkomi jautrūs asmens duomenys (pavyzdžiui, duomenys apie sveikatą), pažeidimas turi neigiamą poveikį dideliam duomenų subjektų skaičiui ir pan. |
| * 1. Už asmens duomenų saugą atsakingas asmuo duomenų subjektui aiškia ir paprasta kalba aprašo asmens duomenų saugumo pažeidimo pobūdį ir pateikia bent jau žemiau nurodytą informaciją: |
| * + 1. Kontaktinio asmens, galinčio suteikti daugiau informacijos, vardą, pavardę ir kontaktinius duomenis; |
| * + 1. Tikėtinų asmens duomenų saugumo pažeidimo pasekmių aprašymą; |
| * + 1. Priemones, kurių ėmėsi arba planuoja imtis Administracija tam, kad būtų pašalintas asmens duomenų saugumo pažeidimas, įskaitant, kai tinkama, priemones galimoms neigiamoms jo pasekmėms sumažinti. |
| * 1. Šios Procedūros 27 punkte nurodytas komunikavimas su duomenų subjektu nebus reikalingas tada, jei egzistuoja bet kuri iš šių aplinkybių: |
| * + 1. Administracija įgyvendino tinkamas technines ir organizacines apsaugos priemones ir tos priemonės taikytos asmens duomenims, kuriems asmens duomenų saugumo pažeidimas turėjo poveikio, visų pirma tas priemones, kuriomis užtikrinama, kad asmeniui, neturinčiam leidimo susipažinti su asmens duomenimis, jie būtų nesuprantami, pavyzdžiui, šifravimo priemones; |
| * + 1. Administracija vėliau ėmėsi priemonių, kuriomis užtikrinama, kad ateityje negalėtų kilti didelis pavojus duomenų subjektų teisėms ir laisvėms; |
| * + 1. tai pareikalautų neproporcingai daug pastangų. Tokiu atveju apie įvykusį asmens duomenų saugumo pažeidimą paskelbiama viešai arba taikoma panaši priemonė, kuria duomenų subjektai būtų informuojami taip pat efektyviai; |
| * 1. Priežiūros institucija, apsvarsčiusi, kokia yra tikimybė, kad dėl asmens duomenų saugumo pažeidimo kils didelis pavojus, gali pareikalauti, kad Savivaldybė informuotų duomenų subjektus apie asmens duomenų saugumo pažeidimą. Už asmens duomenų saugą atsakingas asmuo gavęs tokį nurodymą turi nedelsdamas jį vykdyti. |
| 1. **ASMENS DUOMENŲ SAUGUMO PAŽEIDIMO DOKUMENTAVIMAS IR PROCEDŪROS UŽBAIGIMAS** |
| * 1. Už asmens duomenų saugą atsakingas asmuo, gavęs supažindinto su asmens duomenų saugumo pažeidimo ir jo pašalinimo aplinkybėmis Administracijos direktoriaus pritarimą, priima sprendimą užbaigti Procedūrą tada, kai asmens duomenų saugumo pažeidimas laikytinas pašalintu, o visoms reikalingoms šalims apie pažeidimą yra pranešta. |
| * 1. Visi veiksmai, kurių imamasi Procedūros metu turi būti aprašomi ir visi susiję įrašai apie asmens duomenų saugumo pažeidimą peržiūrimi tam, kad būtų užtikrintas jų išbaigtumas, tikslumas ir atitiktis atitinkamam teisiniam reguliavimui.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |