Kauno rajono savivaldybės
administracijos
asmens duomenų apsaugos
politikos
2 priedas

REAGAVIMO Į ASMENS DUOMENŲ SAUGUMO PAŽEIDIMUS PROCEDŪRA

I. SĄVOKOS

1. **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.

2. **Administracija** – Kauno rajono savivaldybės administracija, juridinio asmens kodas: 188756386, buveinės adresas: Savanorių pr. 371, Kaunas.

3. **Už duomenų saugą atsakingas asmuo** – Administracijos direktoriaus paskirtas Darbuotojas, turintis kompetenciją imtis reagavimo į Duomenų saugumo pažeidimą procedūros vykdymo.

4. **Priežiūros institucija** reiškia valstybės narės pagal BDAR 51 straipsnį įsteigtą nepriklausomą valdžios instituciją. Lietuvos Respublikos atveju tokia institucija yra Valstybinė duomenų apsaugos inspekcija.

5. **Procedūra** reiškia šią Reagavimo į asmens duomenų saugumo pažeidimus procedūrą.

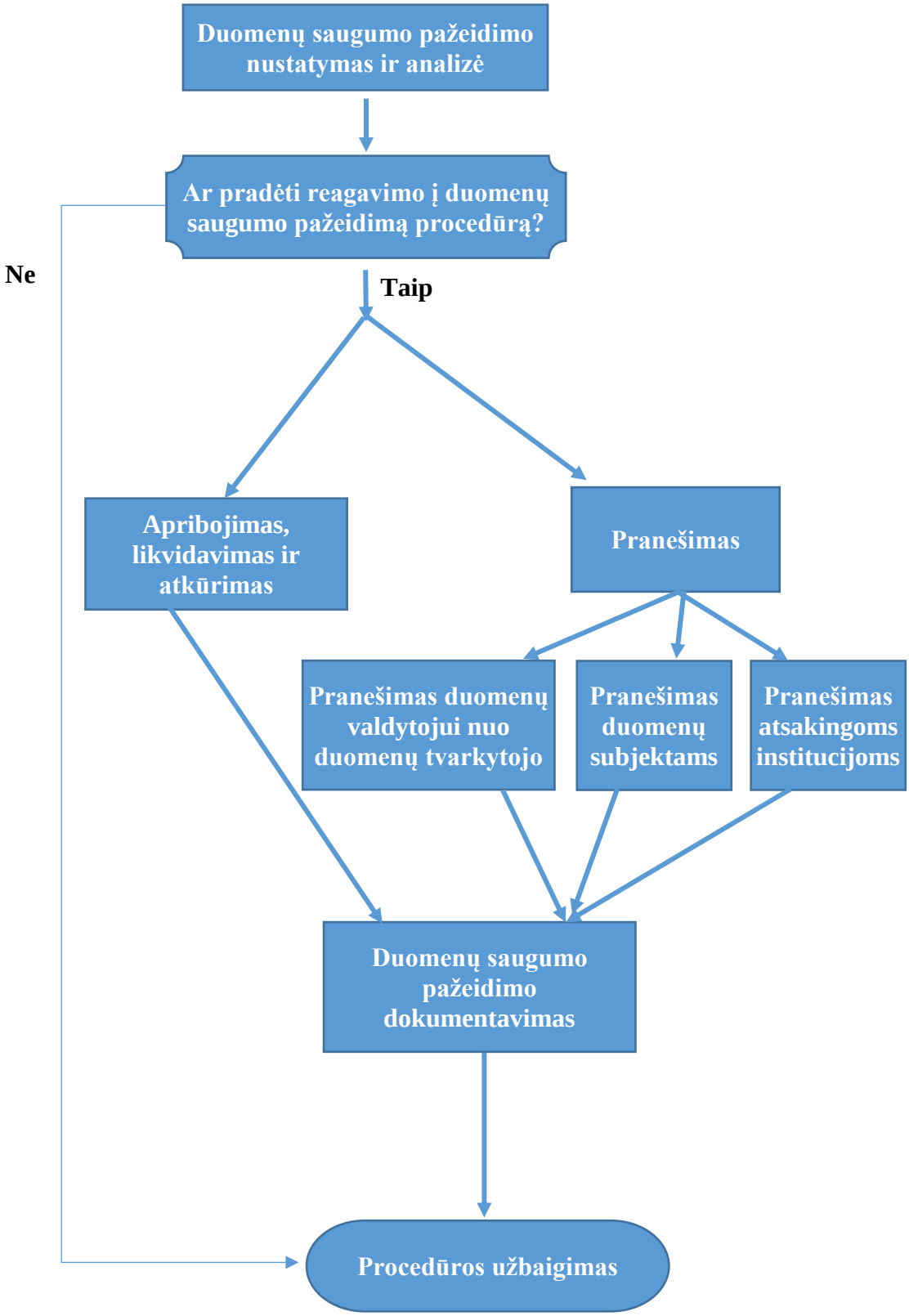
II. APIMTIS

6. Ši procedūra taikoma įvykus asmens duomenų saugumo pažeidimui pagal BDAR 33 straipsnį ir 34 straipsnį.

7. Šiame dokumente išdėstyta procedūra turėtų būti vadovaujamasi reaguojant į duomenų saugumo pažeidimą, atsižvelgiant į konkrečios situacijos faktines aplinkybes.

III. ATSAKOMYBĖ

8. Visi asmenys, turintys prieigą prie Administracijos tvarkomų asmens duomenų privalo žinoti ir vadovautis šia Procedūra duomenų saugumo pažeidimo atveju.



1 pav. Reagavimo į duomenų saugumo pažeidimus schema

IV.PROCEDŪRA – DUOMENŲ SAUGUMO PAŽEIDIMO NUSTATYMAS IR ANALIZĖ

9. Kaip ir galima spręsti iš Procedūros 1 punkte nurodyto apibrėžimo, saugumo pažeidimu laikomas toks saugumo incidentas, dėl kurio įvyksta (konkretus pažeidimas gali patekti į daugiau nei vieną kategoriją):

9.1. Konfidencialumo pažeidimas – netyčia ar neteisėtai atskleidžiami asmens duomenys arba prie duomenų suteikiama prieiga tam teisės neturintiems asmenims. Tokio pobūdžio pažeidimo pavyzdžiais galėtų būti duomenų kopijos išsiuntimas trečiajam asmeniui, neturinčiam teisinio pagrindo juos gauti, prisijungimo prie duomenų bazės slaptažodžio paviešinimas ir pan.;

9.2. 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 Administracijos veiklą sutrikdęs prieigos prie duomenų praradimas;

9.3. 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.

10. Kai yra nustatomas duomenų saugumo pažeidimas, jį nustatęs Darbuotojas turi kuo skubiau informuoti už duomenų saugą atsakingą asmenį asmeniškai, el. paštu, telefonu, ir / arba kitomis komunikacijos priemonėmis.

11. Už duomenų saugą atsakingas asmuo atlieka pradinį vertinimą tam, kad nuspręstų dėl tinkamo veiksmų plano. Šis vertinimas turėtų apimti šiuos pagrindinius veiksnius:

11.1. Poveikio informacinių technologijų (toliau – IT) infrastruktūrai apimtis;

11.2. Informaciniai ištekliai, kuriems gali kilti arba yra kilęs pavojus (kokios duomenų bazės yra arba gali būti paveiktos);

11.3. Tikėtina duomenų saugumo pažeidimo trukmė (kada prasidėjo ir kada buvo sustabdytas pažeidimas arba kaip skubiai tikėtina galima būtų tai padaryti);

11.4. Paveikti duomenų subjektai ir poveikio jiems apimtis (ar paveikti tik konkrečios duomenų subjektų grupės duomenys, kokia konkrečios grupės dalis yra paveikta ir pan.);

11.5. Pradiniai duomenų saugumo pažeidimo pasekmių požymiai (tai galėtų būti prieigos prie duomenų praradimas, nustatyti neteisėti duomenų pakeitimai, rasti paviešinti duomenys ir pan.).

12. 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.

13. Atsižvelgdamas į aukščiau aprašytą pradinę analizę, Už duomenų saugą atsakingas asmuo pagal Procedūros 11 punkte nurodytus kriterijus įvertina, ar duomenų saugumo pažeidimo apimtis ir faktinis ar galimas poveikis lemia Reagavimo į duomenų saugumo pažeidimus procedūros pradėjimą.

V. PROCEDŪRA – REAGAVIMO Į DUOMENŲ SAUGUMO PAŽEIDIMUS PROCEDŪROS PRADĖJIMAS

14. Formalus reagavimas į Duomenų saugumo pažeidimą visais atvejais turėtų būti pradėtas tada, jei nustatytos bet kurios iš toliau nurodytų aplinkybių:

14.1. Prarastas arba gali būti prarastas reikšmingas kiekis asmens duomenų;

14.2. Duomenų pažeidimas tikėtinai gali kelti didelį pavojų fizinių asmenų teisėms ir laisvėms;

14.3. Daromas poveikis dideliam duomenų subjektų skaičiui;

14.4. Bet kokia kita situacija, kuri gali sukelti reikšmingą poveikį Administracijai ir / arba duomenų subjektams.

15. Jei nusprendžiama nepradėti Procedūros, tada Procedūros 11 punkte aprašytas vertinimas turi būti tinkamai dokumentuotas už duomenų saugą atsakingo asmens ir ši Procedūra užbaigta.

VI. PROCEDŪRA – DUOMENŲ SAUGUMO PAŽEIDIMO APRIBOJIMAS, LIKVIDAVIMAS IR ATKŪRIMAS

16. Pirmasis žingsnis sprendžiant 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:

16.1. Duomenų ištrynimas nuotoliniu būdu iš pamesto ar pavogto įrenginio;

16.2. Kuo skubesnis kreipimasis į asmenį, kuriam per klaidą buvo išsiųsti duomenys, su prašymu neatidarinėti atsiųstų duomenų ir juos ištrinti be galimybės atkurti;

16.3. Atskleisto tretiesiems asmenims prisijungimo prie duomenų bazės slaptažodžio pakeitimas;

16.4. Prarastų duomenų atkūrimas iš turimos atsarginės kopijos.

17. Vykdant šią procedūrą reikia imtis atsargumo priemonių tam, kad būtų užtikrinta, jog būtų surinkti kiek įmanoma tikslesni duomenys bei įrodymai apie įvykusį 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 duomenimis).

18. Veiksmai, skirti atitaisyti žalą, sukeltą duomenų saugumo pažeidimo, turėtų būti nukreipti ne vien į esamo pažeidimo priežasties pašalinimą, bet ir skirti neleisti duomenų saugumo pažeidimui pasikartoti. Turėtų būti nustatytas bet koks pažeidžiamumas, kuris gali būti išnaudotas siekiant įvykdyti pažeidimą.

19. Prireikus gali būti pasitelkiama IT specialistų ar teisininkų pagalba.

20. Atkūrimo stadijoje sistemos turėtų būti pagal galimybes atstatytos į ankstesnę būklę, tačiau turėtų būti imamasi būtinų veiksmų tam, kad būtų atsižvelgta į trūkumus ir duomenų tvarkymo silpnąsias vietas, kurios buvo išnaudotos įvykdant duomenų saugumo pažeidimą.

VII. PROCEDŪRA – DUOMENŲ VALDYTOJO PRANEŠIMAS PRIEŽIŪROS INSTITUCIJAI APIE DUOMENŲ SAUGUMO PAŽEIDIMĄ

21. Administracija, kaip duomenų valdytojas, nedelsdama privalo informuoti Priežiūros instituciją apie duomenų saugumo pažeidimą tada, jei Už duomenų saugą atsakingas asmuo nustato, kad duomenų saugumo pažeidimas tikėtinai gali kelti pavojų duomenų subjektų, paveiktų 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.

22. Jei duomenų saugumo pažeidimas kelia pavojų duomenų subjektų teisėms ir laisvėms, Už duomenų saugą atsakingas asmuo ne vėliau kaip per 72 valandas nuo Administracijos sužinojimo apie pažeidimą Priežiūros institucijai pateikia tokią informaciją:

22.1. 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;

22.2. Kontaktinio asmens, galinčio suteikti daugiau informacijos, vardą, pavardę ir kontaktinius duomenis;

22.3. Tikėtinų duomenų saugumo pažeidimo pasekmių aprašymą;

22.4. Priemones, kurių ėmėsi arba planuoja imtis Administracija tam, kad būtų pašalintas duomenų saugumo pažeidimas, įskaitant, kai tinkama, priemones galimoms neigiamoms jo pasekmėms sumažinti.

23. Jeigu visos informacijos neįmanoma pateikti tuo pačiu metu, tolesnė informacija nepagrįstai nedelsiant gali būti teikiama etapais.

VIII. PROCEDŪRA – DUOMENŲ VALDYTOJO PRANEŠIMAS DUOMENŲ SUBJEKTUI APIE DUOMENŲ SAUGUMO PAŽEIDIMĄ

24. Kai dėl duomenų saugumo pažeidimo gali kilti didelis pavojus duomenų fizinių asmenų teisėms ir laisvėms, Administracija nepagrįstai nedelsdama praneša apie asmens duomenų saugumo pažeidimą duomenų subjektams. Didelį pavojų keliančiu gali būti laikytinas bet kuris 21 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.

25. Už duomenų saugą atsakingas asmuo duomenų subjektui aiškia ir paprasta kalba aprašo duomenų saugumo pažeidimo pobūdį ir pateikia bent jau žemiau nurodytą informaciją:

25.1. Kontaktinio asmens, galinčio suteikti daugiau informacijos, vardą, pavardę ir kontaktinius duomenis;

25.2. Tikėtinų duomenų saugumo pažeidimo pasekmių aprašymą;

25.3. Priemones, kurių ėmėsi arba planuoja imtis Administracija tam, kad būtų pašalintas duomenų saugumo pažeidimas, įskaitant, kai tinkama, priemones galimoms neigiamoms jo pasekmėms sumažinti.

26. Šios Procedūros 25 punkte nurodytas komunikavimas su duomenų subjektu nebus reikalingas tada, jei egzistuoja bet kuri iš šių aplinkybių:

26.1. Administracija įgyvendino tinkamas technines ir organizacines apsaugos priemones ir tos priemonės taikytos asmens duomenims, kuriems 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;

26.2. Administracija vėliau ėmėsi priemonių, kuriomis užtikrinama, kad ateityje negalėtų kilti didelis pavojus duomenų subjektų teisėms ir laisvėms;

26.3. Tai pareikalautų neproporcingai daug pastangų. Tokiu atveju apie įvykusį duomenų saugumo pažeidimą paskelbiama viešai arba taikoma panaši priemonė, kuria duomenų subjektai būtų informuojami taip pat efektyviai;

27. Priežiūros institucija, apsvarsčiusi, kokia yra tikimybė, kad dėl duomenų saugumo pažeidimo kils didelis pavojus, gali pareikalauti, kad Administracija informuotų duomenų subjektus apie duomenų saugumo pažeidimą. Už duomenų saugą atsakingas asmuo gavęs tokį nurodymą turi nedelsdamas jį vykdyti.

IX. DUOMENŲ SAUGUMO PAŽEIDIMO DOKUMENTAVIMAS IR PROCEDŪROS UŽBAIGIMAS

28. Už duomenų saugą atsakingas asmuo, gavęs supažindinto su duomenų saugumo pažeidimo ir jo pašalinimo aplinkybėmis Administracijos direktoriaus pritarimą, priima sprendimą užbaigti Procedūrą tada, kai duomenų saugumo pažeidimas laikytinas pašalintu, o visoms reikalingoms šalims apie pažeidimą yra pranešta.

29. Visi veiksmai, kurių imamasi Procedūros metu turi būti aprašomi ir visi susiję įrašai apie duomenų saugumo pažeidimą peržiūrimi tam, kad būtų užtikrintas jų išbaigtumas, tikslumas ir atitiktis atitinkamam teisiniam reguliavimui.