PATVIRTINTA
UAB Panevėžio regiono atliekų
tvarkymo centro direktoriaus
2022 m. liepos 14 d. įsakymu Nr. ĮVK-73

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ VALDYMO UAB PANEVĖŽIO REGIONO ATLIEKŲ TVARKYMO CENTRE TVARKOS APRAŠAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Asmens duomenų saugumo pažeidimų valdymo UAB Panevėžio regiono atliekų tvarkymo centre (toliau – PRATC) tvarkos aprašas (toliau – Tvarkos aprašas) reglamentuoja, kokia tvarka PRATC nustato, tiria, fiksuoja asmens duomenų pažeidimus, praneša apie juos Valstybinei duomenų apsaugos inspekcijai (toliau – VDAI), duomenų subjektams.

2. Galimi šie asmens duomenų saugumo pažeidimai:

2.1. konfidencialumo pažeidimas – neleistinas arba netyčinis asmens duomenų atskleidimas arba prieigos prie jų suteikimas;

2.2. vientisumo pažeidimas – neleistinas arba netyčinis asmens duomenų pakeitimas;

2.3. prieinamumo pažeidimas – neleistinas arba netyčinis prieigos prie asmens duomenų praradimas arba asmens duomenų sunaikinimas.

3. Atsižvelgiant į aplinkybes, asmens duomenų saugumo pažeidimas vienu metu gali būti susijęs su asmens duomenų konfidencialumu, vientisumu ir prieinamumu, taip pat su bet kokiu jų deriniu.

4. Asmens duomenų saugumo pažeidimas gali įvykti dėl šių priežasčių:

4.1. žmogiškoji klaida (pvz., asmens duomenys persiųsti ne tam adresatui, kuriam jie buvo skirti; ne saugojimui skirtoje vietoje palikti dokumentai, kuriuose yra asmens duomenų; pamesti nešiojami/mobilieji įrenginiai (telefonas, nešiojamasis kompiuteris, išorinės duomenų laikmenos), kuriuose saugomi asmens duomenys ir kt.);

4.2. vagystė (pvz., pavogti nešiojami/mobilieji įrenginiai, kuriuose saugomi asmens duomenys; pavogtos bylos, kuriose yra asmens duomenų ir kt.);

4.3. kibernetinė ataka (pvz., duomenų bazėje ar informacinėje sistemoje esantys asmens duomenys užšifruojami, naudojant išpirkos reikalaujančią programą; internete paskelbiami informacinių sistemų naudotojų vardai ir slaptažodžiai ir kt.);

4.4. neleistina (neautorizuota) prieiga prie asmens duomenų (pvz., įgaliojimų neturintys asmenys patenka į patalpas, kuriose saugomos bylos su asmens duomenimis; įgaliojimų neturintys asmenys prisijungia prie duomenų bazių ar informacinių sistemų ir kt.);

4.5. įrenginių ar programinės įrangos gedimas, saugos sistemos spragos (pvz., energijos tiekimo nutrūkimas, dėl kurio negalima prieiga prie asmens duomenų; programos kodo, kuriuo kontroliuojamas prieigos teisių suteikimas informacinių sistemų naudotojams, klaida ir kt.);

4.6. nenugalimos jėgos (*force majeure*) aplinkybės ir kitos priežastys (gaisras, vandens užliejimas, dėl kurių sugadinami arba prarandami asmens duomenys ir kt.).

5. Asmens duomenų saugumo 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., asmuo gali patirti teisių apribojimą, diskriminaciją, gali būti

pavogta ar suklastota jo asmens tapatybė, jam padaryta finansinių nuostolių, pakenkta jo reputacijai, prarastas duomenų, kurie laikomi profesine paslaptimi, konfidencialumas ir kt.).

6. Tvarkos aprašo nuostatų privalo laikytis visi PRATC darbuotojai, kurie tvarko asmens duomenis arba eidami savo pareigas juos sužino bei juridiniai asmenys, tvarkantys PRATC duomenis sutartiniais pagrindais, kuriems pagal Reglamento 33 straipsnio 2 dalį yra nustatyta prievolė pranešti Tarnybai apie kiekvieną asmens duomenų saugumo pažeidimą.

II SKYRIUS
PRANEŠIMAS APIE GALIMĄ ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ

7. PRATC darbuotojas, nustatęs galimą asmens duomenų saugumo pažeidimą, arba gavęs informaciją apie galimą asmens duomenų saugumo pažeidimą iš duomenų tvarkytojo, žiniasklaidos ar kito šaltinio:

7.1. nedelsdamas, bet ne vėliau kaip per 2 darbo valandas nuo asmens duomenų saugumo pažeidimo sužinojimo momento, žodžiu (tiesiogiai ar telefonu) arba elektroniniu paštu informuoja tiesioginį vadovą ir PRATC duomenų apsaugos pareigūną;

7.2. užpildo Pranešimą apie asmens duomenų saugumo pažeidimą (Tvarkos aprašo 1 priedas) (toliau – pranešimas) ir nedelsdamas, bet ne vėliau kaip per 2 darbo valandas nuo saugumo pažeidimo sužinojimo momento, perduoda pasirašytą pranešimą PRATC direktoriui, kuris rezoliucija nukreipia tolimesniam vykdymui PRATC duomenų apsaugos pareigūnui;

7.3. jei įmanoma, nedelsdamas imasi priemonių pašalinti saugumo pažeidimą ir (ar) priemonių sumažinti jo sukeltas neigiamas pasekmes.

8. Bet kuris PRATC duomenų tvarkytojo darbuotojas, pastebėjęs ar kitaip sužinojęs apie galimą duomenų tvarkytojo tvarkomų asmens duomenų saugumo pažeidimą, privalo nedelsiant apie tai informuoti duomenų tvarkytojo įgaliotus asmenis, atsakingus už asmens duomenų saugumo pažeidimų tyrimą, valdymą ir šalinimą. Duomenų tvarkytojo įgalioti asmenys apie galimą asmens duomenų saugumo pažeidimą atitinkamai nedelsdami, bet ne vėliau kaip per 24 valandas nuo sužinojimo, apie tai raštu praneša PRATC, pateikdami informaciją, numatytą Reglamento (ES) 2016/679 33 straipsnio 3 dalyje. Duomenų tvarkytojai pateikia PRATC visą kitą jo prašomą informaciją, susijusią su pažeidimu ir jo tyrimu, per PRATC nurodytą terminą. Duomenų tvarkytojų pareigos, susijusios su pranešimu apie pažeidimą PRATC bei su bendradarbiavimu tiriant pažeidimą įtvirtinamos su duomenų tvarkytoju sudaromoje duomenų tvarkymo sutartyje.

III SKYRIUS
ASMENS DUOMENŲ SAUGUMO PAŽEIDIMO TYRIMAS IR PAŠALINIMAS

9. PRATC duomenų apsaugos pareigūnas, šio Tvarkos aprašo 8.1 ir 8.2 papunkčiuose nurodyta tvarka gavęs informaciją apie asmens duomenų saugumo pažeidimą, atlieka šias asmens duomenų saugumo pažeidimo tyrimo procedūras:

9.1. nedelsdamas nagrinėja pranešime nurodytas aplinkybes;

9.2. prireikus, konsultuojasi su VDAI;

9.3. jei asmens duomenų saugumo pažeidimas yra susijęs su elektroninės informacijos saugos incidentu, pasitelkia PRATC ar duomenų tvarkytojo specialistus ir informacinių sistemų saugos specialistus;

9.4. įvertina, ar padarytas asmens duomenų saugumo pažeidimas;

9.5. jei asmens duomenų saugumo pažeidimas padarytas, nustato pažeidimo pobūdį, priežastis, asmens duomenų kategorijas, jų pobūdį ir kiekį, duomenų subjektų kategorijas ir jų kiekį, įvertina padarytą žalą fiziniams asmenims bei tikėtinas pažeidimo pasekmes;

9.6. įvertina, kokių skubių ir tinkamų priemonių būtina imtis, kad būtų pašalintas saugumo pažeidimas (pvz., naudoti atsargines kopijas, siekiant atkirti prarastus ar sugadintus duomenis ar kt.);

9.7. nustato, ar apie saugumo pažeidimą būtina pranešti VDAI;

9.8. nustato, ar būtina nedelsiant pranešti duomenų subjektui apie asmens duomenų saugumo pažeidimą;

10. PRATC darbuotojai, atsakingi už asmens duomenų tvarkymą, pateikia duomenų apsaugos pareigūnui visą jo prašomą informaciją, susijusią su asmens duomenų saugumo pažeidimu ir tyrimu, per jo nurodytą terminą.

11. Atliekant asmens duomenų saugumo pažeidimo tyrimą ir siekiant nustatyti, ar pažeidimas iš tikrųjų įvyko, esamos situacijos įrodymai privalo būti fiksuojami dokumentuose ir užtikrinamas jų atsekamumas.

12. Jei asmens duomenų saugumo pažeidimas nustatomas, duomenų apsaugos pareigūnas papildomai įvertina pažeidimo keliamos rizikos duomenų subjektų teisėms ir laisvėms lygį.

13. Vertinant rizikos lygį, atsižvelgiama į konkrečias pažeidimo aplinkybes, pavojaus duomenų subjektų teisėms ir laisvėms atsiradimo tikimybę ir rimtumą. Rizikos lygis vertinamas atsižvelgiant į šiuos kriterijus:

13.1. saugumo pažeidimo pobūdis (konfidencialumo, vientisumo ar prieinamumo pažeidimas) – nustatomas saugumo pažeidimo pobūdis, nuo kurio gali priklausyti pavojaus duomenų subjektams dydis;

13.2. asmens duomenų pobūdis, jautrumas ir kiekis – nustatomas asmens duomenų, kurių saugumas buvo pažeistas, pobūdis, jautrumas ir jų kiekis: kuo jautresni asmens duomenys ir kuo didesnis jų kiekis, tuo didesnis žalos pavojus;

13.3. galimybė identifikuoti fizinį asmenį – įvertinama, ar neįgaliotiems asmenims, kuriems tapo prieinami asmens duomenys, bus lengva nustatyti konkrečių asmenų tapatybę arba susieti tuos duomenis su kita informacija (pvz., tinkamai užšifruoti asmens duomenys nebus suprantami neįgaliotiems asmenims, todėl pažeidimas padarys mažesnį poveikį duomenų subjektams);

13.4. fizinio asmens specifiniai ypatumai – nustatomi fizinių asmenų, kurių asmens duomenims kilo pavojus, specifiniai ypatumai: kuo asmenys yra labiau pažeidžiami (pvz., vaikai, negalią turintys asmenys), tuo didesnį poveikį pažeidimas gali jiems padaryti;

13.5. nukentėjusių duomenų subjektų skaičius – nustatomas nukentėjusių asmenų skaičius: kuo daugiau yra asmenų, kuriems pažeidimas turi poveikio, tuo didesnis žalos pavojus;

13.6. pasekmės, sukeltos fiziniams asmenims – įvertinamos visos galimos pažeidimo pasekmės bei jų rimtumas; taip pat atsižvelgiama į pasekmių ilgalaikiškumą: jei pažeidimo pasekmės yra ilgalaikės, tai poveikis fiziniams asmenims bus didesnis.

14. Įvertinus riziką, nustatomas vienas iš trijų rizikos tikimybių lygių – mažas, vidutinis ar didelis.

15. Duomenų apsaugos pareigūnas, atlikęs asmens duomenų saugumo pažeidimo tyrimą, užpildo Asmens duomenų saugumo pažeidimo tyrimo ataskaitą (Tvarkos aprašo 2 priedas).

16. Asmens duomenų saugumo pažeidimo tyrimo ataskaita pateikiama PRATC direktoriui ir (ar) duomenų tvarkytojo vadovui, jei tai susiję su duomenų tvarkytojo atliekamais asmens duomenų tvarkymo veiksmais.

17. Atsižvelgiant į Asmens duomenų saugumo pažeidimo tyrimo ataskaitą, PRATC direktorius, jei reikia, tvirtina priemonių planą, kuriame numatomos būtinos priemonės dėl asmens duomenų saugumo pažeidimo pašalinimo, taip pat paskiria atsakingus vykdytojus ir nustato priemonių įgyvendinimo terminus. Šį priemonių planą rengia PRATC duomenų apsaugos pareigūnas.

18. Sprendžiant asmens duomenų saugumo pažeidimo pašalinimo klausimą bei tvirtinant priemonių planą, priklausomai nuo konkrečių pažeidimo aplinkybių, pirmiausia būtina atlikti veiksmus, siekiant apriboti ar sustabdyti saugumo incidentą: ištrinti asmens duomenis nuotoliniu būdu iš pamesto ar pavogto nešiojamo/mobiliojo įrenginio (telefono, nešiojamojo kompiuterio ir kt.); jei asmens duomenys per klaidą išsiunčiami ne tam adresatui, kuo skubiau kreiptis į jį su prašymu ištrinti atsiųstus asmens duomenis be galimybės juos atkurti; pakeisti prisijungimo prie duomenų bazės ar informacinės sistemos vardus ir slaptažodžius, jeigu jie tapo žinomi tretiesiems asmenims; atkuriant prarastus ar sugadintus asmens duomenis, naudoti atsargines kopijas ir kt.

19. Siekiant apriboti ar sustabdyti asmens duomenų saugumo pažeidimą, būtina kiek įmanoma tiksliau surinkti duomenis ir įrodymus apie įvykusį saugumo incidentą (pvz., kas, kada ir iš kokio įrenginio jungėsi prie duomenų bazės ar informacinės sistemos, kam per klaidą išsiųsti asmens duomenys, kokiomis aplinkybėmis buvo prarastas įrenginys su asmens duomenimis ir kt.).

20. Priemonių plane turi būti numatytos prevencinės ir kitos priemonės, užtikrinančios, kad asmens duomenų saugumo pažeidimas nepasikartotų.

21. PRATC duomenų apsaugos pareigūnas, atlikęs galimai įvykusio asmens duomenų saugumo pažeidimo tyrimą ir nustatęs, kad asmens duomenų saugumo pažeidimas nebuvo padarytas, surašo Asmens duomenų saugumo incidento ataskaitą (Tvarkos aprašo 3 priedas) ir pateikia ją administratoriui užregistruoti.

IV SKYRIUS
PRANEŠIMAS APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ PRIEŽIŪROS INSTITUCIJAI

22. Tyrimo metu nustačius, kad asmens duomenų saugumo pažeidimas buvo, PRATC duomenų apsaugos pareigūnas nedelsdamas ir, jei įmanoma, praėjus ne daugiau kaip 72 valandoms nuo tada, kai jam tapo žinoma apie pažeidimą, apie tai raštu informuoja VDAI, išskyrus atvejus, kai saugumo pažeidimas nekelia pavojaus fizinių asmenų teisėms ir laisvėms.

23. VDAI informuojama Pranešimo apie asmens duomenų saugumo pažeidimą pateikimo Valstybinei duomenų apsaugos inspekcijai tvarkos aprašo, patvirtinto VDAI direktoriaus 2018 m. liepos 27 d. įsakymu Nr. 1T-72(1.12. E) „Dėl Pranešimo apie asmens duomenų saugumo pažeidimą pateikimo Valstybinei duomenų apsaugos inspekcijai tvarkos aprašo patvirtinimo“, nustatyta tvarka ir sąlygomis, užpildant Pranešimo apie asmens duomenų saugumo pažeidimo formą, patvirtintą VDAI direktoriaus 2018 m. rugpjūčio 29 d. įsakymu Nr. 1T-82(1.12. E) „Dėl Pranešimo apie asmens duomenų saugumo pažeidimą rekomenduojamos formos patvirtinimo“ (toliau – Pranešimas).

24. Jeigu įvertinus riziką abejojama, ar asmens duomenų saugumo pažeidimas kelia pavojų fizinių asmenų teisėms ir laisvėms, apie pažeidimą pranešama VDAI.

25. Jeigu įvertinus riziką nustatoma, kad apie saugumo pažeidimą VDAI pranešti nereikia, tačiau po kurio laiko situacija pasikeičia, saugumo pažeidimas bei jo keliamas pavojus fizinių asmenų teisėms ir laisvėms turi būti vertinamas iš naujo ir, jeigu reikia, pranešama VDAI (pvz., pamesta USB atmintinė, kurioje saugomi užšifruoti asmens duomenys taikant pažangų algoritmą. Jeigu yra atsarginės duomenų kopijos ir nėra pavojaus šifro saugumui, apie tokį saugumo pažeidimą pranešti VDAI nereikia, tačiau jei vėliau paaiškėja, kad gali kilti pavojus šifro saugumui, pažeidimo keliamas pavojus turi būti vertinamas iš naujo ir apie tokį pažeidimą reikia pranešti VDAI).

26. Tuo atveju, kai pagal pažeidimo pobūdį būtina atlikti išsamesnį tyrimą, tačiau per 72 valandas dėl objektyvių priežasčių ištirti padarytą pažeidimą nėra įmanoma, informacija VDAI teikiama etapais, nurodant vėlavimo priežastis. Apie informacijos teikimą etapais VDAI informuojama teikiant pirminį Pranešimą.

27. Jeigu pateikus VDAI Pranešimą ir atlikus tolesnį tyrimą yra nustatoma, kad saugumo incidentas buvo sustabdytas ir faktiškai nebuvo asmens duomenų saugumo pažeidimo, apie tai nedelsiant informuojama VDAI.

28. Tuo atveju, kai yra įtariama, kad asmens duomenų saugumo pažeidimas turi nusikalstamos veikos požymių, informacija apie galimą nusikalstamą veiką pateikiama atitinkamoms valstybės institucijoms, įgaliotoms atlikti ikiteisminį tyrimą.

V SKYRIUS
RANEŠIMAS APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ DUOMENŲ SUBJEKTUI

29. Tyrimo metu nustačius, kad dėl asmens duomenų saugumo pažeidimo gali kilti didelis pavojus fizinių asmenų teisėms ir laisvėms, PRATC duomenų apsaugos pareigūnas nedelsdamas ir, jei įmanoma, praėjus ne daugiau kaip 72 valandoms nuo to laiko, kai buvo sužinota apie pažeidimą, praneša apie tai duomenų subjektui, kurio teisėms ir laisvėms gali kilti pavojus.

30. Duomenų subjektas informuojamas tiesiogiai, t. y. siunčiant jam pranešimą paštu arba elektroniniu paštu arba trumpąja žinute (SMS) ar kitu būdu.

31. Pagrindinis pranešimo duomenų subjektui tikslas – pateikti konkrečią informaciją apie tai, kokių veiksmų jis turėtų imtis, kad apsisaugotų nuo neigiamų pažeidimo pasekmių. Pranešime duomenų subjektui aiškia ir paprasta kalba pateikiama ši informacija:

31.1. asmens duomenų saugumo pažeidimo pobūdžio ir tikėtinų pažeidimo pasekmių aprašymas;

31.2. priemonių, kurių ėmėsi PRATC, kad būtų pašalintas saugumo pažeidimas, įskaitant priemonių galimoms neigiamoms jo pasekmėms sumažinti, aprašymas;

31.3. PRATC duomenų apsaugos pareigūno arba kito kontaktinio asmens, galinčio suteikti daugiau informacijos, vardas, pavardė ir kontaktiniai duomenys;

31.4. kita reikšminga informacija, susijusi su pažeidimu, turėtų būti pateikta duomenų subjektui, pvz., patarimai, kaip apsisaugoti nuo galimų neigiamų pažeidimo pasekmių.

32. Pranešimo apie asmens duomenų saugumo pažeidimą duomenų subjektams teikti nereikia, jeigu:

32.1. PRATC įgyvendino tinkamas technines ir organizacines apsaugos priemones ir tos priemonės taikytos asmens duomenims, kuriems pažeidimas turėjo poveikio, visų pirma tas priemones, kuriomis užtikrinama, kad asmeniui, neturinčiam leidimo susipažinti su duomenimis, jie būtų nesuprantami (pvz., asmens duomenų šifravimo priemonės);

32.2. iš karto po pažeidimo Tarnyba ėmėsi priemonių, kuriomis užtikrinama, kad nekiltų didelis pavojus duomenų subjektų teisėms ir laisvėms;

32.3. tiesioginio pranešimo duomenų subjektui pateikimas pareikalautų neproporcingai didelių pastangų, pvz., jei jų kontaktiniai duomenys buvo prarasti dėl pažeidimo arba iš pradžių nebuvo žinomi.

33. Jeigu įvertinus riziką nustatoma, kad apie saugumo pažeidimą duomenų subjektui pranešti nereikia, tačiau po kurio laiko situacija pasikeitė, pažeidimas bei jo keliamas pavojus fizinių asmenų teisėms ir laisvėms turėtų būti vertinamas iš naujo (pvz., įvykdoma kibernetinė ataka, naudojant išpirkos reikalaujančią programą, – duomenų bazėje esantys asmens duomenys užšifruojami. Jei atlikus tyrimą paaiškėja, kad vienintelė išpirkos reikalaujančios programos užduotis buvo užšifruoti asmens duomenis ir jokio kito kenksmingo poveikio duomenų bazei nėra, apie saugumo pažeidimą reikės pranešti tik VDAI, tačiau jei vėliau paaiškėja, kad prarastas ne tik duomenų prieinamumas, bet ir konfidencialumas, saugumo pažeidimo keliamas pavojus bus vertinamas iš naujo bei sprendžiama, ar atsižvelgiant į tikėtinas saugumo pažeidimo pasekmes reikia apie jį pranešti duomenų subjektams).

34. Tarnyba, atsižvelgdama į esamas pagrįstas aplinkybes ir teisėtus teisėsaugos institucijų reikalavimus, gali atidėti asmenų, kuriems pažeidimas turi poveikio, informavimą iki to laiko, kol tai netrukdys saugumo pažeidimo ar kitam tyrimui.

VI SKYRIUS
ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ DOKUMENTAVIMAS

35. Visi asmens duomenų saugumo pažeidimai, nepriklausomai nuo to, ar apie juos buvo pranešta VDAI, registruojami Asmens duomenų saugumo pažeidimų UAB PRATC žurnale (toliau – Asmens duomenų saugumo pažeidimų registravimo žurnalas) (Tvarkos aprašo 4 priedas).

36. Informacija apie pažeidimą registruojama nedelsiant, kai tik nustatomas pažeidimo faktas ir įvertinama rizika, bet ne vėliau kaip per 5 darbo dienas.

37. Asmens duomenų saugumo pažeidimų registravimo žurnale nurodoma:

37.1. pažeidimo nustatymo aplinkybės (pažeidimo nustatymo data, laikas, vieta, subjektas, pranešęs apie pažeidimą);

37.2. pažeidimo aplinkybės (pažeidimo data, vieta, pažeidimo pobūdis, priežastys, asmens duomenų, kurių saugumas pažeistas, kategorijos ir apytikslis skaičius, duomenų subjektų, kurių asmens duomenų saugumas pažeistas, kategorijos ir apytikslis skaičius);

37.3. tikėtinos pažeidimo pasekmės ir pavojus duomenų subjekto teisėms ir laisvėms;

37.4. priemonės, kurių buvo imtasi, kad būtų pašalintas pažeidimas, įskaitant priemones galimoms neigiamoms pažeidimo pasekmėms sumažinti;

37.5. informacija apie pranešimą ar nepranešimą VDAI:

37.5.1. jei apie asmens duomenų saugumo pažeidimą buvo nepranešta VDAI, nurodomi tokio sprendimo motyvai; jei apie asmens duomenų saugumo pažeidimą buvo pranešta VDAI, nurodoma pranešimo data ir numeris, taip pat, ar pranešimas teikiamas etapais;

37.5.2. jeigu apie asmens duomenų saugumo pažeidimą buvo vėluojama pranešti VDAI, nurodomos tokio vėlavimo priežastys;

37.6. informacija apie pranešimą ar nepranešimą duomenų subjektui (subjektams):

37.6.1. jei apie asmens duomenų saugumo pažeidimą buvo nepranešta duomenų subjektui (subjektams), nurodomi tokio sprendimo motyvai; jei apie asmens duomenų saugumo pažeidimą buvo pranešta duomenų subjektui (subjektams), nurodoma pranešimo (pranešimų) data (datos) ir būdas (būdai);

37.6.2. jeigu apie asmens duomenų saugumo pažeidimą buvo vėluojama pranešti duomenų subjektui (subjektams), nurodomos tokio vėlavimo priežastys;

37.7. kita reikšminga informacija, susijusi su asmens duomenų saugumo pažeidimu.

38. Už Asmens duomenų saugumo pažeidimų registravimo žurnalo pildymą, tvarkymą ir saugojimą atsakingas Teisės, viešųjų pirkimų ir projektinės veiklos padalinio vadovas.

VII SKYRIUS
BAIGIAMOSIOS NUOSTATOS

39. PRATC darbuotojai, pažeidę šio Tvarkos aprašo reikalavimus, atsako Lietuvos Respublikos teisės aktų nustatyta tvarka.

40. Aprašas peržiūrimas periodiškai, ne rečiau kaip kartą per metus, arba įvykus organizaciniams, sisteminiams ar kitiems pokyčiams arba pasikeitus teisės aktų reikalavimams. Už peržiūrą atsakingas juristas.

Asmens duomenų saugumo pažeidimų valdymo
UAB Panevėžio regiono atliekų tvarkymo centre
tvarkos aprašo
1 priedas

_____
(struktūrinio padalinio pavadinimas)

_____
(pareigų pavadinimas/fizinio asmens vardas, pavardė)

_____
(telefono ryšio ir (ar) elektroninio pašto adresas, ir (ar) elektroninės siuntos pristatymo dėžutės adresas)

UAB Panevėžio regiono
Atliekų tvarkymo centro direktoriui

PRANEŠIMAS
APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ

_____ Nr. _____
(data, dokumento numeris)

Informuoju apie asmens duomenų saugumo pažeidimą, pateikdamas turimą informaciją:
1. Asmens duomenų saugumo pažeidimo apibūdinimas:
1.1. Asmens duomenų saugumo pažeidimo data ir laikas:
Asmens duomenų saugumo pažeidimo:

Data _____ Laikas _____

Asmens duomenų saugumo pažeidimo nustatymo:

Data _____ Laikas _____

1.2. Asmens duomenų saugumo pažeidimo vieta (pažymėti tinkamą (-us):

- ☐ Informacinė sistema
- ☐ Duomenų bazė
- ☐ Tarnybinė stotis
- ☐ Interneto svetainė
- ☐ Debesų kompiuterijos paslaugos
- ☐ Nešiojamieji / mobilieji įrenginiai
- ☐ Neautomatiniu būdu susistemintos bylos (archyvas)
- ☐ Kita

(nurodyti)_____
_____

1.3. Asmens duomenų saugumo pažeidimo aplinkybės (pažymėti tinkamą / -us):

- ☐ Asmens duomenų konfidencialumo praradimas (neautorizuota prieiga ar atskleidimas)

 Asmens duomenų vientisumo praradimas (neautorizuotas asmens duomenų pakeitimas)

 Asmens duomenų prieinamumo praradimas (asmens duomenų praradimas, sunaikinimas)

2. Duomenų subjektų, kurių asmens duomenų saugumas pažeistas, kategorijos (pvz., PRATC darbuotojai, asmenys, pateikę prašymus, skundus ir kt.) ir apytikslis jų skaičius (jei žinoma):

_____
_____
_____

3. Asmens duomenų, kurių saugumas pažeistas, kategorijos (pažymėti tinkamą (-us):

3.1. Asmens duomenys:

Vardas	
Pavardė	
Asmens kodas	
Adresas	
Telefono numeris	
Elektroninio pašto adresas	
Banko sąskaitos numeris	
Banko kortelės numeris	
Prisijungimo duomenys (vartotojo vardas, slaptažodis)	
Asmens dokumento (-ų) duomenys	
Duomenys apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas	
Kiti duomenys	

3.2. Specialių kategorijų asmens duomenys:

Duomenys, susiję su asmens sveikata	
Genetiniai duomenys	
Duomenys, susiję su asmens politinėmis pažiūromis, religiniais, filosofiniais įsitikinimais	
Duomenys, susiję su asmens naryste profesinėse sąjungose	
Duomenys, susiję su asmens rasine ar etnine kilme	
Duomenys, susiję su asmens lytiniu gyvenimu ir lytine orientacija	
Duomenys apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas	

3.3. Kiti asmens duomenys (įrašyti):

_____
_____
_____

4. Apytikslis asmens duomenų, kurių saugumas pažeistas, skaičius:

_____
_____

5. Galimos asmens duomenų saugumo pažeidimo pasekmės:

5.1. Konfidencialumo praradimo atveju:

 Asmens duomenų išplitimas labiau nei būtina ir duomenų subjekto asmens duomenų kontrolės praradimas (pavyzdžiui, asmens duomenys išplito internete);

 Skirtingos informacijos susiejimas (pavyzdžiui, gyvenamosios vietos adreso susiejimas su asmens buvimo vieta realiu laiku);

 Galimas panaudojimas kitais, nei nustatytais ar neteisėtais tikslais (pavyzdžiui, komerciniais, asmens tapatybės pasisavinimo, informacijos panaudojimo prieš asmenį);

 Kita

_____
_____
_____
_____

5.2. Vientisumo praradimo atveju:

 Pakeitimas į neteisingus duomenis, dėl ko asmuo gali netekti galimybės naudotis paslaugomis;

 Pakeitimas į galiojančius duomenis, kad asmens duomenų tvarkymas būtų nukreiptas (pavyzdžiui, pavogta asmens tapatybė, susiejant vieno asmens identifikuojančius duomenis su kito asmens biometriniais duomenimis);

 Kita.

5.3. Duomenų prieinamumo praradimo atveju:

 Dėl asmens duomenų trūkumo negalima teikti paslaugų (pavyzdžiui, procesų sutrikdymas, dėl ko negalima patekti, pavyzdžiui, prie asmens sveikatos istorijų ir teikti pacientams sveikatos paslaugų, arba įgyvendinti duomenų subjekto teises);

 Dėl klaidų asmens duomenų tvarkymo procesuose negalima teikti tinkamos paslaugos (pavyzdžiui, asmens sveikatos istorijoje neliko informacijos apie asmens alergijas, išnyko tam tikra informacija iš mokesčių deklaracijos, todėl negalima tinkamai apskaičiuoti mokesčių ir pan.);

 Kita

5.4. Kita:

_____

6. Kokių veiksmų (priemonių) buvo imtasi sužinojus apie padarytą asmens duomenų saugumo pažeidimą (pvz., pakeisti kompiuterio slaptažodžiai, nutraukta neteisėta prieiga prie tvarkomų asmens duomenų, panaudotos atsarginės kopijos, siekiant atkurti prarastus ar sugadintus duomenis, atnaujinta programinė įranga, surinkti ne saugojimui skirtoje vietoje palikti dokumentai su asmens duomenimis ir pan.):

_____
_____
_____

_____ _____

(pareigos) (vardas ir pavardė)

_____

Asmens duomenų saugumo pažeidimų valdymo
UAB Panevėžio regiono atliekų tvarkymo centre
tvarkos aprašo
2 priedas

UAB PANEVĖŽIO REGIONO ATLIEKŲ TVARKYMO CENTRAS
ASMENS DUOMENŲ SAUGUMO PAŽEIDIMO TYRIMO ATASKAITA

_____ Nr. _____
(data, dokumento numeris)

1. Asmens duomenų saugumo pažeidimo aprašymas

1.1. Asmens duomenų saugumo pažeidimo:
Data _____, laikas _____ir vieta _____;
Asmens duomenų saugumo pažeidimo nustatymo:
data _____, laikas _____ir vieta _____ .

1.2. Asmens duomenų saugumo pažeidimo vieta (pažymėti tinkamą (-us):
1.2.1. Informacinė sistema
1.2.2. Duomenų bazė
1.2.3. Tarnybinė stotis
1.2.4. Interneto svetainė
1.2.5. Debesų kompiuterijos paslaugos
1.2.6. Nešiojami/mobilieji įrenginiai
1.2.7. Neautomatiniu būdu susistemintos bylos (archyvas)
1.2.8. Kita (įrašyti):
_____
_____

1.3. Asmens duomenų saugumo pažeidimo pobūdis (pažymėti tinkamą (-us):
1.3.1. Konfidencialumo pažeidimas (be leidimo ar neteisėtai atskleidžiami asmens duomenys arba gaunama prieiga prie jų);
1.3.2. Vientisumo pažeidimas (asmens duomenys pakeičiami be leidimo ar netyčia);
1.3.3. Prieinamumo praradimas (netyčia arba neteisėtai prarandama prieiga prie jos arba sunaikinami asmens duomenys)

1.4. Asmens duomenų, kurių saugumas pažeistas, kategorijos (pažymėti tinkamą (-us) ir aprašyti):
1.4.1. Asmens tapatybę patvirtinantys duomenys (vardas, pavardė, gimimo data, lytis ir kt.):
_____
_____

1.4.2. Asmens identifikaciniai ar prisijungimo duomenys (asmens kodas, mokėtojo kodas, slaptažodžiai ir kt.):
_____
_____

1.4.3. Asmens kontaktiniai duomenys (gyvenamosios vietos adresas, telefono numeris, elektroninio pašto adresas ir kt.):
_____

_____

1.4.4. Specialiųjų kategorijų asmens duomenys (duomenys, susiję su asmens sveikata, genetiniai duomenys, biometriniai duomenys, duomenys, susiję su asmens rasine ar etnine kilme, duomenys, susiję su asmens politinėmis pažiūromis, religiniais, filosofiniais įsitikinimais ar naryste profesinėse sąjungose, duomenys, susiję su asmens lytiniu gyvenimu ir lytine orientacija, ir kt.):

_____

_____

1.4.5. Duomenys apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas:

_____

_____

1.4.6. Kiti asmens duomenys:

_____

_____

1.5. Apytikslis asmens duomenų, kurių saugumas pažeistas, skaičius:

_____

1.6. Duomenų subjektų, kurių asmens duomenų saugumas pažeistas, kategorijos (administracijos darbuotojai, pacientai, vaikai, asmenys, pateikę prašymus, skundus ir kt.):

_____

_____

1.7. Apytikslis duomenų subjektų, kurių asmens duomenų saugumas pažeistas, skaičius:

_____

1.8. PRATC darbuotojas, pranešęs apie asmens duomenų saugumo pažeidimą (vardas, pavardė, struktūrinio padalinio, kuriame dirba darbuotojas, pavadinimas, telefono numeris, elektroninio pašto adresas):

_____

_____

1.9. Duomenų tvarkytojas, pranešęs apie asmens duomenų saugumo pažeidimą (pavadinimas, kontaktinio asmens duomenys (vardas, pavardė, telefono numeris, elektroninio pašto adresas):

_____

_____

1.10. Kaip ilgai tęsėsi asmens duomenų saugumo pažeidimas

_____

2. Asmens duomenų saugumo pažeidimo keliamos rizikos duomenų subjektų teisėms ir laisvėms įvertinimas

2.1. Priežastys, lėmusios asmens duomenų saugumo pažeidimą (pvz., duomenų ir įrangos, kurioje saugomi asmens duomenys, vagystė, netinkamos prieigos kontrolės priemonės, leidžiančios neteisėtai naudotis asmens duomenimis, įrangos gedimas, žmogiška klaida, įsilaužimo ataka ir pan.)

_____

2.2. Specifiniai fizinių asmenų, kurių asmens duomenų saugumas buvo pažeistas, ypatumai (vaikai, asmenys su negalia ir kt.):

_____

_____

2.3. Galimybė identifikuoti fizinį asmenį (pvz., iki asmens duomenų saugumo pažeidimo

asmens duomenys buvo tinkamai užšifruoti, anonimizuoti, arba iki saugumo pažeidimo asmens duomenims šifravimas nebuvo taikomas ir kt.):

_____

_____

2.3. Kas gavo prieigą prie asmens duomenų, kurių saugumas pažeistas?

_____

_____

2.4. Ar buvo kokių kitų įvykių ar aplinkybių, turėjusių poveikį asmens duomenų saugumo pažeidimo padarymui?

_____

_____

2.5. Kokia žala padaryta fiziniams asmenims (duomenų subjektams, grėsmė fiziniam saugumui, grėsmė emocinei gerovei, žala reputacijai, finansams, tapatybės vagystė, teisinė atsakomybė, konfidencialumo, saugumo nuostatų pažeidimas)?

_____

_____

2.6. Galimos asmens duomenų saugumo pažeidimo pasekmės:

2.6.1. Konfidencialumo pažeidimo atveju (pažymėti tinkamą (-us):

2.6.1.1. Asmens duomenų išplitimas labiau, nei tai yra būtina, ir duomenų subjekto kontrolės praradimas savo asmens duomenų atžvilgiu (pvz., asmens duomenys išplito internete);

2.6.1.2. Skirtingos informacijos susiejimas (pvz., gyvenamosios vietos adreso susiejimas su asmens buvimo vieta realiu laiku);

2.6.1.3. Galimas panaudojimas kitais, nei nustatytais, ar neteisėtais tikslais (pvz., komerciniais tikslais, asmens tapatybės pasisavinimo tikslu, informacijos panaudojimo prieš asmenį tikslu);

2.6.1.4. Kita:

_____

2.6.2. Vientisumo pažeidimo atveju (pažymėti tinkamą (-us):

2.6.2.1. Pakeitimas į neteisingus duomenis, dėl ko asmuo gali netekti galimybės naudotis paslaugomis;

2.6.2.2. Pakeitimas į kitus duomenis, kad asmens duomenų tvarkymas būtų nukreiptas tam tikra linkme (pvz., pavogta asmens tapatybė susiejant vieno asmens identifikuojančius duomenis su kito asmens biometriniais duomenimis);

2.6.2.3. Kita:

_____

_____

2.6.2. Prieinamumo pažeidimo atveju (pažymėti tinkamą (-us):

2.6.3.1. Dėl asmens duomenų trūkumo negalima teikti paslaugų (pvz., tam tikrų procesų sutrikdymas, dėl ko negalima prieiti prie tvarkomų asmens duomenų ir įgyvendinti duomenų subjekto teisę susipažinti su jo tvarkomais asmens duomenimis);

2.6.3.2. Dėl klaidų asmens duomenų tvarkymo procesuose negalima teikti tinkamos paslaugos (pvz., tam tikra informacija iš informacinės sistemos išnyko, dėl ko negalima tinkamai suteikti paslaugos);

2.6.3.3. Kita:

_____

_____

2.7. Asmens duomenų saugumo pažeidimo sukeltos rizikos duomenų subjektų teisėms ir laisvėms lygis:

2.7.1. Žema rizikos tikimybė (dėl asmens duomenų saugumo pažeidimo nėra pavojaus fizinių asmenų teisėms ir laisvėms);

2.7.2. Vidutinė rizikos tikimybė (dėl asmens duomenų saugumo pažeidimo yra/gali kilti pavojus fizinių asmenų teisėms ir laisvėms, būtina pranešti Valstybinei duomenų apsaugos inspekcijai);

2.7.3. Didelė rizikos tikimybė (dėl asmens duomenų saugumo pažeidimo yra/gali kilti didelis pavojus fizinių asmenų teisėms ir laisvėms, būtina pranešti Valstybinei duomenų apsaugos inspekcijai ir duomenų subjektams);

2.8. Kas turėjo prieigą prie pažeistų asmens duomenų iki asmens duomenų saugumo pažeidimo padarymo?

2.9. Kas gavo prieigą prie pažeistų asmens duomenų?

2.10. Ar buvo kokių kitų įvykių, kurie galėjo turėti poveikį asmens duomenų saugumo pažeidimo padarymui?

2.11. Ar iki asmens duomenų saugumo pažeidimo asmens duomenys buvo tinkamai užkoduoti, anonimizuoti ar kitaip lengvai neprieinami?

2.12. Informacinių technologijų sistemos, įrenginiai, įranga, įrašai, susiję su asmens duomenų saugumo pažeidimu:

_____

2.13. Tai yra sisteminė klaida ar vienetinis incidentas?

2.14. Kokių veiksmų/priemonių buvo imtasi sužinojus apie padarytą asmens duomenų saugumo pažeidimą?

_____

2.15. Kokios taikytos priemonės, siekiant sumažinti neigiamą poveikį duomenų subjektams?

_____

_____

2.16. Kokios techninės priemonės buvo taikomos asmens duomenų saugumo pažeidimo paveiktiems asmens duomenims, užtikrinant, kad asmens duomenys nebūtų prieinami neįgaliotiems asmenims?

_____

2.17. Techninės ir (ar) organizacinės saugumo priemonės, kurios įgyvendintos dėl asmens duomenų saugumo pažeidimo, taip pat siekiant, kad pažeidimas nepasikartotų:

_____

2.18. Techninės ir (ar) organizacinės saugumo priemonės, kurios ketinamos įgyvendinti dėl asmens duomenų saugumo pažeidimo, įskaitant ir priemones sumažinti asmens duomenų saugumo pažeidimo pasekmes, ir už priemonių įgyvendinimą atsakingi asmenys:

---

3. Pranešimų apie asmens duomenų saugumo pažeidimą pateikimas

3.1. Ar pranešta Valstybinei duomenų apsaugos inspekcijai (toliau – VDAI) apie asmens duomenų saugumo pažeidimą?

3.1.1. Taip

Pranešimo VDAI data _____ numeris _____

3.1.2. Ne (nurodomos nepranešimo VDAI priežastys):

_____

3.1.3. Apie duomenų saugumo pažeidimą pranešta VDAI vėliau nei per 72 valandas (nurodomos vėlavimo pranešti VDAI priežastys):

_____

3.2. Ar pranešta duomenų subjektui apie asmens duomenų saugumo pažeidimą?

3.2.1. Taip

Pranešimo duomenų subjektui data _____ numeris _____ (jeigu pranešimas užregistruotas)

Pranešimo duomenų subjektui būdas (pažymėti tinkamą (-us):
□ paštu □ elektroniniu paštu □ trumpąja žinute (SMS) □ kitais būdais

Informuotų duomenų subjektų skaičius:

_____

Pranešimo duomenų subjektui turinys:

_____

3.2.2. Ne (nurodomos nepranešimo duomenų subjektui priežastys):

_____

3.2.3. Apie duomenų saugumo pažeidimą duomenų subjektams pranešta vėliau nei per 72 valandas (nurodomos vėlavimo pranešti duomenų subjektui priežastys):

_____

_____

3.2.4. Apie saugumo pažeidimą pranešta viešai (nurodoma, kada ir kur paskelbta informacija viešai, arba, jei taikyta kita priemonė, nurodoma, kokia ir kada taikyta):

_____

3.2.4. Bus pranešta vėliau

_____

3.3. Ar pranešta valstybės institucijoms, įgaliotoms atlikti ikiteisminį tyrimą, apie asmens duomenų saugumo pažeidimą, galimai turintį nusikalstamos veikos požymių (jeigu taip, nurodoma rašto data ir numeris):

_____

_____

3.4. Ar pranešta valstybės institucijoms, nurodytoms Lietuvos Respublikos kibernetinio saugumo įstatyme, apie kibernetinį incidentą, susijusį su asmens duomenų saugumo pažeidimu:

_____

(pareigos, vardas ir pavardė)

Asmens duomenų saugumo pažeidimų
valdymo UAB Panevėžio regiono atliekų
tvarkymo centre tvarkos aprašo
3 priedas

UAB PANEVĖŽIO REGIONO ATLIEKŲ TVARKYMO CENTRAS

_____
(pareigų pavadinimas)

_____
(vardas, pavardė)

ASMENS DUOMENŲ SAUGUMO INCIDENTO ATASKAITA

_____ Nr. _____
(data)

1.	**Asmens duomenų saugumo incidento aprašymas**	
2.	**Tyrimo metu nustatytos aplinkybės**	
3.	**Konsultaciją suteikęs asmuo, konsultacijos metu įvertintos aplinkybės ir išvada (esant poreikiui)**	
4.	**Asmens duomenų saugumo incidento įvertinimas**	
5.	**Rekomendacijos (esant poreikiui)**	

_____ _____
(pareigos) (vardas, pavardė)

_____

Asmens duomenų saugumo pažeidimų valdymo UAB Panevėžio regiono atliekų tvarkymo centre tvarkos aprašo
4 priedas

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ UAB PANEVĖŽIO REGIONO ATLIEKŲ TVARKYMO CENTRE REGISTRAVIMO ŽURNALAS

Eil. Nr.	**Pažeidimo nustatymo data, laikas ir vieta**	**PRATC darbuotojas ar duomenų tvarkytojas, pranešęs apie pažeidimą (vardas, pavardė, pareigos ar pavadinimas)**	**Pažeidimo padarymo data ir vieta**	**Pažeidimo pobūdis, priežastys ir kitos aplinkybės**	**Duomenų subjektų, kurių asmens duomenų saugumas pažeistas, kategorijos ir apytikslis skaičius**	**Asmens duomenų, kurių saugumas pažeistas, kategorijos ir apytikslis skaičius**	**Tikėtinos pažeidimo pasekmės bei pavojus fizinių asmenų teisėms ir laisvėms**	**Priemonės, kurių buvo imtasi pažeidimui pašalinti ir (ar) neigiamoms pažeidimo pasekmėms sumažinti**	**Informacija, ar apie pažeidimą buvo pranešta Valstybinei duomenų apsaugos inspekcijai, priimto sprendimo motyvai**	**Informacija, ar apie pažeidimą buvo pranešta duomenų subjektui (subjektams), priimto sprendimo motyvai**	**Kita informacija, susijusi su asmens duomenų saugumo pažeidimu**
1.											
2.											
3.											
4.											
5.											
6.											
7.											
8.											
9.											
10.											

_____