PATVIRTINTA
Palangos miesto socialinių paslaugų centro direktoriaus
2021 m. gegužės 18 d. įsakymu Nr. V1-126

PALANGOS MIESTO SOCIALINIŲ PASLAUGŲ CENTRO ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ VALDYMO TVARKOS APRAŠAS

I BENDROSIOS NUOSTATOS

1. **Asmens duomenų saugumo pažeidimų valdymo tvarkos aprašo (toliau – Aprašas) tikslas**-nustatyti duomenų tvarkymo metu įvykusių asmens duomenų saugumo pažeidimo valdymo, tyrimo , pašalinimo ir pranešimų apie įvykusį pažeidimą (toliau-Pranešimas) Valstybinei duomenų apsaugos inspekcijai (toliau VDAI) ir (ar) duomenų subjektams įgyvendinimo tvarką Palangos miesto socialinių paslaugų centre (toliau – Centras) , užtikrinti , kad Centro darbuotojai sugebėtų laiku nustatyti galimus pažeidimus bei suprastų, kokie veiksmai privalo būti atlikti valdant juos.
2. **Pagrindinės taisyklėse vartojamos sąvokos:**
   2.1.Asmens duomenų saugumo pažeidimas (neatitiktis) (toliau-Pažeidimas)-duomenų saugumo pažeidimas, dėl kurio netyčia arba neteisėtai sunaikinami , prarandami, pakeičiami , be leidimo atskleidžiami persiųsti , saugomi arba kitaip tvarkomi asmens duomenys arba prie jų be leidimo gaunama prieiga.
   2.2.Informacijos saugumo incidentas- vienas ar daugiau nepageidaujamų ir netikėtų informacijos saugumo įvykių , turinčių didelę tikimybę pakenkti veiklai ir keliančių grėsmę informacijos saugumui.
   2.3.Duomenų apsaugos pareigūnas (toliau Pareigūnas) -Centro direktoriaus paskirtas darbuotojas , atliekantis BDAR nustatytas duomenų apsaugos pareigūno funkcijas.
   2.4.Įgaliotas darbuotojas -Centro direktoriaus paskirtas darbuotojas atsakingas už Pažeidimų tyrimą, pašalinimą ir pranešimą apie juos priežiūros institucijai ir duomenų subjektams.
3. Tiriant galimus Pažeidimus ir teikiant Pranešimus vadovaujamasi 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentu (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB(Bendrasis duomenų apsaugos reglamentas) (toliau -BDAR), Lietuvos Respublikos asmens teisės apsaugos įstatymu (toliau- ADTAĮ) ir kitais teisės aktais, kurie nustato šių procedūrų atlikimo tvarką.

II ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ NUSTATYMAS

4. Galimi šie Pažeidimai pagal pobūdį (tipą):
   4.1. Konfidencialumo pažeidimas-neleistinas arba netyčinis asmens duomenų atskleidimas arba prieigos prie jų suteikimas (pavyzdžiui-atskleisti duomenys ir jie tapo prienami tretiesiems asmenims, suteikiant prieigą, tinkamai nešifruojant , kt.);
   4.2. Duomenų pasiekiamumo/prieinamumo-neleistinas ar netyčinis prieigos prie asmens duomenų praradimas arba asmens duomenų sunaikinimas (pavyzdžiui- prarasti duomenys ir neturima atsarginių kopijų);
   4.3. Duomenų vientisumo pažeidimas- neleistinas arba netyčinis asmens duomenų pakeitimas(pavyzdžiui- prarasti vaikų duomenys, turima tik dalis atsarginių kopijų, dėl ko neįmanoma „atkurti“ visos su vaiku bendravimo istorijos);
   4.4. Mišraus pobūdžio (tipo) pažeidimas- asmens duomenų konfidencialumo, prieinamumo ir vientisumo pažeidimas ar bet kurių aukščiau nurodytų pažeidimų derinys.

5. Pažeidimas gali įvykti dėl šių priežasčių:
   5.1.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 / mobilūs įrenginiai (telefonas, nešiojamas kompiuteris, išorinės duomenų laikmenos) , kuriose saugomi asmens duomenys, kt.);
   5.2.vagystė (pvz., pavogti nešiojami / mobilūs įrenginiai , kuriuose saugomi asmens duomenys; pavogtos neautomatiniu būdu susistemintos bylos, kuriose yra asmens duomenų ir kt.);
   5.3.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.);
   5.4.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.);
   5.5 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.);
   5.6.nenumatytos (force majeure) aplinkybės ir kitos priežastys (gaisras, vandens užliejimas, dėl kurių sugadinami arba prarandami asmens duomenys ir kt.).
6. Pažeidimas , galintis kelti pavojų asmens 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 finansini nuostolių , pakenkta jo reputacijai, prarastas duomenų, kurie laikomi profesine paslaptimi, konfidencialumas ir kt.).

III PRANEŠIMAS APIE GALIMĄ ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ

7. Centro darbuotojas, pastebėjęs , nustatęs , gavęs informaciją apie galimą Pažeidimą iš duomenų tvarkytojo ar kito šaltinio, privalo:
   7.1.nedelsiant , bet ne vėliau kaip per 2 darbo valandas nuo galimo Pažeidimo paaiškėjimo momento informuoti žodžiu, raštu ar elektroninėmis priemonėmis Centro direktoriaus įgaliotą darbuotoją;
   7.2.užpildyti Pranešimą apie asmens duomenų saugumo pažeidimą (toliau- Pranešimas) ir nedelsiant , bet ne vėliu kaip per 4 darbo valandas nuo galimo Pažeidimo paaiškėjimo momento perduoti jį Centro direktoriaus įgaliotam darbuotojui (Pranešimo forma -patvirtinta VDAI direktoriaus 2018 m. rugpjūčio 29 d. įsakymu Nr. 1T-82(1.12.-E));
   7.3.jeigu įmanoma, imtis priemonių pašalinti galimą Pažeidimą ir imtis priemonių galimoms neigiamoms jo pasekmėms sumažinti.

IV ASMENS DUOMENŲ SAUGUMO PAŽEIDIMO TYRIMAS IR PAŠALINIMAS

8. Centro direktoriaus įgaliotas darbuotojas , gavęs Pranešimą apie Pažeidimą, privalo:
   8.1. atlikti Pažeidimo tyrimą ir nedelsdamas , bet ne vėliau kaip per 24 valandas nuo Pranešimo gavimo momento nagrinėti Pranešime nurodytas aplinkybes;
   8.2. įvertinti , ar padarytas Pažeidimas;
   8.3. jei pažeidimas yra susijęs su elektroninės informacijos saugos incidentu, pasitelkti Centro ar duomenų tvarkytojo IT specialistus;
   8.4. jei Pažeidimas padarytas , nustatyti kokio pobūdžio (tipo) Pažeidimas padarytas, asmens duomenų , kurių saugumas pažeistas, kategorijas, įskaitant specialistų kategorijų asmens duomenis, Pažeidimo priežastis, Pažeidimo apimtis (duomenų subjektų kategorijos ir jų skaičius), esamas ir (ar) galimas pasekmes ir žalą , padarytą duomenų subjektui(-ams),

įvertinti pavojų duomenų subjekto teisėms ir laisvėms (toliau-rizika), kuris gali atsirasti dėl galimo Pažeidimo, pateikti užpildytą Asmens duomenų saugumo pažeidimo tyrimo ataskaitą (toliau-Ataskaita) dėl pažeidimo buvimo ir rizikos (Aprašo 1 priedas)

8.5. teikti rekomendacijas Centro darbuotojams, atsakingiems už Pažeidimo ir (ar) jo pasekmių pašalinimą ir (ar) sumažinimą ir (ar) duomenų tvarkytojui dėl tinkamų techninių ir organizacinių priemonių , kad Pažeidimas būtų išsamiai ištirtas ir jis ir (ar) jo pasekmės būtų pašalintos ir (ar) sumažintos ir pažeidimas ateityje nepasikartotų , taikymo ir (arba) pats imtis šių veiksmų;

8.6. įvertinti , kokių skubių ir tinkamų priemonių būtina imtis, kad būtų pašalintas Pažeidimas;

8.7. nustatyti ar apie Pažeidimą būtina pranešti VDAI;

8.8. nustatyti , ar apie Pažeidimą būtina pranešti duomenų subjektams.

9. Atliekant Pažeidimo tyrimą ir siekiant nustatyti, ar Pažeidimas iš tikrųjų įvyko, esamos situacijos įrodymai privalo būti fiksuojami dokumentuose ir užtikrinamas jų atsekamumas.
10. Pažeidimo tyrimo metu darbuotojai ir duomenų tvarkytojas privalo operatyviai teikti Centro direktoriaus įgaliotam asmeniui visą jo paprašytą su Pažeidimu susijusią informaciją ir dokumentus.
11. 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:

    11.1.saugumo pažeidimo pobūdis (konfidencialumo, vientisumo ar prieinamumo pažeidimas)-nustatomas saugumo pažeidimo pobūdis: nuo padaryto pažeidimų pobūdžio gali priklausyti pavojaus duomenų subjektams dydis;

    11.2.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;

    11.3.galimybė identifikuoti fizinį asmenį-įvertinamą , 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);

    11.4.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;

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

    11.6.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.
12. Įvertinus riziką, nustatomas vienas iš trijų rizikos tikimybių lygių- maža, vidutinė ar didelė rizikos tikimybė.
13. Ataskaita yra pateikiama Centro direktoriui .
14. Atsižvelgiant į Ataskaitą, Centro direktorius, jei reikia , tvirtina priemonių planą , kuriame numatomas būtinų techninių, organizacinių, administracinių ir kitų priemonių poreikis dėl Pažeidimo pašalinimo, paskiria atsakingus vykdytojus ir nustato priemonių įgyvendinimo terminus.
15. Sprendžiant Pažeidimo pašalinimo klausimą, bei tvirtinant priemonių planą, pirmiausia būtina atlikti veiksmus, siekiant apriboti ar sustabdyti saugumo incidentą. Priklausomai nuo konkrečių Pažeidimo aplinkybių, turėtų būti atlikti tokie veiksmai, kaip: ištrinti asmens duomenis nuotoliniu būdu iš pamesto a pavogto nešiojamo/ mobilaus įrenginio (telefono, nešiojamo kompiuterio ir kt.); jei asmens duomenys per klaidą išsiunčiami ne tam adresatui, kuriam jie buvo skirti, 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 asmenis; atkuriant prarastus ar sugadintus asmens duomenis, naudoti atsargines kopijas ir kt.

16. Siekiant apriboti ar sustabdyti Pažeidimą, būtina kiek įmanoma tiksliau surinkti duomenų ir įrodymų 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.).
17. Priemonių plane turi būti numatyti veiksmai, nukreipti ne vien į esamo Pažeidimo priežasties pašalinimą, pavojaus fizinių asmenų teisėms ir laisvėms sumažinimą ar pašalinimą, bet taip pat skirti neleisti pasikartoti Pažeidimui. Būtina atsižvelgti į trūkumus ir duomenų tvarkymo silpnąsias vietas, kurios buvo išnaudotos įvykdyti Pažeidimą bei imtis priemonių tuos trūkumus pašalinti.

V PRANEŠIMAS APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ PRIEŽIŪROS INSTITUCIJAI

18. Tyrimo metu nustačius, kad Pažeidimas buvo, Centro direktoriui priėmus sprendimą dėl Pranešimo priežiūros institucijai pateikimo būtinybės, Centro direktoriaus įgaliotas darbuotojas privalo nedelsiant , bet ne vėliau ne per 72 val. nuo tada, kai tapo žinoma apie Pažeidimą, apie tai informuoti VDAI, išskyrus atvejus, kai Pažeidimas nekelia pavojaus fizini asmenų teisėms ir laisvėms.
19. 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 tvarko aprašo patvirtinimo“ (su visais aktualiais pakeitimais), nustatyta tvarka sąlygomis , užpildant Pranešimo apie asmenų duomenų saugumo pažeidimo formą, patvirtintą VDAI direktoriaus 2018 m. rugpjūčio 29 d. įsakymu Nr. 1T-82(1.12.E).
20. Jeigu įvertinus riziką, abejojama , ar Pažeidimas kelia pavojų fizinių asmenų teisėms ir laisvėms, apie pažeidimą pranešama VDAI.
21. Jeigu įvertinus riziką, nustatoma, kad tuo metu apie Pažeidimą VDAI pranešti nereikia, po kurio laiko situacija gali pasikeisti , todėl Pažeidimas bei jo keliamas pavojus fizinių asmenų teisėms ir laisvėms turėtų būti vertinamas iš naujo(pvz., pamesta USB atmintinė, kurioje saugomi asmens duomenys , užšifruoti 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 bus vertinamas iš naujo ir apie tokį pažeidimą reikia pranešti VDAI).
22. Tuo atveju kai, priklausomai nuo Pažeidimo pobūdžio , būtina atlikti išsamesnį tyrimą, nustatyti visus svarbius faktus , susijusius su pažeidimu , ir per 72 valandas dėl objektyvių priežasčių nėra įmanoma ištirti padarytą pažeidimą , informacija VDAI teikiama etapais, nurodant vėlavimo priežastis. Apie informacijos teikimą etapais VDAI informuojama teikiant pirminį pranešimą.
23. Jeigu po pranešimo VDAI pateikimo, atlikus tolesnį tyrimą, yra nustatoma, kad saugumo incidentas buvo sustabdytas ir faktiškai Pažeidimo nebuvo , apie tai nedelsiant informuojama VDAI.
24. Tuo atveju , kai yra įtariama, kad Pažeidimas turi nusikalstamos veiklos požymių , informacija apie galimą nusikalstamą veiklą pateikiama atitinkamos valstybės institucijoms , įgaliotoms atlikti ikiteisminį tyrimą, teisės aktų , reguliuojančių tokios informacijos teikimą, nustatyta tvarka.

VI PRANEŠIMAS APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ DUOMENŲ SUBJEKTUI

25. Tyrimo metu nustačius, kad dėl Pažeidimo gali kilti didelis pavojus fizini asmenų teisėms ir laisvėms. Centro direktoriaus įgaliotas darbuotojas 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 didelis pavojus.
26. Duomenų subjektas informuojamas tiesiogiai, t.y. siunčiant jam pranešimą paštu , elektroniniu paštu , trumpąja žinute (SMS) ar kitu būdu. Pranešimas duomenų subjektui siunčiamas atskirai nuo kitos siunčiamos informacijos , kaip naujienlaiškiai ar standartiniai pranešimai.
27. 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:
    27.1.asmens duomenų saugumo pažeidimo pobūdžio ir tikėtinų pažeidimo pasekmių aprašymas;
    27.2.priemonių , kurių ėmėsi Centras , kad būtų pašalintas saugumo pažeidimas, įskaitant priemonių galimoms neigiamoms jo pasekmėms sumažinti aprašymas;
    27.3.duomenų apsaugos atsakingo darbuotojo arba kito kontaktinio asmens, galinčio suteikti daugiau informacijos, vardas, pavardė ir kontaktiniai duomenys;
    27.4.kita reikšminga informacija, susijusi su Pažeidimu, kuri Centro direktoriaus įgalioto darbuotojo manymu, turėtų būti pateikta duomenų subjektui (pvz., patarimai, kaip apsisaugoti nuo galimų neigiamų pažeidimo pasekmių).
28. Pranešimo apie Pažeidimą duomenų subjektams teikti nereikia, jeigu:
    28.1.Centras 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);
    28.2.iš karto po pažeidimo Centras ėmėsi priemonių , kuriomis užtikrinama , kad nekiltų didelis pavojus duomenų subjektų teisėms ir laisvėms;
    28.3.tiesioginio pranešimo duomenų subjektui patrikimas pareikalautų neproporcingai didelių pastangų (pvz., jei jų kontaktiniai duomenys buvo prarasti dėl pažeidimo arba iš pradžių nebuvo žinomi). Tokiu atveju apie pažeidimą viešai paskelbiamas Centro interneto svetainėje, spaudoje, pasitelkiami ne vienas , o keli informavimo būdai arba taikomos panašios priemonės, kuriomis duomenų subjektai būtų efektyviai informuojami (pvz., vien tik pranešimas interneto svetainėje nėra efektyvi informavimo priemonė).

29. Jeigu įvertinus riziką, nustatoma, kad tuo metu apie Pažeidimą duomenų subjektams pranešti nereikia, po kurio laiko situacija gali pasikeisti, todėl Pažeidimas bei jo keliamas pavojus fizinių asmenų teisėms ir laisvėms turėtų būti vertinamas iš naujo (pvz., įvykdoma kibernetinė ataka, naudojant išpirkos reikalaujančią programą ir duomenų bazėje esantys asmens duomenys užšifruojami- jei atlikus tyrimą , paaiškėja, kad vienintelė išpirkos reikalaujančios programos užduotis buvo užšifruoti asmens duomenimis ir jokio kito kenksmingumo poveikio duomenų bazei nėra, apie saugumo pažeidimą reikės pranešti tik VDAI , tačiau 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).
30. Tam tikromis aplinkybėmis , kai tai yra pagrįsta, Centras pasitaręs su teisėsaugos institucijomis ir atsižvelgdamas į teisėtus teisėsaugos interesus, gali atidėti asmenų , kuriems pažeidimas turi poveikio, informavimą apie saugumo pažeidimą iki to laiko, kai tai netrukdys saugumo pažeidimo tyrimams.

VII ASMENS DUOMENŲ SAUGOJIMO PAŽEIDIMŲ DOKUMENTAVIMAS

31. Visi pažeidimai , nepriklausomai nuo to, ar apie juos buvo pranešta VDAI ir (ar) duomenų subjektui , ar tokie pažeidimai kelia riziką, registruojami /asmens duomenų saugumo pažeidimų registravimo žurnale (toliau -Žurnalas) (Aprašo 2 priedas)
32. Informacija apie Pažeidimą į Žurnalą turi būti įvedama nedelsiant , kai tik paaiškėja galimas Pažeidimas, bet ne vėliau kaip per 5 darbo dienas nuo galimo pažeidimo paaiškėjimo momento. Kai pasikeičia Žurnale nurodyta informacija arba paaiškėja nauja informaciją, Žurnale esanti informacija turi būti papildoma ir (ar) koreguojama.
33. Asmens duomenų saugumo pažeidimų registravimo žurnale nurodoma:
    33.1.pažeidimo nustatymo aplinkybės(Pažeidimo nustatymo data, laikas, vieta, subjektas, pranešęs apie pažeidimą);
    33.2.pažeidimo aplinkybės(pažeidimo data, vieta, pažeidimo pobūdis, priežastys, asmens duomenų , kurių saugumas pažeistas, kategorijos r apytikslis skaičius, duomenų subjektų , kurių asmens duomenų saugumas pažeistas, kategorijos ir apytikslis skaičius);
    33.3.tikėtinos pažeidimo pasekmės ir pavojus duomenų subjekto teisėms ir laisvėms;
    33.4.priemonės, kurių buvo imtasi, kad būtų pašalintas pažeidimas, įskaitant priemones galimoms neigiamoms pažeidimo pasekmėms sumažinti;
    33.5.informacija apie pranešimą VDAI apie asmens duomenų saugumo pažeidimą;
    33.6.jei apie asmens duomenų saugumo pažeidimą nebuvo pranešta VDAI, nurodomi tokio sprendimo motyvai; jei apie asmens duomenų saugumo pažeidimą buvo pranešta VDAI, nurodoma pranešimo data ir numeris, taip pat , ar panešimas teikiamas etapais;
    33.7.jeigu apie asmens duomenų saugumo pažeidimą buvo vėluojama pranešti VDAI, nurodomos tokio vėlavimo priežastys;
    33.8.informacija apie pranešimą duomenų subjektui (subjektams) apie asmens duomenų saugumo pažeidimą;
    33.9.jei apie asmens duomenų saugumo pažeidimą nebuvo praneša 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);
    33.10.jeigu apie asmens duomenų apsaugos pažeidimą buvo vėluojama pranešti duomenų subjektui (subjektams), nurodoma tokio vėlavimo priežastys;
    33.11.kita reikšminga informacija, susijusi su asmens duomenų saugumo pažeidimu.

34. Už Žurnalo pildymą ir saugojimą atsakingas Centro direktoriaus įgaliotas darbuotojas. Žurnalas gali būti popierinis arba elektroninės formos. Užpildytas Žurnalas saugomas 5 metus nuo paskutinio įrašo Žurnale padarymo dienos.
35. Žurnalas yra pateikiamas VDAI jai pareikalavus.

VII BAIGIAMOSIOS NUOSTATOS

36. Aprašas skirtas užtikrinti, kas Centro darbuotojai sugebėtų laiku nustatyti galimus Pažeidimus bei supratų, kokie veiksmai privalo būti atlikti valdant juos.
37. Aprašo privalo laikytis vis Centro darbuotojai, kurie tvarko asmens duomenis arba eidami savo pareigas jus sužino.

38. Centro darbuotojai ir duomenų tvarkytojai privalo išsaugoti esamos situacijos, susijusios su galimu Pažeidimu, įrodymus, kad vėliau naudojant technines ir organizacines priemones(pvz., duomenų srauto ir prisijungimų analizės įrankius ar kt.) galima būtų tirti Pažeidimą.
39. Centro darbuotojai , pažeidę šio Aprašo reikalavimus , atsalo Lietuvos Respublikos teisės aktų nustatyta tvarka.
40. Aprašo priedai yra neatsiejama šio Aprašo dalis.

1 priedas

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMO ATASKAITA

_____ Nr. _____
(data)

_____
(vieta)

1. Asmens duomenų saugumo pažeidimo (toliau – pažeidimas) aprašymas	
1.1. Pažeidimo nustatymo data, laikas (valanda, minutės)	
1.2. Darbuotojas, pranešęs apie pažeidimą (vardas ir pavardė, pareigos, telefono numeris, elektroninio pašto adresas)	
1.3. Duomenų tvarkytojo, pranešusio apie pažeidimą, pavadinimas, jo kontaktinio asmens duomenys (vardas ir pavardė, telefono Nr., elektroninio pašto adresas)	
1.4. Pažeidimo data, laikas (valanda, minutės)	
1.5. Pažeidimo vieta (adresas, informacinės sistemos pavadinimas, duomenų bazė, įrenginys ir pan.)	
1.6. Pažeidimo pobūdis, esmė ir aplinkybės	
1.6.1. Susijusios faktinės aplinkybės:	
1.6.2. Asmens duomenų konfidencialumo praradimas (be leidimo ar neteisėtai atskleidžiami asmens duomenys arba gaunama prieiga prie jų)	
1.6.3. Asmens duomenų vientisumo praradimas (kai asmens duomenys pakeičiami be leidimo ar netyčia)	
1.6.4. Asmens duomenų prieinamumo praradimas (kai netyčia arba neteisėtai prarandama prieiga prie jų arba sunaikinami asmens duomenys)	
1.7. Duomenų subjektų, kurių duomenų saugumas pažeistas, kategorijos (darbuotojas, klientas, IT specialistas ir pan.) ir šių duomenų subjektų apytikslis skaičius (jei įmanoma)	
1.8. Pažeidimo trukmė	
1.9. Asmens duomenų, kurių saugumas pažeistas, kategorijos (jei įmanoma):	
1.9.1. Asmens duomenys (išvardyti kategorijas)	
1.9.2. Specialių kategorijų asmens duomenys (išvardyti kategorijas)	

1.9.3. Duomenys apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas (išvardyti kategorijas)	
1.9.4. Asmens duomenų, kurių saugumas pažeistas, apytikslis skaičius	
2. Pažeidimo rizikos įvertinimas	
2.1. Priežastys bei įvykiai, turėję įtakos įvykti pažeidimui (pvz., duomenų ar įrangos, kurioje yra saugomi asmens duomenys, vagystė, netinkamos prieigos kontrolės priemonės, leidžiančios neteisėtai naudotis asmens duomenimis, įrangos gedimas, žmogiška klaida, įsilaužimo ataka ir pan.)	
2.2. Pažeidimo pasekmės (aprašyti tinkamas):	
2.2.1. Atsitiktinai arba neteisėtai sunaikinti asmens duomenys	
2.2.2. Atsitiktinai arba neteisėtai prarasti asmens duomenys	
2.2.3. Atsitiktinai arba neteisėtai pakeisti asmens duomenys	
2.2.4. Atsitiktinai arba neteisėtai atskleisti asmens duomenys teisės susipažinti su jais neturintiems asmenims (jei įmanoma, nurodomi neteisėtą prieigą gavę asmenys)	
2.2.5. Asmens duomenų išplitimas labiau, nei tai yra būtina, ir duomenų subjekto kontrolės praradimas savo asmens duomenų atžvilgiu (pavyzdžiui, asmens duomenys išplito internete)	
2.2.6. Skirtingos informacijos susiejimas	
2.2.7. Asmens duomenų panaudojimas neteisėtais tikslais	
2.2.8. Dėl asmens duomenų trūkumų negalima vykdyti funkcijų	
2.2.9. Dėl klaidų asmens duomenų tvarkymo procesuose negalima tinkamai vykdyti funkcijų	
2.2.10. Kita	
2.3. Pavojus fizinių asmenų teisėms ir laisvėms (nurodyti tinkamą ir pateikti pagrindžiančius argumentus):	
2.3.1. Dėl pažeidimo nėra pavojaus fizinių asmenų teisėms ir laisvėms	
2.3.2. Dėl pažeidimo yra ar gali kilti pavojus fizinių asmenų teisėms ir laisvėms	
2.3.3. Dėl pažeidimo yra ar gali kilti didelis pavojus fizinių asmenų teisėms ir laisvėms	
2.4. Duomenų subjektui ir (ar) TKA padaryta žala (tapatybės vagystė, grėsmė fiziniam saugumui ir emocinei gerovei, žala reputacijai, teisinė atsakomybė, konfidencialumo, saugumo nuostatų pažeidimas ir pan.)	

2.5. Techninės ir (ar) organizacinės duomenų saugumo priemonės:	
2.5.1. Techninės ir (ar) organizacinės priemonės, kurios buvo taikomos asmens duomenims, kurių saugumas buvo pažeistas, siekiant užtikrinti šių duomenų saugumą (aprašoma arba pridedami patvirtinantys dokumentai; išvada dėl tinkamumo)	
2.5.2. Techninės ir (ar) organizacinės saugumo priemonės, kurios įgyvendintos dėl įvykusio pažeidimo, taip pat siekiant, kad pažeidimas nepasikartotų ir būtų sumažintos pasekmės duomenų subjektui (aprašoma arba pridedami patvirtinantys dokumentai)	
2.6. Pažeidimo pakartotinumas:	
2.6.1. Tokio pobūdžio pažeidimas įvyko pirmą kartą	
2.6.2. Pakartotinis tokio pobūdžio pažeidimas	
2.7. Įvertinus visas aplinkybes nustatytas rizikos tikimybės lygis	
3. Pranešimų pateikimas	
3.1. Pranešimas duomenų subjektui apie įvykusį pažeidimą:	
3.1.1. Pranešimo data, būdas, trumpas turinio aprašymas, informuotų duomenų subjektų skaičius	
3.1.2. Priežastys, dėl kurių nepranešta duomenų subjektui:	
3.1.2.1. Nekyla didelis pavojus duomenų subjektų teisėms ir laisvėms	
3.1.2.2. Įgyvendintos tinkamos techninės ir organizacinės apsaugos priemonės ir tos priemonės taikytos asmens duomenims, kuriems asmens duomenų saugumo pažeidimas turėjo poveikio, visų pirma tos priemonės, kuriomis užtikrinama, kad asmeniui, neturinčiam leidimo susipažinti su asmens duomenimis, jie būtų nesuprantami, pavyzdžiui, šifravimo priemonės	
3.1.2.3. Imtasi priemonių, kuriomis užtikrinama, kad nebegalėtų kilti didelis pavojus duomenų subjektų teisėms ir laisvėms	
3.1.2.4. Pranešimas pareikalautų neproporcingai daug pastangų ir apie tai viešai paskelbta (arba taikyta panaši priemonė) (nurodoma, kada ir kur paskelbta informacija viešai arba, jei taikyta kita priemonė, nurodoma, kokia ir kada taikyta)	
3.2. Pranešimas Inspekcijai apie pažeidimą:	
3.2.1. Pranešimo data, numeris	
3.2.2. Priežastys, dėl kurių nepranešta Inspekcijai	

3.2.3. Pranešimo Inspekcijai vėlavimo priežastys	
3.3. Pranešimas valstybės institucijoms, įgaliotoms atlikti ikiteisminį tyrimą, apie asmens duomenų saugumo pažeidimą, galimai turintį nusikalstamos veikos požymių (jei taikoma) (rašto data, numeris; adresatas)	
3.4. Pranešimas Nacionaliniam kibernetinio saugumo centrui apie TKA valdomose ir (ar) tvarkomuose registruose, ryšių ir informacinėse sistemose įvykusį kibernetinį incidentą ir taikytas kibernetinių incidentų valdymo priemones (jei taikoma) (rašto data, numeris)	
4. Pasiūlymai siekiant išvengti tokio pobūdžio pažeidimų pasikartojimo	
4.1. Techninės priemonės, kurios siūlomos įgyvendinti dėl įvykusio pažeidimo, taip pat siekiant, kad pažeidimas nepasikartotų ir būtų sumažintos pasekmės duomenų subjektui (aprašoma arba pridedami patvirtinantys dokumentai)	
4.2. Organizacinės priemonės, kurios siūlomos įgyvendinti dėl įvykusio pažeidimo, taip pat siekiant, kad pažeidimas nepasikartotų ir būtų sumažintos pasekmės duomenų subjektui (aprašoma arba pridedami patvirtinantys dokumentai)	

_____ _____

(pareigos) *(vardas ir pavardė)*

2 priedas

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ REGISTRAVIMO ŽURNALAS

Pažeidimo nustatymo data, laikas, vieta	Pažeidimo aplinkybės, pažeidimo pasekmės,	Priemonės, kurių buvo imtasi pažeidimui pašalinti	Pranešėjo vardas, pavardė, pareigos	Parašas