PATVIRTINTA
Viešosios įstaigos Vilkpėdės ligoninės direktoriaus
2021 m. kovo 1 d. įsakymu Nr. (1.1.)V-17

VIEŠOSIOS ĮSTAIGOS VILKPĖDĖS LIGONINĖS ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ POLITIKA

I SKYRIUS BENDROSIOS NUOSTATOS

1. VšĮ Vilkpėdės ligoninė (toliau – Įstaiga) asmens duomenų saugumo pažeidimų politikos (toliau – Politika) tikslas – nustatyti asmens duomenų saugumo pažeidimo Įstaigoje tyrimo, pranešimų apie juos ir dokumentavimo tvarką, siekiant įgyvendinti atskaitomybės principą.

2. Įgyvendinant duomenų subjekto teises 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 – Reglamentas) ir Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu.

3. Ši Politika visais atvejais taikoma Įstaigos vykdomoje veikloje ir yra privaloma visiems Įstaigos darbuotojams.

4. Šioje Politikoje vartojamos sąvokos:

4.1. **Asmens duomenys** – bet kokia informacija apie fizinį asmenį, kurio tapatybė nustatyta arba kurio tapatybę galima nustatyti (duomenų subjektas); fizinis asmuo, kurio tapatybę galima nustatyti, yra asmuo, kurio tapatybę tiesiogiai arba netiesiogiai galima nustatyti, visų pirma pagal identifikatorių, kaip antai vardą ir pavardę, asmens identifikavimo numerį, buvimo vietos duomenis ir interneto identifikatorių arba pagal vieną ar kelis to fizinio asmens fizinės, fiziologinės, genetinės, psichinės, ekonominės, kultūrinės ar socialinės tapatybės požymius.

4.2. **Saugumo pažeidimas** - asmens 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.

4.3. **Duomenų subjektas -** fizinis asmuo, kurio asmens duomenis Įstaiga tvarko.

4.4. **Saugumo pranešimas -** informacinis pranešimas priežiūros institucijai – Valstybinei duomenų apsaugos inspekcijai, o tam tikrais atvejais ir duomenų subjektams, kuriame pateikta su saugumo pažeidimu susijusi informacija.

4.5. **Asmens duomenų sunaikinimas -** tokie atvejai, kai asmens duomenys nebeegzistuoja arba nebeegzistuoja tokioje formoje, kuri gali būti skirta bet kokiam Duomenų valdytojo naudojimui.

4.6. **Asmens duomenų sugadinimas -** tokie atvejai, kai asmens duomenys buvo pakeisti, sugadinti arba yra išnykęs jų vientisumas.

4.7. **Asmens duomenų praradimas -** tokie atvejai, kai asmens duomenys vis tiek gali egzistuoti, tačiau Duomenų valdytojas yra praradęs šių duomenų valdymą ir kontrolę arba prieigą prie jų.

4.8. **Duomenų tvarkymas -** bet kokia automatizuotomis arba neautomatizuotomis priemonėmis su asmens duomenimis ar asmens duomenų rinkiniais atliekama operacija ar operacijų seka, kaip antai rinkimas, įrašymas, rūšiavimas, sisteminimas, saugojimas, adaptavimas ar keitimas, išgava, susipažinimas, naudojimas, atskleidimas persiunčiant, platinant ar kitu būdu sudarant galimybę jais

naudotis, taip pat sugretinimas ar sujungimas su kitais duomenimis, apribojimas, ištrynimas arba sunaikinimas.

4.9. **Duomenų tvarkytojas -** fizinis arba juridinis asmuo, valdžios institucija, agentūra ar kita įstaiga, kuri Duomenų valdytojo vardu tvarko asmens duomenis.

4.10. **Priežiūros institucija -** Valstybinė duomenų apsaugos inspekcija (VDAI).

II SKYRIUS
ASMENS DUOMENŲ SAUGUMO PAŽEIDIMO REAGAVIMO KOMANDA

5. Įstaigos asmens duomenų saugumo pažeidimo reagavimo komanda (toliau - Komanda) sudaroma iš Įstaigos darbuotojų ir/ar įgaliotų trečiųjų šalių asmenų, kurie yra kvalifikuoti ir patyrę įvairių sričių specialistai. Komandos tikslas - nedelsiant, veiksmingai ir kvalifikuotai reaguoti į visus galimus Įstaigai ar Duomenų subjektams įtakos turinčius asmens duomenų saugumo pažeidimus.

6. Įstaigos vadovo įsakymu suformuojama asmens duomenų saugumo pažeidimo reagavimo komanda.

7. Komanda sudaroma nepriklausomai nuo to, ar įvyko asmens duomenų saugumo pažeidimas, ir veikia „ad hoc“ principu, tai yra – reaguoja į bet kokį galimai įvykusį arba įvykusį asmens duomenų saugumo pažeidimą. Komanda gali veikti tiek toje pačioje vietovėje fiziškai, tiek ir virtualiai (jos nariams esant skirtingose vietovėse).

8. Esant poreikiui, vykdydami savo pareigas Komandos nariai, Įstaigos vadovui pritarus, gali pasitelkti specialistus iš išorės tam, kad būtų sustabdytas asmens duomenų saugumo pažeidimas ir arba sumažinta ar pašalinta jo padaryta žala.

9. Vienu metu Komanda gali valdyti daugiau nei vieną galimą asmens duomenų saugumo pažeidimą, tačiau vykstant keliems incidentams vienu metu Įstaigos vadovas turi apsvarstyti galimybę laikinai išplėsti Komandą pasitelkiant būtinus įvairių sričių specialistus iš Įstaigos darbuotojų ar trečiųjų šalių.

10. Komandos sudėtis ir jos narių duomenys kontaktams paskelbiami Įstaigos vidiniais komunikacijos kanalais.

III SKYRIUS
DUOMENŲ SAUGUMO PAŽEIDIMŲ KLASIFIKAVIMAS

11.Galimi pažeidimo tipai:

11.1. konfidencialumo pažeidimas – kai yra be leidimo ar neteisėtai atskleidžiami asmens duomenys arba gaunama prieiga prie jų;

11.2. prieinamumo pažeidimas – kai netyčia arba neteisėtai prarandama prieiga prie asmens duomenų arba sunaikinami asmens duomenys;

11.3. vientisumo pažeidimas – kai asmens duomenys pakeičiami be leidimo ar netyčia.

12. Priklausomai nuo aplinkybių, Pažeidimas tuo pat metu gali sietis su asmens duomenų konfidencialumu, prieinamumu ir vientisumu, taip pat su kuriuo nors jų deriniu.

IV SKYRIUS
ASMENS DUOMENŲ SAUGUMO PAŽEIDIMO VALDYMAS

13. Asmens duomenų saugumo pažeidimo valdymo stadijos:

13.1. Asmens duomenų saugumo pažeidimo identifikavimas. Asmens duomenų saugumo pažeidimui nesant akivaizdžiam, būtina atlikti pradinį vertinimą.

13.2. Jei nustatoma, kad Asmens duomenų saugumo pažeidimas įvyko arba jo grėsmė reali, atliekamas rizikos ir poveikio duomenų subjektams vertinimas.

13.3. Asmens duomenų saugumo pažeidimo rizikos vertinimą bei rekomenduojamą veiksmų planą pasirašytinai tvirtina Įstaigos vadovas.

13.4. Jei būtina apie Asmens duomenų saugumo pažeidimą pranešama Priežiūros institucijai ir/ar Duomenų subjektams.

13.5. Atliekami Asmens duomenų saugumo pažeidimo lokalizavimo ir sustabdymo veiksmai (Apribojimo stadija).

13.6. Atliekami Asmens duomenų saugumo pažeidimo pasekmių likvidavimo veiksmai.

13.7. Atliekama Asmens duomenų saugumo pažeidimo analizė.

V SKYRIUS
ASMENS DUOMENŲ SAUGUMO PAŽEIDIMO INDENTIFIKAVIMAS

14. Asmens duomenų saugumo pažeidimo indentifikavimas vyksta:

14.1. Įstaigos darbuotojas sužinojęs apie galimą Asmens duomenų saugumo pažeidimą privalo nedelsdamas apie tai informuoti savo tiesioginį vadovą ir Bendrųjų reikalų skyriaus vedėją ir Ūkio skyriaus vedėją.

14.2. Komanda atlieka pradinį vertinimą ir nusprendžia, ar Asmens duomenų saugumo pažeidimas tikrai įvyko. Šis vertinimas gali apimti šiuos pagrindinius veiksmus:

14.2.1. asmens duomenų, kurie galėjo būti ar buvo paveikti Asmens duomenų saugumo pažeidimo, identifikavimas;

14.2.2. informacinės sistemos, kurioms gali kilti arba yra kilęs pavojus;

14.2.3. tikėtina Asmens duomenų saugumo pažeidimo trukmė (kada prasidėjo ir kada buvo sustabdytas pažeidimas arba kaip skubiai būtų galima jį sustabdyti);

14.2.4. paveikti Duomenų subjektai ir poveikio jiems mastas;

14.2.5. pradiniai Asmens duomenų saugumo pažeidimo pasekmių (žalos) požymiai (prieigos prie duomenų praradimas, nustatyti neteisėti duomenų pakeitimai, rasti paviešinti duomenys ir pan.).

14.3. Atlikusi pradinį vertinimą Komanda gali padaryti išvadą, kad:

14.3.1. Asmens duomenų saugumo pažeidimo nebuvo, todėl Komanda šią išvadą dokumentuoja ir procedūrą užbaigia arba

14.3.2. Asmens duomenų saugumo pažeidimas įvyko, todėl priklausomai nuo pažeidimo apimties bei faktinio ar galimo poveikio duomenų subjektams imasi tolimesnio reagavimo į Asmens duomenų saugumo pažeidimą kaip nustatyta šioje Politikoje.

14.4. Atliekant pažeidimo identifikavimą išsaugomi esamos situacijos įrodymai.

14.5. Nustačius, kad Asmens duomenų saugumo pažeidimas įvyko:

14.5.1. pradedamas skaičiuoti 72 val. terminas dėl pranešimo Priežiūros institucijai apie Duomenų saugumo pažeidimą, jei apie incidentą pranešti būtina remiantis galiojančiais teisės aktais ir šia Politika;

14.5.2. pradedamos reagavimo į Asmens duomenų saugumo pažeidimą procedūros;

14.5.3. imamasi veiksmų Asmens duomenų saugumo pažeidimui sustabdyti (pašalinti), jo padarytai žalai sumažinti ar panaikinti bei imamasi veiksmų, kad šis pažeidimas ateityje nepasikartotų.

VI SKYRIUS
RIZIKOS IR POVEIKIO DUOMENŲ SUBJEKTAMS VERTINIMAS

15. Asmens duomenų saugumo pažeidimo rizikos vertinimas yra būtinas, jeigu yra bent viena iš šių aplinkybių:

15.1. Prarasti arba gali būti prarasti daugiau nei vieno Duomenų subjekto Asmens duomenys;

15.2. Asmens duomenų saugumo pažeidimas tikėtinai gali kelti didelį pavojų fizinių asmenų teisėms ir laisvėms dėl prarastų duomenų turinio;

15.3. Asmens duomenų saugumo pažeidimu daromas poveikis dideliam Duomenų subjektų skaičiui;

15.4. Dėl Asmens duomenų saugumo pažeidimo galimas reikšmingas poveikis darbuotojams ir (ar) Duomenų subjektams.

16. Vertinant Asmens duomenų saugumo pažeidimo pasekmių riziką, turi būti atsižvelgiama į konkrečias Asmens duomenų saugumo pažeidimo aplinkybes, pavojaus Duomenų subjekto teisėms ir laisvėms atsiradimo tikimybę. Už pasekmių rizikos vertinimo atlikimą yra atsakinga Komanda. Rizika turėtų būti vertinama objektyviai atsižvelgiant į šiuos kriterijus:

16.1. Asmens duomenų saugumo pažeidimo tipą;

16.2. Asmens duomenų kategorijas;

16.3. Asmens duomenų apimtį;

16.4. sudėtingumą identifikuoti asmenį (kaip lengvai identifikuojamas fizinis asmuo, pavyzdžiui, jeigu duomenys buvo nuasmeninti ar užšifruoti, rizika sumažėja);

16.5. pasekmių Duomenų subjektams sunkumą;

16.6. ar Asmens duomenys susiję su ypatingais asmenimis ar specialiomis jų savybėmis;

16.7. paveiktų (ar nukentėjusių) Duomenų subjektų skaičių;

16.8. Asmens duomenų tvarkymo pobūdį;

16.9. pasekmių Duomenų subjektams pastovumą;

16.10. kai yra konfidencialumo pažeidimas, asmenų, kurie neteisėtai pasinaudojo duomenis, ketinimai.

17. Atlikus Asmens duomenų saugumo pažeidimo pasekmių rizikos įvertinimą, Komanda gali padaryti vieną iš šių išvadų:

17.1. žema rizikos tikimybė – nėra realaus pavojaus (grėsmės) fizinių asmenų teisėms ir laisvėms;

17.2. vidutinė rizikos tikimybė – mažai tikėtina, kad kiltų pavojus (grėsmė) fizinių asmenų teisėms ir laisvėms;

17.3. didelė (aukšta) rizikos tikimybė – egzistuoja didelė rizika dėl grėsmės (pavojaus) fizinių asmenų teisėms ir laisvėms.

18. Vertinant riziką, turėtų būti laikoma, kad pavojų keliančiu laikytinas toks pažeidimas, dėl kurio Duomenų subjektas galėtų patirti kūno sužalojimą, materialinę ar nematerialinę žalą.

19. Atlikto Asmens duomenų saugumo pažeidimo pasekmių rizikos įvertinimo išvadą dėl Asmens duomenų saugumo pažeidimo buvimo kartu su rekomendacijomis dėl tolimesnių veiksmų, Komanda pateikia raštu Įstaigos vadovui, kurią jis ją patvirtina pasirašydamas ir priima sprendimą dėl tolimesnių veiksmų. Visus tolimesnius veiksmus, susijusius su Asmens duomenų saugumo pažeidimo valdymu, atlieka Komanda.

VII SKYRIUS
SAUGUMO PRANEŠIMAS

20. Priklausomai nuo Asmens duomenų saugumo pažeidimo identifikavimo ir jo pasekmių fizinių asmenų teisėms ir laisvėms rizikos įvertinimo toliau atliekama arba ne pranešimo procedūra:

20.1. jeigu nustatoma, kad Asmens duomenų saugumo pažeidimas tikrai buvo ir išvada „žema rizikos tikimybė“ pranešimas nėra teikiamas;

20.2. jeigu nustatoma, kad Asmens duomenų saugumo pažeidimas buvo ir išvada „vidutinė rizikos tikimybė“ turi būti pateiktas pranešimas Priežiūros institucijai;

20.3. jeigu nustatoma, kad Asmens duomenų saugumo pažeidimas buvo ir išvada „didelė (aukšta) rizikos tikimybė“ turi būti pateiktas pranešimas Priežiūros institucijai ir Duomenų subjektams, kurių Asmens duomenys buvo paveikti Asmens duomenų saugumo pažeidimo;

20.4. jeigu nustatoma, kad Asmens duomenų saugumo pažeidimas buvo, tik sudėtinga nustatyti rizikos tikimybė yra žema ar vidutinė, tokiu atveju turi būti pateiktas pranešimas Priežiūros institucijai.

21. Komanda, visų pirma, imasi visų tinkamų techninių ir organizacinių priemonių, kad Asmens duomenų saugumo pažeidimas būtų išsamiai ištirtas ir pašalintas (sustabdytas, ištaisytas) bei ateityje nepasikartotų ir tuomet pateikia pranešimą Priežiūros institucijai.

22. Pranešimo Priežiūros institucijai ir Duomenų subjektui rekomenduojama naudoti forma yra patvirtinta kaip Asmens duomenų saugumo pažeidimų politikos 1 Priedas.

23. Pranešimas Priežiūros institucijai, turi būti pateiktas ne vėliau kaip per 72 valandas nuo to momento, kai įsitikinta, kad Asmens duomenų saugumo pažeidimas įvyko. Jeigu Priežiūros institucija informuojama vėliau nei per 72 valandas, būtina nurodyti priežastis, dėl kurių vėluojama.

24. Jeigu, priklausomai nuo Asmens duomenų saugumo pažeidimo pobūdžio, nėra galima nurodyti ir (ar) pateikti visų aplinkybių, susijusių su pažeidimu per 72 valandas nuo sužinojimo apie pažeidimą dėl objektyvių galimybių, Priežiūros institucija informuojama etapais, teikiant dalinius pranešimus, pirmąjį pranešimą pateikiant per 72 valandų terminą, ir vėliau tokį pranešimą atnaujinti (pateikti papildytą). Esant galimybei, apie numatomą informacijos teikimą etapais nurodoma teikiant pirminį pranešimą.

25. Jeigu po pranešimo Priežiūros institucijai pateikimo yra nustatoma, kad galimas Asmens duomenų saugumo pažeidimas (incidentas) buvo sustabdytas ir faktiškai neįvyko jokio pažeidimo, apie tai informuojama Priežiūros institucija ir dokumentuojama taip kaip numatoma šioje Politikoje.

26. Tuo atveju, jeigu Įstaiga Asmens duomenų tvarkymui pasitelkė Duomenų tvarkytoją, šis, sužinojęs ar pats nustatęs galimą Asmens duomenų saugumo pažeidimą, turi būti įpareigotas ne vėliau kaip per 24 valandas nuo pažeidimo sužinojimo ar nustatymo momento informuoti apie tai Duomenų valdytoją, pateikiant pranešimą Įstaigai raštu ar elektroninėmis priemonėmis.

VIII SKYRIUS
PRANEŠIMAS DUOMENŲ SUBJEKTUI

27. Nustačius, kad Pažeidimas buvo ir, kad yra didelė rizika fizinių asmenų teisėms ir laisvėms, per 72 valandas apie tai turi būti pranešta duomenų subjektui, kurio teisėms ir laisvėms dėl šio Pažeidimo gali kilti didelis pavojus. Politikos pakeitimus ir (ar) papildymus įsakymu tvirtina Įstaigos vadovas.

28. Pranešime duomenų subjektui aiškia ir paprasta kalba pateikiama:

28.1. pažeidimo pobūdžio aprašymas;

28.2. Duomenų apsaugos pareigūno asmens vardas, pavardė ir kontaktiniai duomenys.

28.3. tikėtinų Pažeidimo pasekmių aprašymas;

28.4. priemonių, kurių ėmėsi arba pasiūlė imtis duomenų valdytojas, kad būtų pašalintas Pažeidimas, įskaitant priemonių galimoms neigiamoms jo pasekmėms sumažinti, aprašymas;

28.5. kita reikšminga informacija, susijusi su Pažeidimu.

29. Duomenų subjektai apie Pažeidimą informuojami tiesiogiai, siunčiant jiems pranešimą el. paštu, siunčiant žinutę telefonu, siunčiant paštu.

30. Esant Pažeidimui, pranešimo duomenų subjektui teikti nereikia:

30.1. jeigu yra įgyvendintos tinkamas techninės ir organizacinės apsaugos priemonės ir tos priemonės taikytos asmens duomenims, kuriems Pažeidimas turėjo poveikio;

30.2. iš karto po Pažeidimo imtasi priemonių, kuriomis užtikrinama, kad nebegali kilti didelis pavojus asmenų teisėms ir laisvėms.

IX SKYRIUS
ATSAKOMYBĖ

31. Įstaigos darbuotojai ir visi Įstaigos įgalioti asmenys, kurie gali turėti prieigą prie Įstaigoje tvarkomų Asmens duomenų, atsako už šios Politikos nuostatų laikymąsi ir gali būti traukiami atsakomybėn už jų pažeidimą teisės aktų nustatyta tvarka.

32. Visi klausimai, susiję su Asmens duomenų saugumo pažeidimais, kurių neapima ši Politika, turi būti adresuojami Komandai arba už asmens duomenų apsaugą atsakingam darbuotojui (Duomenų apsaugos pareigūnui).

X SKYRIUS
ASMENS DUOMENŲ SAUGUMO PAŽEIDIMO APRIBOJIMAS, LIKVIDAVIMAS, ATKŪRIMAS IR ANALIZĖ

33. Visi klausimai, susiję su Asmens duomenų saugumo pažeidimais, kurių neapima ši Politika, turi būti adresuojami Komandai arba už asmens duomenų apsaugą atsakingam darbuotojui (Duomenų apsaugos pareigūnui):

33.1. duomenų ištrynimas nuotoliniu būdu iš pamesto ar pavogto įrenginio;

33.2. paveikto įrenginio ar sistemos išjungimas iš Įstaigos informacinių sistemų ar kitoks izoliavimas;

33.3. kuo skubesnis kreipimasis į asmenį, kuriam per klaidą buvo išsiųsti Įstaigoje tvarkomi Asmens duomenys, su prašymu neatidarinėti atsiųstų duomenų ir juos ištrinti be galimybės atkurti;

33.4. atskleisto tretiesiems asmenims prisijungimo prie duomenų bazės slaptažodžio pakeitimas;

33.5. paskyros, kurią buvo gauta neteisėta prieiga blokavimas, ir pan.

34. Apribojimo stadijoje reikia imtis priemonių, kad būtų surinkti kiek įmanoma tikslesni duomenys bei įrodymai apie įvykusį Asmens duomenų saugumo pažeidimą.

35. Įsitikinus, kad Asmens duomenų saugumo pažeidimas sustabdytas, būtina pereiti prie likvidavimo stadijos (atkurti prarastus duomenis iš turimos atsarginės kopijos, jeigu saugu, iš naujo įjungti paveiktas sistemas pagal galimybes atkuriant jų pirminį funkcionalumą, ir pan.).

36. Likvidavimo stadijoje, veiksmai, skirti atitaisyti žalą, sukeltą Asmens duomenų saugumo pažeidimo, nukreipiami ne vien į esamo pažeidimo priežasties pašalinimui, bet ir panašių Asmens duomenų saugumo pažeidimų pasikartojimo užkardymui ir prevencijai.

37. Asmens duomenų saugumo pažeidimo analizės stadijoje, analizuojama Asmens duomenų saugumo pažeidimo eiga, jo atsiradimo priežastys, numatomi būtini veiksmai tam, kad būtų atsižvelgta į trūkumus ir duomenų tvarkymo silpnąsias vietas, kurios tapo Asmens duomenų saugumo pažeidimo priežastimi.

XI SKYRIUS
ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ DOKUMENTAVIMAS

38. Visi Pažeidimai, nepriklausomai nuo to, ar apie juos buvo pranešta Priežiūros institucijai, ar ne, registruojami Asmens duomenų saugumo pažeidimų žurnale (toliau – Žurnalas) 2 Priedas.

39. Informacija apie Pažeidimą į Žurnalą įvedama nedelsiant, kai tik nustatomas Pažeidimo faktas ir įvertinama rizika (per 5 darbo dienas). Žurnale esanti informacija papildoma ir (ar) koreguojama.

40. Žurnale nurodomi:

40.1. visi su Pažeidimu susiję faktai – Pažeidimo priežastis, kas įvyko ir kokie asmens duomenys pažeisti;

40.2. Pažeidimo poveikis ir pasekmės;

40.3. taisomieji veiksmai (techninės priemonės), kurių buvo imtasi;

40.4. priežastys dėl su Pažeidimu susijusių sprendimų priėmimo;

40.5. pranešimo Priežiūros institucijai pateikimo vėlavimo priežastys (jeigu Pranešimą vėluojama pateikti ar Pranešimas teikiamas etapais);

40.6. informacija, susijusi su pranešimu duomenų subjektui;

40.7. kita reikšminga informacija susijusi su Pažeidimu.

41. Žurnalas tvarkomas raštu, įskaitant elektroninę formą, ir saugomas pagal patvirtintą dokumentų saugojimo tvarką. Už Asmens duomenų saugumo pažeidimų žurnalo užpildymą yra atsakingas už asmens duomenų apsaugą atsakingas darbuotojas.

42. Asmens duomenų saugumo pažeidimų žurnalo įrašus privaloma saugoti 5 (penkerius) metus.

XII SKYRIUS
BAIGIAMOSIOS NUOSTATOS

43. Įstaiga ne rečiau kaip kartą per 1 metus, atlieka pažeidimų analizę ir sprendžia kokių reiktų imtis prevencijos priemonių.

44. Politikos laikymosi kontrolę atlieka direktoriaus įsakymu paskirtas darbuotojas.

45. Darbuotojai nesilaikantys ar pažeidę Politikos reikalavimus atsako teisės aktų nustatyta tvarka.

Viešoji įstaiga Vilkpėdės ligoninės
asmens duomenų saugumo
pažeidimų politika
1 priedas

Viešoji įstaiga Vilkpėdės ligoninė, juridinio asmens kodas 124245322, Vilkpėdės g. 3, LT-03151 Vilnius

Valstybinei duomenų apsaugos inspekcijai

PRANEŠIMAS
APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ

_____Nr. _____
(data) (rašto numeris)

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
- ☐ Internetinė svetainė
- ☐ Debesų kompiuterijos paslaugos
- ☐ Nešiojami / mobilus įrenginiai
- ☐ Neautomatiniu būdu susistemintos bylos (archyvas)
- ☐ Kita _____

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)

1.4. Apytikslis duomenų subjektų, kurių asmens duomenų saugumas pažeistas, skaičius:
_____

1.5. Duomenų subjektų, kurių asmens duomenų saugumas pažeistas, kategorijos (atskiriamos pagal jai būdingą požymį):
_____
_____

1.6. Asmens duomenų, kurių saugumas pažeistas, kategorijos (pažymėti tinkamą (-as):

☐ Asmens tapatybę patvirtinantys asmens duomenys (vardas, pavardė, amžius, gimimo data, lytis ir kt.):
_____
_____

☐ Specialių kategorijų asmens duomenys (duomenys, atskleidžiantys rasinę ar etninę kilmę, politines pažiūras, religinius ar filosofinius įsitikinimus, ar narystę profesinėse sąjungose, genetiniai duomenys, biometriniai duomenys, sveikatos duomenys, duomenys apie lytinį gyvenimą ir lytinę orientaciją):
_____
_____
_____

☐ Duomenys apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas:
_____

☐Prisijungimo duomenys ir (ar) asmens identifikaciniai numeriai (pavyzdžiui, asmens kodas, mokėtojo kodas, slaptažodžiai):
_____

☐Kiti:
_____

☐Nežinomi (pranešimo teikimo metu)

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

1.8. Kita duomenų valdytojo nuomone reikšminga informacija apie asmens duomenų saugumo pažeidimą:
_____
_____
_____
_____
_____

2. Galimos asmens duomenų saugumo pažeidimo pasekmės

2.1. Konfidencialumo praradimo atveju:

☐Asmens duomenų išplitimas labiau nei yra būtina ir duomenų subjekto kontrolės praradimas savo asmens duomenų atžvilgiu (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 tikslais, asmens tapatybės pasisavinimo tikslu, informacijos panaudojimo prieš asmenį tikslu)
☐Kita
_____
_____
_____
_____
_____

2.2. 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
_____
_____
_____
_____
_____

2.3. Duomenų prieinamumo praradimo atveju:

☐Dėl asmens duomenų trūkumo negalima teikti paslaugų (pavyzdžiui, administracinių procesų sutrikdymas, dėl ko negalima prieiti, 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, tam tikra informacija iš mokesčių deklaracijos išnyko, dėl ko negalima tinkamai apskaičiuoti mokesčių ir pan.)
☐Kita
_____
_____
_____
_____
_____

2.4. Kita:
_____
_____
_____
_____
_____

3. Priemonės, kurių imtasi siekiant pašalinti pažeidimą ar sumažinti jo pasekmes

3.1. Taikytos priemonės siekiant sumažinti poveikį duomenų subjektams:
_____
_____
_____
_____
_____

3.2. Taikytos priemonės siekiant pašalinti asmens duomenų saugumo pažeidimą:
_____
_____
_____
_____

3.3. Taikytos priemonės siekiant, kad pažeidimas nepasikartotų:
_____
_____
_____
_____

3.4. Kita:
_____
_____

4. Siūlomos priemonės sumažinti asmens duomenų saugumo pažeidimo pasekmėms

_____
_____
_____
_____
_____
_____

5. Duomenų subjektų informavimas apie asmens duomenų saugumo pažeidimą

5.1. Duomenys apie informavimo faktą:

☐Taip, duomenų subjektai informuoti (nurodoma data)_____
☐Ne, bet jie bus informuoti (nurodoma data)_____
☐Ne

5.2. Duomenų subjektų, kurių asmens duomenų saugumas pažeistas, neinformavimo priežastys:

☐Ne, nes nekyla didelis pavojus duomenų subjektų teisėms ir laisvėms (nurodoma kodėl) _____
_____
_____

☐Ne, nes įgyvendintos tinkamos techninės ir organizacinės priemonės, užtikrinančios, kad asmeniui, neturinčiam leidimo susipažinti su asmens duomenimis, jie būtų nesuprantami (nurodomos kokios) _____
_____
_____

☐Ne, nes įgyvendintos tinkamos techninės ir organizacinės priemonės, užtikrinančios, kad nekiltų didelis pavojus duomenų subjektų teisėms ir laisvėms (nurodomos kokios) _____
_____
_____

☐Ne, nes tai 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)
_____

☐Ne, nes dar neidentifikuoti duomenų subjektai, kurių asmens duomenų saugumas pažeistas

5.3. Informacija, kuri buvo pateikta duomenų subjektams (gali būti pridėtas pranešimo duomenų subjektui kopija):

_____
_____
_____
_____
_____
_____

5.4. Būdas, kokiu duomenų subjektai buvo informuoti:

☐Paštu
☐Elektroniniu paštu
☐Kitu būdu _____

5.5. Informuotų duomenų subjektų skaičius _____

6. Asmuo galintis suteikti daugiau informacijos apie asmens duomenų saugumo pažeidimą (duomenų apsaugos pareigūnas ar kitas kontaktinis asmuo)

6.1. Vardas ir pavardė_____

6.2. Telefono ryšio numeris _____

6.3. Elektroninio pašto adresas _____

6.4. Pareigos _____

6.5. Darbovietės pavadinimas ir adresas_____

_____

7. Pranešimo pateikimo Valstybinei duomenų apsaugos inspekcijai pateikimo vėlavimo priežastys

_____
_____
_____
_____
_____
_____

8. Kita reikšminga informacija

_____
_____
_____
_____
_____
_____
_____

_____ _____ _____

(pareigos) (parašas) (vardas, pavardė)

Viešosios įstaigos Vilkpėdės ligoninės
asmens duomenų saugumo
pažeidimų politika
2 priedas

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ REGISTRAVIMO ŽURNALAS

Eil. Nr.	Pažeidimo priežastis (kas įvyko)	Kokie asmens duomenys pažeisti	Kada pažeidimas įvyko (data ir laikas)	Pažeidimo poveikis ir pasekmės	Taisomieji veiksmai	Priežastys dėl su pažeidimu susijusių sprendimų priėmimo	Pranešimo VDAI pateikimas	Informacija, susijusi su pranešimu duomenų subjektui	Kita reikšminga informacija susijusi su pažeidimu	Pastabos
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*

DETALŪS METADUOMENYS	
Dokumento sudarytojas (-ai)	Vilkpėdės ligoninė
Dokumento pavadinimas (antraštė)	DĖL VIEŠOSIOS ĮSTAIGOS VILKPĖDĖS LIGONINĖS ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ POLITIKOS PATVIRTINIMO IR ASMENS DUOMENŲ SAUGUMO PAŽEIDIMO REAGAVIMO KOMANDOS SUDARYMO
Dokumento registracijos data ir numeris	2021-03-01 Nr. V-17 (1.1)
Dokumento gavimo data ir dokumento gavimo registracijos numeris	-
Dokumento specifikacijos identifikavimo žymuo	ADOC-V1.0
Parašo paskirtis	Pasirašymas
Parašą sukūrusio asmens vardas, pavardė ir pareigos	Ina Čebotariova Direktorius
Parašo sukūrimo data ir laikas	2021-03-01 16:24
Parašo formatas	Einamojo galiojimo (XAdES-EPES)
Laiko žymoje nurodytas laikas	
Informacija apie sertifikavimo paslaugų teikėją	EID-SK 2016
Sertifikato galiojimo laikas	2019-09-26 11:26 - 2024-09-24 23:59
Informacija apie būdus, naudotus metaduomenų vientisumui užtikrinti	-
Pagrindinio dokumento priedų skaičius	3
Pagrindinio dokumento pridedamų dokumentų skaičius	0
Pridedamo dokumento sudarytojas (-ai)	-
Pridedamo dokumento pavadinimas (antraštė)	Asmens duomenų saugumo pažeidimų politika.docx
Pridedamo dokumento registracijos data ir numeris	-
Pridedamo dokumento sudarytojas (-ai)	-
Pridedamo dokumento pavadinimas (antraštė)	Pranesimas 1 priedas.docx
Pridedamo dokumento registracijos data ir numeris	-
Pridedamo dokumento sudarytojas (-ai)	-
Pridedamo dokumento pavadinimas (antraštė)	REGISTRAVIMO ŽURNALAS 2 priedas.xlsx
Pridedamo dokumento registracijos data ir numeris	-
Programinės įrangos, kuria naudojantis sudarytas elektroninis dokumentas, pavadinimas	Elpako v.20210210.1
Informacija apie elektroninio dokumento ir elektroninio (-ių) parašo (-ų) tikrinimą (tikrinimo data)	
Elektroninio dokumento nuorašo atspausdinimo data ir ją atspausdinęs darbuotojas	2021-03-03 nuorašą suformavo Lina Dringelė
Paieškos nuoroda	-
Papildomi metaduomenys	-