PATVIRTINTA
VšĮ Telšių rajono pirminės sveikatos
priežiūros centro direktoriaus
2019 m. rugpjūčio 2 d.
įsakymu Nr. V-81

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ VALDYMO VŠĮ TELŠIŲ RAJONO PIRMINĖS SVEIKATOS PRIEŽIŪROS CENTRE TVARKOS APRAŠAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Asmens duomenų saugumo pažeidimų valdymo VšĮ Telšių rajono pirminės sveikatos priežiūros centre tvarkos aprašas (toliau – Aprašas) nustato asmens duomenų saugumo pažeidimų nustatymo, tyrimo, fiksavimo VšĮ Telšių rajono pirminės sveikatos priežiūros centre (toliau – Telšių PSPC) tvarką ir pranešimo apie asmens duomenų saugumo pažeidimą turinį ir pateikimo Valstybinei duomenų apsaugos inspekcijai ir duomenų subjektams tvarką.

2. Aprašas taikomas duomenų valdytojai – Telšių PSPC, tvarkančiam asmens duomenis, ir Telšių PSPC pasitelktiems juridiniams ir fiziniams asmenims, tvarkantiems asmens duomenis Telšių PSPC vardu ir pagal jo nurodymus (toliau – duomenų tvarkytojai).

3. Aprašas parengtas vadovaujantis 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) (OL 2016 L 119, p. 1–88) (toliau – Reglamentas (ES) 2016/679) ir atsižvelgiant į Europos Parlamento ir Tarybos direktyvos 95/46/EB 29 straipsnio darbo grupės 2017 m. spalio 3 d. parengtas Pranešimo apie asmens duomenų saugumo pažeidimą gaires pagal Reglamentą 2016/679, Valstybinės duomenų apsaugos inspekcijos Rekomendaciją dėl asmens duomenų saugumo pažeidimų nustatymo, tyrimo, pranešimo apie juos ir dokumentavimo tvarkos.

4. Apraše vartojamos sąvokos apibrėžtos Reglamente (ES) 2016/679.

II SKYRIUS
UŽ ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ VALDYMĄ ATSAKINGI ASMENYS

5. Už asmens duomenų saugumo pažeidimų valdymą Telšių PSPC atsakingas Telšių PSPC direktorius kartu su duomenų apsaugos pareigūnu.

6. Telšių PSPC darbuotojas (toliau – darbuotojas), sužinojęs apie galimą asmens duomenų saugumo pažeidimą (toliau – Pažeidimas) turi nedelsdamas, bet ne vėliau kaip per 2 darbo valandas nuo sužinojimo, apie tai žodžiu, raštu ar elektroninėmis priemonėmis informuoti Telšių PSPC direktorių arba duomenų apsaugos pareigūną.

7. Duomenų tvarkytojai, sužinoję apie asmens duomenų saugumo pažeidimą, nedelsdami, bet ne vėliau kaip per 1 darbo dieną nuo sužinojimo, apie tai raštu praneša Telšių PSPC, pateikdami informaciją, numatytą Reglamento (ES) 2016/679 33 straipsnio 3 dalyje. Duomenų tvarkytojai pateikia Telšių PSPC visą kitą jos prašomą informaciją, susijusią su Pažeidimu ir jo tyrimu, per Telšių PSPC nurodytą terminą. Duomenų tvarkytojų pareigos, susijusios su pranešimu apie duomenų saugumo pažeidimą Telšių PSPC bei su bendradarbiavimu tiriant pažeidimą įtvirtinamos su duomenų tvarkytoju sudaromoje sutartyje.

8. Gavus Aprašo 6 ir 7 punktuose nurodytą informaciją, Telšių PSPC direktorius nedelsiant paveda duomenų apsaugos pareigūnui pradėti Pažeidimo tyrimą.

III SKYRIUS
ASMENS DUOMENŲ SAUGUMO PAŽEIDIMO TYRIMAS

9. Duomenų apsaugos pareigūnas turi imtis visų veiksmų ir priemonių, kad Pažeidimas būtų išsamiai ištirtas bei pašalintas (sustabdytas, ištaisytas) ir ateityje nepasikartotų.

10. Pažeidimo tyrimui ir pašalinimui duomenų apsaugos pareigūnas turi teisę pasitelkti Telšių PSPC darbuotojus, informacinių sistemų ir kompiuterinių darbo vietų priežiūros paslaugų teikėją, jeigu toks yra. Telšių PSPC darbuotojai, informacinių sistemų ir kompiuterinių darbo vietų priežiūros paslaugų teikėjas duomenų apsaugos pareigūno prašymu privalo teikti jam informaciją ir atlikti kitus veiksmus, būtinus pažeidimo tyrimui ir pašalinimui per įmanomai trumpiausią laiką.

11. Sužinojęs apie galimą Pažeidimą ir (ar) gavęs Aprašo 6 ir 7 punktuose nurodytą informaciją, duomenų apsaugos pareigūnas kuo greičiau atlieka pirminį tyrimą, išsiaiškina ir nustato, ar Pažeidimas iš tikrųjų įvyko, Pažeidimo aplinkybes ir priežastis, kokios galimos Pažeidimo pasekmės, kokias organizacines ir technines asmens duomenų saugumo priemones reikia įgyvendinti.

12. Pažeidimo tyrimo metu nustatomas Pažeidimo tipas. Galimi Pažeidimo tipai:

12.1. „Konfidencialumo Pažeidimas“ – kai yra be leidimo ar neteisėtai atskleidžiami asmens duomenys arba gaunama prieiga prie jų;

12.2. „Prieinamumo Pažeidimas“ – kai netyčia arba neteisėtai prarandama prieiga prie asmens duomenų arba asmens duomenys sunaikinami;

12.3. „Vientisumo Pažeidimas“ – kai asmens duomenys pakeičiami be leidimo ar netyčia.

13. Priklausomai nuo aplinkybių, Pažeidimas tuo pat metu gali būti priskiriamas keliems Aprašo 12 punkte nurodytiems tipams.

14. Duomenų apsaugos pareigūnas, atsižvelgdamas į konkretaus Pažeidimo tipą ir aplinkybes, nedelsiant imasi veiksmų Pažeidimui sustabdyti ir užkirsti kelią galimoms neigiamoms pasekmėms. Kiekvienu konkrečiu Pažeidimo atveju, jeigu yra būtina, imamasi šių veiksmų, kad būtų:

14.1. nuotoliniu būdu asmens duomenys ištrinami iš pamesto ar pavogto įrenginio;

14.2. kuo skubiau kreipiamasis į asmenį, kuriam per klaidą buvo išsiųsti asmens duomenys, su prašymu neatidaryti atsiųstų asmens duomenų ir juos ištrinti be galimybės atkurti;

14.3. pakeisti prisijungimo prie duomenų bazės slaptažodį, kuris buvo atskleistas tretiesiems asmenims;

14.4. atkurti prarasti asmens duomenys iš turimos atsarginės kopijos;

14.5. panaikinta prieiga prie asmens duomenų;

14.6. įgyvendintos kitos reikalingos priemonės.

15. Imantis Aprašo 14 punkte nurodytų veiksmų, imamasi atsargumo priemonių tam, kad būtų užkirstas kelias galimoms neigiamoms pasekmėms tiek Telšių PSPC, tiek duomenų subjektui.

16. Pažeidimo tyrimo metu vertinama, kokį pavojų fizinių asmenų teisėms ir laisvėms kelia Pažeidimas.

17. Vertinant Pažeidimo keliamą pavojų, atsižvelgiama į konkrečias Pažeidimo aplinkybes ir šiuos kriterijus:

17.1. Pažeidimo tipą;

17.2. Pažeidimo metu paveiktas asmens duomenų kategorijas ir paveiktų duomenų apimtį;

17.3. Pažeidimo metu paveiktas duomenų subjektų kategorijas ir šių subjektų specifines ypatybes;

17.4. pasekmių rimtumą fiziniams asmenims;

17.5. fizinio asmens identifikavimo galimybę;

17.6. nukentėjusių fizinių asmenų skaičių;

17.7. veiklos, kurią vykdant tvarkomi asmens duomenys, pobūdį;

17.8. kitas reikšmingas aplinkybes.

18. Vertinant Pažeidimą, laikoma, kad Pažeidimas, galintis kelti pavojų fizinių asmenų teisėms ir laisvėms, yra toks, dėl kurio, laiku nesiėmus tinkamų priemonių, fizinis asmuo gali patirti kūno sužalojimą, materialinę ar nematerialinę žalą (pvz., prarasti savo asmens duomenų kontrolę, patirti teisių apribojimą, diskriminaciją, gali būti pavogta ar suklastota jo asmens tapatybė, jam padaryta finansinių nuostolių, neleistinai panaikinti pseudonimai, gali būti pakenkta jo reputacijai, prarastas asmens duomenų, kurie saugomi profesine paslaptimi, konfidencialumas arba padaryta kita ekonominė ar socialinė žala).

19. Tyrimo metu, įvertinus visas Pažeidimo aplinkybes, ir nustačius, kad Pažeidimas kelia pavojų fizinių asmenų teisėms ir laisvėms, nustatomas pavojaus rimtumas:

19.1. žemas;

19.2. vidutinis;

19.3. didelis;

19.4. labai didelis.

20. Atliekant Pažeidimo tyrimą išsaugomi esamos situacijos įrodymai bei įrodymai, kokios techninės ir organizacinės priemonės buvo pritaikytos.

21. Išvadą dėl Pažeidimo buvimo ir pavojaus fizinių asmenų teisėms ir laisvėms įvertinimo kartu su siūlymu dėl duomenų saugumo priemonių įgyvendinimo duomenų apsaugos pareigūnas, pateikia Telšių PSPC direktoriui, o šis priima sprendimą dėl tolesnių veiksmų, susijusių su Pažeidimu.

IV SKYRIUS
PRANEŠIMAS PRIEŽIŪROS INSTITUCIJAI

22. Nustačius, kad Pažeidimas buvo ir kad yra pavojus fizinių asmenų teisėms ir laisvėms, duomenų apsaugos pareigūnas nedelsdamas, bet ne vėliau kaip per 72 val. nuo sužinojimo apie Pažeidimą, Telšių PSPC direktoriaus pavedimu apie Pažeidimą praneša Valstybinei duomenų apsaugos inspekcijai pateikdamas užpildytą Pranešimo apie asmens duomenų saugumo pažeidimą rekomenduojamą formą, patvirtintą Valstybinės duomenų apsaugos inspekcijos direktoriaus 2018 m. gegužės 24 d. įsakymu Nr. 1T-53(1.12.) ,,Dėl Pranešimo apie asmens duomenų saugumo pažeidimą rekomenduojamos formos patvirtinimo“.

23. Jeigu, atsižvelgiant į Pažeidimo pobūdį, yra būtina atlikti išsamesnį tyrimą ir nustatyti visus svarbius faktus, susijusius su Pažeidimu, ir todėl per 72 val. nuo sužinojimo apie Pažeidimą neįmanoma pranešti Valstybinei duomenų apsaugos inspekcijai, duomenų apsaugos pareigūnas informaciją apie Pažeidimą teikia Valstybinei duomenų apsaugos inspekcijai etapais ir nurodo, kodėl visos informacijos neįmanoma pateikti iš karto.

24. Jeigu atlikus tyrimą abejojama, ar yra pavojus asmenų teisėms ir laisvėms ir ar reikia apie Pažeidimą pranešti Valstybinei duomenų apsaugos inspekcijai, sprendimą dėl to priima Telšių PSPC direktorius.

25. Pranešimas apie Pažeidimą Valstybinei duomenų apsaugos inspekcijai pateikiamas Pranešimo apie asmens duomenų saugumo pažeidimą pateikimo Valstybinei duomenų apsaugos inspekcijai tvarkos aprašo, patvirtinto Valstybinės duomenų apsaugos inspekcijos 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.

V SKYRIUS
PRANEŠIMAS DUOMENŲ SUBJEKTUI

26. Nustačius, kad Pažeidimas buvo ir dėl jo gali kilti didelis pavojus fizinių asmenų teisėms ir laisvėms, duomenų apsaugos pareigūnas nedelsdamas apie Pažeidimą praneša duomenų subjektui.

27. Pranešime duomenų subjektui glaustai ir aiškiai pateikiama ši informacija:

27.1. Pažeidimo pobūdžio aprašymas;

27.2. duomenų apsaugos pareigūno ar kito kontaktinio asmens, galinčio suteikti informaciją apie Pažeidimą ir jo valdymo priemones, vardas, pavardė ir kontaktiniai duomenys;

27.3. tikėtinų Pažeidimo pasekmių aprašymas;

27.4. priemonių, kurių ėmėsi arba imsis Telšių PSPC, kad Pažeidimas būtų pašalintas, sumažintos galimos neigiamos jo pasekmės, aprašymas;

27.5. kita reikšminga informacija, susijusi su Pažeidimu, kuri, Telšių PSPC manymu, būtų svarbi duomenų subjektui.

28. Duomenų subjektai apie Pažeidimą informuojami tiesiogiai siunčiant jiems pranešimą el. paštu, SMS, paštu ar kitu būdu. Šis pranešimas siunčiamas atskirai nuo kitos informacijos, įprastai siunčiamos duomenų subjektui.

29. Pranešimas apie Pažeidimą duomenų subjektui neteikiamas, jeigu:

29.1. buvo įgyvendintos tinkamos techninės ir organizacinės apsaugos priemonės ir tos priemonės taikytos asmens duomenims, kuriems Pažeidimas turėjo poveikį;

29.2. iš karto po Pažeidimo Telšių PSPC ėmėsi priemonių užtikrinti, kad nebegalėtų kilti didelis pavojus fizinių asmenų teisėms ir laisvėms;

29.3. jeigu tiesioginio pranešimo duomenų subjektui pateikimas pareikalautų neproporcingai daug pastangų. Tokiu atveju Telšių PSPC informaciją apie įvykusį Pažeidimą paskelbia savo interneto svetainėje aiškiai, duomenų subjektams lengvai prieinamoje vietoje ir (ar) visuomenės informavimo priemonėse.

30. Telšių PSPC išsaugo duomenų subjektams siųsto pranešimo tekstą ir įrodymus, kad toks pranešimas buvo išsiųstas.

VI SKYRIUS
ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ FIKSAVIMAS

31. Pažeidimai, nepriklausomai nuo to, ar apie juos buvo pranešta Valstybinei duomenų apsaugos inspekcijai ir duomenų subjektui, ar ne, registruojami Asmens duomenų saugumo pažeidimų registravimo žurnale (toliau – Žurnalas).

32. Informacija apie Pažeidimą į Žurnalą įrašoma nedelsiant, bet ne vėliau kaip per 5 darbo dienas, kai tik nustatomas Pažeidimo faktas ir įvertinamas pavojus. Prireikus, atsižvelgiant į Pažeidimo tyrimo metu nustatytas papildomas aplinkybes, Žurnale esanti informacija papildoma ir (ar) patikslinama.

33. Žurnale nurodoma:

33.1. Darbuotojo ar kito subjekto, pranešusio apie pažeidimą duomenys – vardas, pavardė, pareigos, kontaktiniai duomenys;

33.2. su Pažeidimu susiję faktai – Pažeidimo nustatymo data, valanda (minučių tikslumu) ir vieta, Pažeidimo padarymo data ir vieta, Pažeidimo tipas, Pažeidimo pradžia, pabaiga, pobūdis, priežastis, kitos aplinkybės, pažeistų asmens duomenų kategorijos, paveiktų duomenų subjektų kategorijos;

33.3. Pažeidimo poveikis ir galimos pasekmės;

33.4. asmens duomenų saugumo priemonių, kurių buvo imtasi, aprašymas;

33.5. informacija, ar apie Pažeidimą buvo pranešta Valstybinei duomenų apsaugos inspekcijai (pranešimo Valstybinei duomenų apsaugos inspekcijai data ir numeris; jeigu pranešimas pateiktas praleidus Aprašo 22 punkte nustatytą terminą, nurodomos to priežastys; jeigu Valstybinei duomenų apsaugos inspekcijai pranešta nebuvo, nurodomos to priežastys);

33.5. informacija, ar apie Pažeidimą buvo pranešta duomenų subjektui (pranešimo duomenų subjektui data ir numeris; jeigu duomenų subjektui pranešta nebuvo, nurodomos to priežastys);

33.6. kita reikšminga informacija, susijusi su Pažeidimu;

33.7. Žurnalą pildžiusio asmens vardas, pavardė, pareigos.

34. Žurnalo forma pateikiama šio Aprašo priede. Žurnalas pildomas *Excel* formatu ir saugomas teisės aktų nustatyta tvarka Telšių PSPC dokumentacijos planuose nurodytą terminą.

35. Už Žurnalo pildymą atsakingas duomenų apsaugos pareigūnas arba kitas Telšių PSPC direktoriaus paskirtas asmuo.

36. Žurnalas pateikiamas Valstybinei duomenų apsaugos inspekcijai jos prašymu.

37. Žurnale esančius įrašus duomenų apsaugos pareigūnas kartu su už asmens duomenų tvarkymą atsakingais asmenimis, periodiškai, ne rečiau kaip kartą per metus, peržiūri ir teikia Telšių PSPC direktoriui pasiūlymus, kokios prevencinės priemonės turėtų būti įgyvendintos papildomai ir kaip reikėtų kontroliuoti šių priemonių įdiegimą, kad ateityje analogiški Pažeidimai nesikartotų.

VII SKYRIUS
BAIGIAMOSIOS NUOSTATOS

38. Jeigu įtariama, kad Pažeidimas turi nusikalstamos veikos požymių, informacija apie galimą nusikalstamą veiką pateikiama valstybės institucijoms, įgaliotoms atlikti ikiteisminį tyrimą.

39. Aprašas peržiūrimas įvykus organizaciniams, sisteminiams ar kitiems pokyčiams arba pasikeitus teisės aktų reikalavimams.

40. Telšių PSPC darbuotojai su Aprašu supažindinami pasirašytinai arba per dokumentų valdymo sistemą.

_____

Asmens duomenų saugumo pažeidimų valdymo
VšĮ Telšių rajono pirminės sveikatos priežiūros centre
tvarkos aprašo priedas

(Asmens duomenų saugumo pažeidimų registravimo žurnalo forma)

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ REGISTRAVIMO ŽURNALAS

Eil. Nr.	Darbuotojo ar kito subjekto, pranešusio apie pažeidimą duomenys (vardas, pavardė, pareigos, kontaktiniai duomenys)	Pažeidimo nustatymo data, valanda (minučių tikslumu) ir vieta	Pažeidimo padarymo data ir vieta	Pažeidimo tipas	Pažeidimo pradžia ir pabaiga, pobūdis, priežastis, kitos aplinkybės	Asmens duomenų, kurių saugumas pažeistas, kategorijos	Duomenų subjektų, kurių asmens duomenų saugumas pažeistas, kategorijos	Pažeidimo poveikis ir galimos pasekmės	Priemonės, kurių buvo imtasi pažeidimui pašalinti ir (ar) neigiamoms pažeidimo pasekmėms sumažinti	Informacija, ar apie pažeidimą buvo pranešta Valstybinei duomenų apsaugos inspekcijai (pranešimo data, numeris, pavėluoto pranešimo priežastys, priimto sprendimo neteikti pranešimo motyvai)	Informacija, ar apie pažeidimą buvo pranešta duomenų subjektui (data ir numeris), arba nepranešimo priežastys	Kita reikšminga informacija	Žurnalą pildžiusio asmens vardas, pavardė, pareigos
1.													
2.													
3.													
4.													
5.													
6.													
7.													
8.													
9.													
10.													

_____