VIEŠOSIOS ĮSTAIGOS
UKMERGĖS LIGONINĖS
VYRIAUSIASIS GYDYTOJAS

ĮSAKYMAS

DĖL VŠĮ UKMERGĖS LIGONINĖS ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ VALDYMO POLITIKOS PATVIRTINIMO

2021 m. sausio 15 d. Nr. V-8
Ukmergė

Vadovaudamasis 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), Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu

1. T v i r t i n u Viešosios įstaigos Ukmergės ligoninės asmens duomenų saugumo pažeidimo valdymo politiką (pridedama).

2. Pripažįstu netekusiu galios VšĮ Ukmergės ligoninės vyriausiojo gydytojo 2018 m. spalio 11 d. įsakymą Nr. V-132 „Dėl pranešimo apie asmens duomenų saugumo pažeidimą pateikimo tvarkos aprašo patvirtinimo“.

3. Į p a r e i g o j u Personalo skyriaus darbuotojus su patvirtinta politika elektroniniu paštu supažindinti skyriaus vedėjus ir vyresniuosius slaugytojus, kurie su šia politika pasirašytinai supažindina sau pavaldžius darbuotojus.

Vyriausiasis gydytojas Rimvydas Civilka

PATVIRTINTA
VšĮ Ukmergės ligoninės vyr. gydytojo
2021 m. sausio 15 d. įsakymu Nr. V-8

VIEŠOSIOS ĮSTAIGOS UKMERGĖS LIGONINĖ ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ VALDYMO POLITIKA

SĄVOKOS

BDAR	reiškia 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentą (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).
Darbuotojas	reiškia Ligoninės darbuotoją.
Duomenų apsaugos pareigūnas	reiškia Ligoninės vadovo paskirtą duomenų apsaugos pareigūną.
Ligoninė	reiškia Viešąją įstaigą Ukmergės ligoninė, juridinio asmens kodas: 182935350, adresas: Vytauto g. 105, LT-20184 Ukmergė, Lietuvos Respublika, įregistruotą Lietuvos Respublikos juridinių asmenų registre.
Ligoninės vadovas	reiškia Ligoninės vienasmenį valdymo organą (Ligoninės vyriausiąjį gydytoją).
Paskirtasis asmuo	reiškia Ligoninės vadovo paskirtą asmenį, atsakingą už asmens duomenų saugumo pažeidimo valdymą.
Pažeidimas	reiškia asmens duomenų saugumo pažeidimą, 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.
Pažeidimo ataskaita	reiškia Pažeidimo tyrimo ataskaitą, kuria rengia Pažeidimą tiriantis atsakingas asmuo.
Pažeidimų registras	reiškia vidinį Pažeidimų registrą, kuriame registruojami visi įvykę Pažeidimai.
Politika	reiškia šią Asmens duomenų saugumo pažeidimų valdymo politiką.
VDAI	reiškia Valstybinę duomenų apsaugos inspekciją (L. Sapiegos g. 17, Vilnius, Lietuvos Respublika).

I POLITIKOS APIMTIS IR TIKSLAI

1. Šioje Politikoje yra išdėstyti bendrieji reikalavimai dėl incidentų, kurie lemia Ligoninės kontroliuojamų ir (arba) tvarkomų asmens duomenų pažeidimus, nustatymo, įvertinimo, valdymo ir administravimo.
2. Šios Politikos tikslai – užtikrinti, kad Ligoninė tinkamai vykdytų savo teisines pareigas; užtikrinti geresnę asmens duomenų apsaugą; padidinti skaidrumą; sudaryti galimybę asmenims būti informuotiems apie visus reikšmingus incidentus, susijusius su jų asmens duomenimis; ir užtikrinti, kad bet kokia galima tokių incidentų sukeliama žala būtų minimali.

3. Politika parengta vadovaujantis BDAR, Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu bei kitais galiojančiais teisės aktais.
4. Šioje Politikoje vartojamos sąvokos atitinka BDAR, Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatyme ir kituose taikytinuose teisės aktuose įtvirtintas sąvokas.
5. Ši Politika taikoma:
5.1. visiems asmens duomenims, kuriuos Ligoninė sugeneravo arba gavo bet kokiu formatu (įskaitant įrašus popieriniu formatu); naudojamiems darbo vietose; saugomiems nešiojamuose prietaisuose ir laikmenose; transportuojamiems iš darbo vietų fiziškai ar elektroniniu būdu; arba prieinamiems nuotoliniu būdu;
5.2. asmens duomenims, saugomiems visose Ligoninės IT sistemose;
5.3. bet kokioms kitoms IT sistemoms, kuriose saugomi ar tvarkomi Ligoninės duomenys, įskaitant sistemas, kurias valdo paslaugas Ligoninei teikiantys duomenų tvarkytojai.
6. Politika taikoma šiems asmenims, atsakingiems už Pažeidimų valdymą: Duomenų apsaugos pareigūnui, Paskirtajam asmeniui, darbuotojams, atsakingiems už tam tikrą asmens duomenų kategoriją, arba kitiems darbuotojams, kuriems gali būti nurodyta atlikti tam tikras užduotis įvykus Pažeidimui. Politikos III skyriuje nustatyta pranešimo apie galimą Pažeidimą tvarka yra taikoma visiems Ligoninės darbuotojams.

II ASMENS DUOMENŲ SAUGUMO PAŽEIDIMAS

7. Pažeidimas – tai 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.
8. Šie duomenys apima tiek automatizuotomis priemonėmis tvarkomus duomenis (t. y. saugomus ar kitaip tvarkomus elektroniniu būdu), tiek duomenis, saugomus ranka padarytuose įrašuose ar dokumentuose (t. y. saugomus ar kitaip tvarkomus popierine forma).
9. Pažeidimai gali apimti (nebaigtinis sąrašas):
9.1. konfidencialių duomenų atskleidimą leidimo neturintiems asmenims;
9.2. dokumentų ar įrangos, kurioje duomenys saugomi, praradimą ar vagystę;
9.3. įrašų popieriniuose dokumentuose praradimą ar vagystę;
9.4. netinkamą prieigos kontrolę, leidžiančią neteisėtai susipažinti su ar naudotis duomenimis;
9.5. bandymus neleistinai pasiekti informacines sistemas, pavyzdžiui, į jas įsilaužti;
9.6. nesant atsakingo asmens leidimo pakeistus ar ištrintus įrašus;
9.7. virusus, kitą kenkėjišką programinę įrangą ar kitas saugumo atakas IT įrangos sistemose ar tinkluose;
9.8. fizinio saugumo pažeidimus, pavyzdžiui, jėga atidarius saugomos patalpos duris ar langus, dokumentų spintą, kuriuose laikoma konfidenciali informacija;
9.9. IT įrangos palikimą be priežiūros (prisijungus prie naudotojo paskyros ir neužrakinus ekrano), kai informacija tampa prieinama su ja susipažinti teisės neturintiems asmenims;
9.10. elektroninių laiškų, kuriuose yra asmens ar kitų neskelbtinų duomenų, išsiuntimą per klaidą ne tiems gavėjams.
10. Situacijos, kurios gali sukelti Pažeidimus (nebaigtinis sąrašas):
10.1. Prarandamas Darbuotojo naudojamas kompiuteris ar kitas prietaisas;
10.2. asmens, tvarkančio asmens duomenis, klaida;
10.3. Ligoninės naudojamos programinės įrangos klaida;
10.4. Ligoninės valdomos įrangos techninis gedimas;
10.5. neteisėtai prieinama prie slaptažodžių, kitų prisijungimo duomenų, ar jie yra kitaip pažeidžiami.
11. **Pažeidimai duomenų tvarkytojų valdomose duomenų bazėse, informacinėse sistemose**
11.1. Pažeidimai taip pat gali įvykti Ligoninės pasitelktiems duomenų tvarkytojams tvarkant asmens duomenis Ligoninės vardu. Tokie Pažeidimai nagrinėjami taip pat, kaip ir Pažeidimai, kurie įvyksta Ligoninėje, ir valdomi vadovaujantis šioje Politikoje bei duomenų tvarkymo sutartyje išdėstytomis nuostatomis.

III PAŽEIDIMO NUSTATYMAS. PRANEŠIMAS APIE PAŽEIDIMĄ

12. Bet kuris Ligoninės darbuotojas, susidūręs su galimu Pažeidimo atveju, **nedelsdamas apie tai praneša**:

12.1. savo tiesioginiam vadovui, kuris nedelsdamas informuoja Duomenų apsaugos pareigūną ir Ligoninės vadovą, arba
12.2. tiesiogiai Duomenų apsaugos pareigūnui ir Ligoninės vadovui.
13. Jeigu Duomenų apsaugos pareigūnas nepaskirtas, nepasiekiamas ar Pažeidimo metu nedirba, informacija apie galimą Pažeidimą perduodama Paskirtajam asmeniui.
14. Pranešimą apie Pažeidimą perduoti Duomenų apsaugos pareigūnui arba Paskirtajam asmeniui taip pat gali duomenų tvarkytojo, kuris tvarko asmens duomenis Ligoninės vardu, atstovas. Jeigu bet kuris Darbuotojas, išskyrus Duomenų apsaugos pareigūną, gauna tokį pranešimą iš duomenų tvarkytojo ar kitos trečiosios šalies, jis turi nedelsdamas perduoti jį Duomenų apsaugos pareigūnui arba Paskirtajam asmeniui.

IV PIRMINIS PAŽEIDIMO VERTINIMAS

15. Remdamasis pirminiu pranešimu ir (ar) ataskaita apie galimą Pažeidimą, Duomenų apsaugos pareigūnas arba Paskirtasis asmuo atlieka pirminį Pažeidimo vertinimą ir nustato, ar Pažeidimas įvyko; jeigu Pažeidimas įvyko, taip pat nustato:
15.1. kokie asmens duomenys buvo paveikti;
15.2. kokia Pažeidimo priežastis;
15.3. koks Pažeidimo mastas (kiek asmenų buvo paveikti);
15.4. kokia Pažeidimo galimai padaryta žala paveiktiems asmenims;
15.5. kaip galima sustabdyti Pažeidimą ir (arba) sumažinti galimas jo pasekmes.
16. Atlikdamas pirminį Pažeidimo vertinimą, Duomenų apsaugos pareigūnas (arba jam nesant Paskirtasis asmuo) išnagrinėja kiekvieną pranešimą ir (ar) ataskaitą apie galimą Pažeidimą, nustato preliminarų Pažeidimo pobūdį bei mastą ir priima vieną iš šių sprendimų:
16.1. atmesti pranešimą apie Pažeidimą kaip neteisingą, netikslų ar neatitinkantį tikrovės;
16.2. tais atvejais, kai Pažeidimas nesusijęs su asmens duomenimis, informuoti kitą atsakingą Darbuotoją arba Ligoninės vadovą;
16.3. patvirtinti Pažeidimo faktą ir pradėti Pažeidimo tyrimo ir valdymo procedūrą.
17. Tuo atveju, kai atlikus pirminį Pažeidimo vertinimą buvo priimtas sprendimas patvirtinti Pažeidimo faktą, Duomenų apsaugos pareigūnas (arba Paskirtasis asmuo) pradeda Pažeidimo tyrimo ir valdymo procedūrą, informuoja apie pradėtą procedūrą Ligoninės vadovą ir pateikia siūlymą, ar reikia pasitelkti kitus Darbuotojus ar išorinius konsultantus, ekspertus, kurie padėtų atlikti Pažeidimo tyrimą.

V PAŽEIDIMO TYRIMAS

18. Duomenų apsaugos pareigūnas arba Paskirtasis asmuo išnagrinėja visus faktus ir aplinkybes, susijusias su Pažeidimu, ir atlieka Pažeidimo tyrimą, kurio metu, atsižvelgdamas į turimą informaciją bei prieinamus duomenis nustato:
18.1. Pažeidimo datą ir laiką;
18.2. Pažeidimo pobūdį;
18.3. paveiktų asmens duomenų kategorijas ir apytikslį paveiktų duomenų subjektų bei asmens duomenų įrašų skaičių;
18.4. galimas Pažeidimo pasekmes;
18.5. neatidėliotinas taisomąsias priemones, kurių Ligoninė turi imtis, kad pašalintų Pažeidimą ir (ar) sumažintų bet kokią galimą žalą.
19. Įvertinus aukščiau nurodytą informaciją nustatomas Pažeidimo lygis. Tyrimo metu apie jo eigą ir rezultatus informuojamas Ligoninės vadovas.

VI PAŽEIDIMO VALDYMAS IR PAŠALINIMAS

20. Nustačius, kad Pažeidimas įvyko, Ligoninė turi imtis neatidėliotinų ir tinkamų veiksmų, kad suvaldytų Pažeidimą ir galimas jo pasekmes. Duomenų apsaugos pareigūnas (arba jam nesant Paskirtasis asmuo):
20.1. Nustato Ligoninės darbuotojus, kuriems reikia pranešti apie Pažeidimą, informuoja juos apie pažeidimo faktą ir tai, kokių veiksmų iš jų tikimasi siekiant apriboti Pažeidimą (pavyzdžiui, izoliuoti pažeistą tinklo dalį, rasti prarastą įrangos dalį, pakeisti prieigos kodus ir pan.).

20.2. Nustato, ar kokių veiksmų įmanoma imtis siekiant kompensuoti nuostolius ir sumažinti žalą, kurią gali sukelti Pažeidimas (pavyzdžiui, fizinis įrangos ar įrašų susigrąžinimas, atsarginių kopijų panaudojimas siekiant atkurti prarastus ar sugadintus duomenis).
20.3. Nustato, ar apie Pažeidimą reikia nedelsiant pranešti priežiūros institucijai ir (arba) paveiktiems duomenų subjektams (pavyzdžiui, kai yra didelis pavojus arba didelė žala asmenims).
20.4. Esant poreikiui (pavyzdžiui, įvykus vagystei ar kitai nusikalstamai veikai), informuoja teisėsaugos institucijas.

VII PAŽEIDIMO RIMTUMO IR JO SUKELTO PAVOJAUS VERTINIMAS

21. Vertindami Pažeidimo sukeltą pavojų, Duomenų apsaugos pareigūnas arba Paskirtasis asmuo turi apsvarstyti galimas neigiamas pasekmes asmenims, t. y. ar tikėtina, kad kiltų neigiamų pasekmių, ir jei taip, kokio rimtumo ar svarbos jos galėtų būti.
22. Pažeidimo rimtumo ir jo sukelto pavojaus vertinimo tvarka nustatyta Priede Nr. 2.

VIII PAŽEIDIMO ATASKAITA

23. Duomenų apsaugos pareigūnas arba Paskirtasis asmuo parengia ir dokumentais pagrindžia ataskaitą (toliau – „**Pažeidimo ataskaita**“), kurioje pateikiama ši informacija:
23.1. Pažeidimo aprašymas (Pažeidimo data ir laikas, pobūdis);
23.2. Paveiktų asmens duomenų kategorijos ir apytikslis paveiktų duomenų subjektų bei asmens duomenų įrašų skaičius;
23.3. informacija apie informacines, IT sistemas, įrangą ar prietaisus, susijusius su Pažeidimu, taip pat dėl Pažeidimo prarastus ar kitaip paveiktus duomenis;
23.4. Pažeidimo priežastis(-ys);
23.5. taisomosios priemonės, kurių Ligoninė ėmėsi arba siūlo imtis, kad būtų pašalintas Pažeidimas, sumažinta žala ir išvengta Pažeidimų ateityje;
23.6. Pažeidimo pasekmės;
23.7. tyrimo metu nenustatyti, tačiau galimi Pažeidimo padariniai;
23.8. veiksmai ir priemonės, padėsiantys išvengti Pažeidimo pasikartojimo;
23.9. tokių veiksmų ir priemonių šalutinis poveikis, jei toks yra;
23.10. tolesnių veiksmų ir duomenų apsaugos gerinimo rekomendacijos, kiek tai susiję su Pažeidimu;
23.11. bet kokie kiti tyrimo metu nustatyti svarbūs faktai.
24. Pažeidimo ataskaita pateikiama Ligoninės vadovui. Pažeidimo ataskaita remiamasi pildant pagrindinį incidentų žurnalą ir Pažeidimų registrą, kurie yra saugomi ir archyvuojami.
25. Įvertinęs su Pažeidimu susijusius faktus ir aplinkybes, Duomenų apsaugos pareigūnas arba Paskirtasis asmuo nusprendžia, kokių taisomųjų priemonių reikėtų imtis.

IX PRANEŠIMO APIE PAŽEIDIMĄ TVARKA

26. Duomenų apsaugos pareigūnas (arba jam nesant Paskirtasis asmuo) nedelsdamas ir, kai įmanoma, per 72 valandas nuo to momento, kai sužinojo apie Pažeidimą, VDAI nustatyta forma praneša VDAI apie Pažeidimą.
27. Pranešime VDAI turi būti pateikta bent ši informacija:
27.1. Pažeidimo data ir laikas;
27.2. Pažeidimo pobūdis;
27.3. paveiktų asmens duomenų kategorijos ir apytikslis paveiktų duomenų subjektų bei asmens duomenų įrašų skaičius;
27.4. galimos Pažeidimo pasekmės;
27.5. taisomosios priemonės, kurių Ligoninė ėmėsi arba siūlo imtis, kad būtų pašalintas Pažeidimas, sumažinta bet kokia galima žala;
27.6. Duomenų apsaugos pareigūno ar kito kontaktinio asmens, kuris gali pateikti daugiau informacijos, vardas, pavardė ir kontaktiniai duomenys.
28. Kai įmanoma, pranešime taip pat turi būti nurodytos galimos Pažeidimo priežastys (jei tokios nustatomos iki pranešimo parengimo). Jeigu pranešimas išsiunčiamas vėliau nei per 72 valandas nuo to momento, kai buvo sužinota apie Pažeidimą, taip pat nurodomos tokio vėlavimo priežastys.

29. Duomenų apsaugos pareigūnas arba Paskirtasis asmuo gali apie Pažeidimą nepranešti VDAI, jeigu nustatoma, kad Pažeidimas nekelia pavojaus fizinių asmenų teisėms ir laisvėms (1 lygio Pažeidimas).
30. Duomenų subjektai apie Pažeidimą informuojami nedelsiant, jeigu yra tikėtina, kad Pažeidimas gali sukelti didelį pavojų jų teisėms ir laisvėms (2 ar aukštesnio lygio Pažeidimas). Duomenų apsaugos pareigūnas arba Paskirtasis asmuo nusprendžia, kokiu būdu pranešti duomenų subjektams apie Pažeidimą. Paprastai paveiktiems duomenų subjektams išsiunčiamas el. laiškas su pranešimu. Pranešimą (pranešimo forma pateikiama kaip Priedas Nr. 3) turi būti pateikta bent ši aiškiai ir suprantamai išdėstyta informacija:
30.1. galimos Pažeidimo pasekmės;
30.2. taisomosios priemonės, kurių Ligoninė ėmėsi arba siūlo imtis, kad būtų pašalintas Pažeidimas, sumažinta bet kokia galima žala;
30.3. Duomenų apsaugos pareigūno ar kito kontaktinio asmens, kuris gali pateikti daugiau informacijos, vardas, pavardė ir kontaktiniai duomenys.
31. Jei įmanoma ir reikalinga, pranešime taip pat pateikiama ši informacija:
31.1. Pažeidimo paveikti asmens duomenys;
31.2. Pažeidimo data ir laikas;
31.3. Pažeidimo pobūdis;
31.4. galimos Pažeidimo priežastys (jei tokios nustatomos iki pranešimo parengimo);
31.5. rekomenduojamos priemonės, kurių turėtų imtis duomenų subjektas.
32. Duomenų apsaugos pareigūnas arba Paskirtasis asmuo gali nuspręsti neinformuoti duomenų subjektų apie Pažeidimą šiais atvejais:
32.1. dėl Ligoninės įgyvendintų techninių ar organizacinių saugumo priemonių (pavyzdžiui, šifravimo), paveikti asmens duomenys yra nesuprantami tretiesiems asmenims, kurie neturi leidimo su jais susipažinti;
32.2. taisomosios priemonės, kurių ėmėsi Ligoninė, užtikrina, kad duomenų subjektų teisėms ir laisvėms nebekils didelis pavojus.
33. Jeigu atskiras kiekvieno duomenų subjekto informavimas apie Pažeidimą reikalauja neproporcingų Ligoninės pastangų, suderinęs su Ligoninės vadovu Duomenų apsaugos pareigūnas (arba Paskirtasis asmuo) gali parengti ir paskelbti viešą pranešimą, tokiu būdu informuodamas paveiktus duomenų subjektus apie Pažeidimą.

X PAŽEIDIMO DOKUMENTACIJA

34. Užbaigęs tyrimą, Duomenų apsaugos pareigūnas arba Paskirtasis asmuo užpildo Pažeidimų registrą (Priedas Nr. 5), įrašydamas aktualią informaciją apie Pažeidimą.
35. Kad priežiūros institucija galėtų patikrinti atitiktį teisiniams reikalavimams, turi būti užfiksuota bent ši informacija:
35.1. Pažeidimo aprašymas;
35.2. paveiktos asmens duomenų kategorijos ir įrašai;
35.3. Pažeidimo priežastys;
35.4. galimos Pažeidimo pasekmės;
35.5. vidaus tyrimo rezultatai;
35.6. taisomosios priemonės, kurių ėmėsi Ligoninė.
36. Kiekvieno rimto (3 lygio) Pažeidimo atveju Duomenų apsaugos pareigūnas (arba jam nesant Paskirtasis asmuo) atlieka patikrinimą, kurio metu apsvarsto ir Ligoninės vadovą informuoja apie tai:
36.1. kokių veiksmų reikia imtis, siekiant sumažinti Pažeidimų pavojų ateityje ir jų poveikį?
36.2. ar reikia tobulinti šioje Politikoje įtvirtintą procedūrą, siekiant padidinti reagavimo į Pažeidimus veiksmingumą?
36.3. ar saugumo užtikrinimo srityje yra silpnų vietų, kurias reikia stiprinti?
36.4. ar darbuotojai ir paslaugų teikėjai žino savo atsakomybes už duomenų saugumą ir yra tinkamai apmokyti?
36.5. ar reikalingos papildomos investicijos, siekiant sumažinti Pažeidimų poveikį?
37. Duomenų apsaugos pareigūnas arba Paskirtasis asmuo parengia šio patikrinimo ataskaitą, kurioje yra nurodomos aptiktos problemos ar neatitikimai, galimi jų sprendimo būdai ir šių sprendimo būdų įgyvendinimo išlaidos.

XI ATSAKOMYBĖ

38. Bendra atsakomybė už Pažeidimų valdymą bei institucijų ir (arba) duomenų subjektų informavimą tenka Duomenų apsaugos pareigūnui (arba jam nesant Paskirtajam asmeniui). Atsakomybė už Duomenų apsaugos pareigūno arba Paskirtojo asmens nurodymų, susijusių su Pažeidimo valdymu, vykdymą tenka Darbuotojui, kuriam tie nurodymai yra skirti.

XII BAIGIAMOSIOS NUOSTATOS

39. Ši Politika įsigalioja 2021 m. sausio 15 d.
40. Ši Politika yra periodiškai peržiūrima ir prireikus atnaujinama.
41. Šioje Politikoje įtvirtintą Pažeidimų valdymo tvarką gali patikslinti ar papildyti kiti Ligoninės vidaus dokumentai ar lokaliniai teisės aktai.

Priedai:
Priedas Nr. 1. Pranešimo apie pažeidimą forma.
Priedas Nr. 2. Pažeidimo rimtumo ir jo keliamo pavojaus vertinimas.
Priedas Nr. 3. Pranešimo duomenų subjektui forma.
Priedas Nr. 4. Pažeidimų registro forma.

PRIEDAS NR. 1. PRANEŠIMO APIE PAŽEIDIMĄ FORMA

Forma patvirtinta
Valstybinės duomenų apsaugos inspekcijos
direktoriaus 2018 m. rugpjūčio 29 d.
įsakymu Nr. 1T-82(1.12.E)

Pranešimo apie asmens duomenų saugumo pažeidimą rekomenduojama forma

_____

(duomenų valdytojo (juridinio asmens) pavadinimas, duomenų valdytojo atstovo pavadinimas, duomenų valdytojo (fizinio asmens) vardas, pavardė)[1]

_____

(juridinio asmens kodas ir buveinės adresas arba fizinio asmens kodas, gimimo data (jeigu asmuo neturi asmens kodo) ir asmens duomenų tvarkymo vieta

_____

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

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] Kai pranešimas apie asmens duomenų saugumo pažeidimą teikiamas pagal Lietuvos Respublikos asmens duomenų, tvarkomų nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas, bausmių vykdymo arba nacionalinio saugumo ar gynybos tikslais, teisinės apsaugos įstatymo (toliau – Įstatymas) 29 straipsnį, nurodomi tik duomenų valdytojo (juridinio asmens) duomenys.

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)[2]

6.1. Vardas ir pavardė _____

6.2. Telefono ryšio numeris _____

6.3. Elektroninio pašto adresas _____

6.4. Pareigos _____

6.5. Darbovietės pavadinimas ir adresas _____

[2] Kai pranešimas apie asmens duomenų saugumo pažeidimą teikiamas pagal Įstatymo 29 straipsnį, nenurodomi šios formos 6.4 ir 6.5 papunkčiuose nurodyti duomenys.

7. Pranešimo pateikimo Valstybinei duomenų apsaugos inspekcijai pateikimo vėlavimo priežastys

8. Kita reikšminga informacija

(pareigos) (parašas) (vardas, pavardė)

PRIEDAS NR. 2. PAŽEIDIMO RIMTUMO IR JO KELIAMO PAVOJAUS VERTINIMAS

1. Norėdamas nustatyti Pažeidimo lygį, Duomenų apsaugos pareigūnas arba Paskirtasis asmuo turi įvertinti visas su Pažeidimu susijusias aplinkybes, įskaitant, be kita ko, galimas pasekmes, šių pasekmių atsiradimo tikimybę, paveiktų duomenų subjektų ir asmens duomenų įrašų skaičių ir bet kokią kitą svarbią informaciją apie Pažeidimą. Pažeidimo rimtumas ir jo keliamas pavojus vertinamas atsižvelgiant į žemiau dėstomą informaciją.

I RIMTUMO ĮVERTINIMAS

2. **Vertinant Pažeidimo rimtumą, turi būti apsvarstytos šios aplinkybės**:
2.1. Informacija apie IT sistemas, įrangą, prietaisus, įrašus, susijusius su Pažeidimu.
2.2. Informacija apie paveiktus duomenis:
   2.2.1. Koks paveiktų duomenų pobūdis?
   2.2.2. Kiek duomenų paveikta? Jeigu pavogtas ar kitaip parastas nešiojamasis kompiuteris: kada paskutinį kartą buvo padaryta atsarginė nešiojamame kompiuteryje saugomos informacijos kopija pagrindinėse IT sistemose?
   2.2.3. Ar paveikti duomenys unikalūs? Ar jų praradimas turėtų neigiamų veiklos, tyrimų, finansinių, teisinių, atsakomybės ar reputacijos pasekmių Ligoninei ar trečiosioms šalims?
   2.2.4. Kiek duomenų subjektų patyrė poveikį?
   2.2.5. Ar duomenims taikomi kokie nors sutartiniai saugumo reikalavimai, pavyzdžiui, pagal duomenų tvarkymo sutartis?
   2.2.6. Koks duomenų neskelbtinumo pobūdis? Ar kurie nors iš paveiktų duomenų laikomi susijusiais su dideliu pavojumi (kaip nurodyta toliau)?
2.3. Asmens duomenys laikomi susijusiais su **dideliu pavojumi**, kai šie duomenys yra:
   2.3.1. priskiriami specialių kategorijų asmens duomenims;
   2.3.2. informacija, kuri gali būti panaudota siekiant suklastoti tapatybę, pavyzdžiui, asmeninė banko sąskaita ir kiti finansiniai duomenys, taip pat nacionaliniai identifikatoriai, pavyzdžiui, identifikacinis numeris, asmens kodas, pasų ar vizų kopijos;
   2.3.3. asmeninė informacija, susijusi su pažeidžiamais suaugusiais ir vaikais;
   2.3.4. išsami informacija apie asmenis, įskaitant informaciją apie darbo rezultatus, atlyginimą ar asmeninį gyvenimą, kurios atskleidimas sukeltų tam asmeniui didelę žalą ar kančią;
   2.3.5. saugumo informacija, kurios atskleidimas sukeltų grėsmę asmenų saugumui.

II PAVOJAUS ĮVERTINIMAS

3. **Vertinant pavojų asmenims, turi būti apsvarstyta**:
3.1. Kokie asmens duomenys buvo paveikti?
3.2. Kokios galimos neigiamos pasekmės asmenims?
3.3. Kokio rimtumo ar svarbos yra neigiamos pasekmės?
3.4. Kokia tikimybė, kad neigiamos pasekmės kils?
4. **Vertinant pavojų Ligoninei, turi būti apsvarstyta**:
4.1. Strateginės ir veiklos pasekmės.
4.2. Atitikties ir teisinės pasekmės.
4.3. Finansinės pasekmės.
4.4. Pasekmės reputacijai.
4.5. Pasekmės veiklos tęstinumui.

III PAŽEIDIMŲ LYGIAI

5. **Išskiriami šie Pažeidimų lygiai**:
5.1. **1 lygis**: jokio arba nedidelis pavojus duomenų subjektų teisėms bei laisvėms ir Ligoninei.
5.2. **2 lygis**: vidutinis pavojus duomenų subjektų teisėms bei laisvėms ir Ligoninei.
5.3. **3 lygis**: didelis pavojus duomenų subjektų teisėms bei laisvėms ir Ligoninei.

IV PAŽEIDIMO LYGIO NUSTATYMAS

6. **1 lygis: vietinės reikšmės arba nedidelis Pažeidimas**

6.1. Vietinės reikšmės Pažeidimas – nedidelis veiklos sutrikdymas; nėra rimtos grėsmės asmenų gyvybei, turtui ar teisėms bei laisvėms; nėra grėsmės Ligoninės įvaizdžiui ir reputacijai.

6.2. Pažeidimo pasekmės, turto praradimas arba neprieinamumas gali būti suvaldyti vietos lygiu vykdant įprastas veiklos procedūras.

6.3. Pasekmės duomenų subjektams: laikinai neprieinamos, vėluojančios arba lėtesnės paslaugos, laikinas (Ligoninės Darbuotojų) negalėjimas užbaigti darbo užduočių arba jokių pasekmių.

6.4. Apskritai jokio arba nedidelis pavojus duomenų subjektų teisėms bei laisvėms ir Ligoninei.

6.5. Šiuo atveju Duomenų apsaugos pareigūnas arba Paskirtasis asmuo apie tyrimo išvadas turi pranešti tik Ligoninės vadovui.

7. **2 lygis: vidutiniškai ekstremali situacija arba vidutinis Pažeidimas**

7.1. Vidutiniškai ekstremali situacija – pagrindinės Ligoninės veiklos (paslaugų teikimo) sutrikdymas. Galima nedidelė grėsmė pavienių asmenų sveikatai, turtui arba teisėms bei laisvėms; grėsmė Ligoninės įvaizdžiui ar reputacijai.

7.2. Pažeidimo suvaldymas ir pašalinimas reikalauja kitų Ligoninės Darbuotojų arba išorės specialistų pagalbos.

7.3. Pasekmės duomenų subjektams: asmens duomenų vientisumo netekimas, užsitęsęs paslaugų neprieinamumas.

7.4. Apie Pažeidimą būtina pranešti Ligoninės vadovybei, priežiūros institucijoms ar paveiktiems asmenims.

7.5. Tokiu atveju Duomenų apsaugos pareigūnas arba Paskirtasis asmuo turi nuspręsti, kam reikia pranešti apie pažeidimą, pavyzdžiui:

7.5.1. priežiūros institucijai;

7.5.2. paveiktiems duomenų subjektams;

7.5.3. Ligoninės vadovui.

7.6. Vidutinis pavojus duomenų subjektų teisėms bei laisvėms ir Ligoninei.

8. **3 lygis: labai ekstremali situacija arba didelis Pažeidimas**

8.1. Labai ekstremali situacija – visiškas Ligoninės pagrindinės veiklos (paslaugų teikimo) sutrikdymas; galima ilgalaikė žala. Didelė grėsmė asmenų sveikatai, turtui arba teisėms bei laisvėms. Didelis paveiktų duomenų subjektų skaičius. Didelė grėsmė Ligoninės įvaizdžiui ar reputacijai. Labai tikėtina, kad Pažeidimas turės neigiamų finansinių, teisinių, atsakomybės ar reputacijos pasekmių Ligoninei.

8.2. Pažeidimo suvaldymas ir pašalinimas reikalauja didelių Ligoninės išteklių, viršijančių įprastas veiklos sąnaudas.

8.3. Paveikti asmens duomenys apima daug asmens duomenų, susijusių su dideliu pavojumi (kaip apibrėžta šio priedo I skyriuje).

8.4. Pasekmės duomenų subjektams: neskelbtinų asmens duomenų konfidencialumo praradimas, apgaulės ar tapatybės vagystės pavojus, neleistinas asmens duomenų, įskaitant duomenis, susijusius su dideliu pavojumi, atskleidimas nežinomam trečiųjų asmenų skaičiui, ilgalaikis paslaugų teikimo nutrūkimas.

8.5. Apie Pažeidimą būtina nedelsiant pranešti Ligoninės vadovybei, priežiūros institucijoms ir duomenų subjektams.

8.6. Didelis pavojus duomenų subjektų teisėms bei laisvėms ir Ligoninei.

PRIEDAS NR. 3. PRANEŠIMO DUOMENŲ SUBJEKTUI FORMA

[MMMM-mm-dd]

Gerb. [_____],

Apgailestaudami informuojame, kad Ligoninėje buvo užfiksuotas asmens duomenų saugumo pažeidimas (toliau – „**Saugumo pažeidimas**"). Prie tam tikrų su jumis susijusių asmens duomenų buvo arba galėjo būti neteisėtai gauta prieiga, jie buvo arba galėjo būti nukopijuoti, jų saugumas buvo arba galėjo būti pažeistas. Mes intensyviai dirbame siekdami sumažinti padarinius ir nustatyti, kas nulėmė šį Saugumo pažeidimą. Siekdami užtikrinti skaidrumą, žemiau esančioje lentelėje pateikiame konkrečią informaciją apie Saugumo pažeidimą.

1. **Saugumo pažeidimo data ir laikas:**
2. **Saugumo pažeidimo pobūdis:**
3. **Saugumo pažeidimo galima(-os) priežastis(-ys):**
4. **Jūsų asmens duomenys, prie kurių buvo arba galėjo būti neteisėtai gauta prieiga, kurie buvo arba galėjo būti nukopijuoti, kurių saugumas buvo arba galėjo būti pažeistas:**
5. **Tikėtinos Saugumo pažeidimo pasekmės:**
6. **Priemonės, kurių imtasi siekiant sušvelninti galimą žalą ir pašalinti šį Saugumo pažeidimą:**
7. **Rekomenduojame jums imtis šių priemonių:**

Jeigu turite klausimų dėl Saugumo pažeidimo ar tai kelia jums susirūpinimą, susisiekite su mūsų Duomenų apsaugos pareigūnu Lina Žukliene el. pašto adresu personalas@uklig.lt.

Dedame visas pastangas, kad užtikrintume savo Ligoninės pacientų bei kitų duomenų subjektų privatumą ir tinkamą jų duomenų apsaugą.

Rimvydas Civilka

Ligoninės vyriausiasis gydytojas

Viešoji įstaiga Ukmergės ligoninė, juridinio asmens kodas: 182935350
Vytauto g. 105, LT-20184 Ukmergė, Lietuvos Respublika
Tel. 8 340 65299, el. paštas administracija@uklig.lt

PRIEDAS NR. 4. PAŽEIDIMŲ REGISTRO FORMA

Pažeidimo data ir laikas	Pažeidimo aprašymas (jo santrauka)	Paveiktų asmens duomenų kategorijos	Paveikti asmens duomenys	Pažeidimo priežastis	Galimos pasekmės	Pažeidimo tyrimo rezultatai	Priemonės, kurių buvo imtasi