VALSTYBINĖS LIGONIŲ KASOS PRIE SVEIKATOS APSAUGOS MINISTERIJOS DIREKTORIUS

ĮSAKYMAS DĖL VALSTYBINĖS LIGONIŲ KASOS PRIE SVEIKATOS APSAUGOS MINISTERIJOS DIREKTORIAUS 2021 M. KOVO 23 D. ĮSAKYMO NR. 1K-94 „DĖL VALSTYBINĖS LIGONIŲ KASOS PRIE SVEIKATOS APSAUGOS MINISTERIJOS IR TERITORINIŲ LIGONIŲ KASŲ TVARKOMŲ ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ VALDYMO TVARKOS APRAŠO PATVIRTINIMO“ PAKEITIMO

2025 m. d. Nr. 1K-
Vilnius

1. P a k e i č i u Valstybinės ligonių kasos prie Sveikatos apsaugos ministerijos direktoriaus 2021 m. kovo 23 d. įsakymą Nr. 1K-94 „Dėl Valstybinės ligonių kasos prie Sveikatos apsaugos ministerijos ir teritorinių ligonių kasų tvarkomų asmens duomenų saugumo pažeidimų valdymo tvarkos aprašo patvirtinimo“ ir jį išdėstau nauja redakcija:

„VALSTYBINĖS LIGONIŲ KASOS PRIE SVEIKATOS APSAUGOS MINISTERIJOS DIREKTORIUS

ĮSAKYMAS DĖL VALSTYBINĖS LIGONIŲ KASOS PRIE SVEIKATOS APSAUGOS MINISTERIJOS TVARKOMŲ ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ VALDYMO TVARKOS APRAŠO PATVIRTINIMO

Vadovaudamasis 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamento (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) 24 straipsnio 1 dalimi:

1. T v i r t i n u Valstybinės ligonių kasos prie Sveikatos apsaugos ministerijos tvarkomų asmens duomenų saugumo pažeidimų valdymo tvarkos aprašą (pridedama).

2. P a v e d u Valstybinės ligonių kasos prie Sveikatos apsaugos ministerijos valstybės tarnautojams ir darbuotojams, dirbantiems pagal darbo sutartį, vadovautis šio įsakymo 1 punktu patvirtintu tvarkos aprašu.“

2. N u s t a t a u, kad šis įsakymas įsigalioja 2025 m. liepos 1 d.

Direktorius Gytis Bendorius

PATVIRTINTA
Valstybinės ligonių kasos
prie Sveikatos apsaugos ministerijos
direktoriaus 2021 m. kovo 23 d.
įsakymu Nr. 1K-94
(Valstybinės ligonių kasos prie
Sveikatos apsaugos ministerijos
direktoriaus 2025 m. d.
įsakymo Nr. 1K- redakcija)

VALSTYBINĖS LIGONIŲ KASOS PRIE SVEIKATOS APSAUGOS MINISTERIJOS TVARKOMŲ ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ VALDYMO TVARKOS APRAŠAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Valstybinės ligonių kasos prie Sveikatos apsaugos ministerijos tvarkomų asmens duomenų saugumo pažeidimų valdymo tvarkos aprašas (toliau – Aprašas) nustato pagrindinius reikalavimus, taikomus incidentams, dėl kurių pažeidžiamas Valstybinės ligonių kasos prie Sveikatos apsaugos ministerijos (toliau – VLK) valdomų ir (ar) turimų asmens duomenų saugumas, nustatyti, vertinti, valdyti ir administruoti.

2. Aprašas nustato VLK galimybę vykdyti teisines prievoles, užtikrinti didesnį asmens duomenų saugumą, didinti šių duomenų skaidrumą, informuoti asmenis apie visus reikšmingus su jų asmens duomenimis susijusius incidentus ir užtikrinti kuo mažesnę dėl tokių incidentų padaromą žalą.

3. Pagrindinės Apraše vartojamos sąvokos:

3.1. **Asmens duomenys** – bet kokia informacija apie fizinį asmenį, kurio tapatybė nustatyta arba kurio tapatybę galima nustatyti pagal vardą, 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.

3.2. **Asmens duomenų praradimas** – atvejai, kai asmens duomenys yra išsaugoti, tačiau duomenų valdytojas yra praradęs galimybę šiuos duomenis valdyti ir kontroliuoti arba prieigą prie jų.

3.3. **Asmens duomenų sugadinimas** – atvejai, kai asmens duomenys buvo pakeisti, sugadinti arba yra išnykęs jų vientisumas.

3.4. **Asmens duomenų sunaikinimas** – atvejai, kai asmens duomenų nebėra arba jie yra tokios formos, kuri gali būti tinkama bet kokiam duomenų valdytojo naudojimui.

3.5. **Asmens duomenų tvarkymas** – bet koks automatizuotomis arba neautomatizuotomis priemonėmis su asmens duomenimis ar asmens duomenų rinkiniais atliekamas veiksmas ar jų seka, pavyzdžiui, duomenų rinkimas, įrašymas, rūšiavimas, sisteminimas, saugojimas, adaptavimas ar keitimas, susipažinimas, naudojimas, atskleidimas persiunčiant, platinant ar kitu būdu sudarant galimybę jais naudotis, taip pat sugretinimas ar sujungimas su kitais duomenimis, apribojimas, ištrynimas arba sunaikinimas.

3.6. **Bendrasis duomenų apsaugos reglamentas** – 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB.

3.7. **Duomenų apsaugos pareigūnas** – VLK direktoriaus įsakymu paskirtas asmuo, atsakingas už asmens duomenų apsaugą VLK.

3.8. **Duomenų savininkas** – VLK skyriaus (padalinio) vadovas arba kitas VLK direktoriaus įsakymu paskirtas atsakingas asmuo, kuris, valdydamas veiklos procesų žemėlapiuose nustatytus

procesus, siekdamas savo skyriaus tikslų ir vykdydamas pavestas užduotis, tvarko duomenų subjektų asmens duomenis.

3.9. **Duomenų subjektas** – fizinis asmuo, kurio tapatybė yra nustatyta (gali būti nustatyta) ir kurio duomenis tvarko (valdo) VLK.

3.10. **Duomenų tvarkytojas** – fizinis arba juridinis asmuo (valdžios institucija, agentūra ar kita įstaiga), kuris duomenų valdytojo vardu tvarko asmens duomenis.

3.11. **Informacinės sistemos „Enablor“ (toliau – IS „Enablor“) Incidentų valdymo modulis** – trečiųjų šalių sukurta ir VLK naudojama informacinė sistema, skirta incidentams, dėl kurių pažeidžiamas VLK valdomų ir (ar) turimų asmens duomenų saugumas, fiksuoti, vertinti, valdyti ir administruoti.

3.12. **Priežiūros institucija** – Lietuvos Respublikos valstybinė duomenų apsaugos inspekcija.

3.13. **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.

3.14. **Saugumo pranešimas** – informacinis pranešimas, kuriame pateikiama su saugumo pažeidimu susijusi informacija. Šis pranešimas skirtas Priežiūros institucijai, tam tikrais atvejais – ir duomenų subjektams.

3.15. **VLK darbuotojas (toliau – darbuotojas)** – VLK valstybės tarnautojas ar darbuotojas, dirbantis pagal darbo sutartį.

4. Apraše vartojamos sąvokos atitinka Lietuvos Respublikos įstatymuose, Europos Sąjungos teisės aktuose, įskaitant Bendrąjį duomenų apsaugos reglamentą, vartojamas sąvokas, jei Aprašo 3 punkte nenustatytas kitoks vartojamos sąvokos apibrėžimas.

5. Aprašas taikomas valdant asmens duomenis, tvarkomus elektroniniu būdu, ir asmens duomenis, saugomus neelektronine forma.

II SKYRIUS
SAUGUMO UŽTIKRINIMAS

6. VLK, taikydama tinkamas technines ir organizacines priemones, garantuoja, kad asmens duomenys būtų tvarkomi užtikrinant jų saugumą, įskaitant apsaugą nuo neteisėto duomenų tvarkymo ir atsitiktinio jų sunaikinimo, sugadinimo ar praradimo.

7. VLK, atsižvelgdama į technines galimybes, jų įgyvendinimo sąnaudas ir duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus, taip pat dėl duomenų tvarkymo kylantį pavojų fizinių asmenų teisėms ir laisvėms, įgyvendina reikiamas technines ir organizacines priemones, kad būtų užtikrintas atitinkamo lygio saugumas. Prireikus atliekami šie veiksmai:

7.1. pseudonimų suteikimas asmens duomenims ir jų šifravimas;

7.2. nuolatinis duomenų tvarkymo sistemų ir paslaugų konfidencialumo, vientisumo, prieinamumo ir atsparumo užtikrinimas;

7.3. sąlygų ir galimybių naudotis asmens duomenimis fizinio ar techninio incidento atveju atkūrimas laiku;

7.4. techninių ir organizacinių priemonių, kuriomis užtikrinamas duomenų tvarkymo saugumas, tikrinimas ir reguliarus jų veiksmingumo vertinimas.

8. Nustatydama tinkamą saugumo lygį, VLK įvertina pavojus, kurie gali kilti dėl asmens duomenų tvarkymo, visų pirma – dėl tvarkomų asmens duomenų sunaikinimo, praradimo, pakeitimo, atskleidimo ar neteisėtos prieigos prie jų suteikimo.

III SKYRIUS
SAUGUMO PAŽEIDIMO NUSTATYMAS

9. Saugumo pažeidimu laikomas:

9.1. konfidencialių asmens duomenų atskleidimas leidimo neturintiems asmenims;

9.2. duomenų ir (ar) įrangos, kurioje asmens duomenys saugomi, praradimas ar vagystė;

9.3. dokumentų praradimas ar vagystė;

9.4. netinkamos prieigos kontrolės priemonės, leidžiančios naudotis informacija be leidimo;

9.5. bandymai be leidimo gauti prieigą prie kompiuterių sistemų (pvz., įsibrovimas);

9.6. asmens duomenų pakeitimas ar ištrynimas be duomenų subjekto leidimo;

9.7. virusai ir kitos kibernetinės atakos prieš informacinių technologijų įrangos sistemas ar tinklus;

9.8. fizinio saugumo pažeidimas, pavyzdžiui, saugios patalpos ir (ar) dokumentų spintos, kurioje laikoma konfidenciali informacija, durų ar langų priverstinis atidarymas;

9.9. patalpų ir (ar) dokumentų spintos, kurioje laikoma konfidenciali informacija, neužrakinimas;

9.10. informacinių technologijų įrangos palikimas be priežiūros, neatsijungus nuo naudotojo paskyros ir neužrakinus ekrano;

9.11. elektroninių laiškų, kuriuose yra asmens duomenų ir (ar) neatskleistinos informacijos, išsiuntimas ne tam gavėjui;

9.12. kiti su asmens duomenų konfidencialumo, vientisumo ar prieinamumo pažeidžiamumu susiję atvejai.

10. Situacijos, dėl kurių gali kilti saugumo pažeidimai:

10.1. darbuotojo tarnybinio kompiuterio ar įrenginio praradimas;

10.2. VLK naudojamos programinės įrangos klaida;

10.3. VLK valdomos įrangos techninis gedimas;

10.4. slaptažodžių ar kitų prisijungimo duomenų neleistinas (neteisėtas) prieinamumas ar pažeidimas;

10.5. neteisėtas duomenų atskleidimas;

10.6. įsilaužimas;

10.7. kita.

IV SKYRIUS
SAUGUMO PAŽEIDIMŲ RŪŠYS IR TYRIMAS

11. Saugumo pažeidimai skirstomi pagal tris informacijos saugumo principus į šias rūšis:

11.1. konfidencialumo pažeidimas – kai neteisėtai ar atsitiktiniu būdu atskleidžiami asmens duomenys ir (ar) suteikiama prieiga prie jų;

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

11.3. vientisumo pažeidimas – kai neteisėtai ar netyčia asmens duomenys yra pakeičiami.

12. Pagal aplinkybes saugumo pažeidimas tuo pat metu gali būti laikomas konfidencialumo pažeidimu, prieinamumo pažeidimu bei vientisumo pažeidimu arba bet kokiu šių pažeidimo rūšių deriniu.

13. Tyrimas dėl saugumo pažeidimo pradedamas gavus bet kokios pagrįstos informacijos, leidžiančios manyti, kad buvo pažeistas asmens duomenų saugumas.

14. Kiekvienas darbuotojas, įtaręs, supratęs ar sužinojęs, kad yra padarytas / įvykęs saugumo pažeidimas, privalo nedelsiant, bet ne vėliau kaip per 4 (keturias) valandas nuo įtarimo, supratimo ar sužinojimo apie tokį pažeidimą ir veiksmus, kurių imtasi siekiant pašalinti bei sumažinti galimas neigiamas jo pasekmes, užregistruoti saugos incidentą Naudotojų aptarnavimo tarnybos informacinėje sistemoje (toliau – NAT IS), taip pat elektroniniu paštu arba žodžiu informuoti savo tiesioginį vadovą ir duomenų apsaugos pareigūną (duomenusauga@vlk.lt).

15. Saugumo pažeidimų tyrimą inicijuoja duomenų apsaugos pareigūnas ar kitas darbuotojas ir (ar) duomenų savininkas (kartu vadinami – tyrimą atliekantys darbuotojai). Gavę informacijos apie galimą saugumo pažeidimą, šie asmenys:

15.1. imasi visų reikiamų organizacinių priemonių ir gali duoti nurodymus dėl techninių priemonių naudojimo, kad nedelsiant būtų nustatyta, ar buvo padarytas / įvyko saugumo pažeidimas. Tais atvejais, kai darbuotojas negali identifikuoti, ar buvo padarytas / įvyko saugumo pažeidimas, turi būti pasitelktas kitas reikiamos kompetencijos darbuotojas / kviestinis specialistas;

15.2. inicijuoja komisijos atitinkamam pažeidimui ištirti (toliau – komisija) sudarymą;

15.3. registruoja informaciją apie gautą galimą saugumo pažeidimą IS „Enablor“ Incidentų valdymo modulyje.

16. Komisija arba tyrimą atliekantys darbuotojai:

16.1. turi įvertinti duomenų subjektui kylančią riziką. Laikoma, kad saugumo pažeidimas, galintis kelti pavojų asmenų teisėms ar laisvėms, yra toks, dėl kurio, laiku nesiėmus tinkamų priemonių, duomenų subjektai gali patirti kūno sužalojimus, materialinę ar nematerialinę žalą, pvz., prarasti savo asmens duomenų kontrolę, patirti teisių apribojimą, diskriminaciją, gali būti pavogta ar suklastota jų asmens tapatybė, padaryta finansinių nuostolių, pakenkta reputacijai, prarasta asmens duomenų, kurie laikomi profesine paslaptimi, ar padaryta kita ekonominė ar socialinė žala. Nustatant riziką duomenų subjektui, vadovaujamasi trijų lygių vertinimo skale: 1 lygis – didelė rizika, kad kils pavojus asmenų teisėms ir laisvėms; 2 lygis – vidutinė rizika; 3 lygis – maža rizika;

16.2. turi įvertinti incidento sukeliamos rizikos (keliamo pavojaus asmenų teisėms ar laisvėms) šalinimo (pasekmių eliminavimo) skubumą. Tam įvertinti svarbu atsižvelgti į incidento poveikio mastą, t. y. incidento paveiktų duomenų subjektų skaičių. Įvertinant incidento šalinimo skubumą, vadovaujamasi trijų lygių skubos vertinimo skale: 1 lygis – didelė skuba (reikia imtis priemonių nedelsiant); 2 lygis – vidutinė skuba; 3 lygis – maža skuba.

17. Pagal IS „Enablor“ Incidentų valdymo modulį nustatomas saugumo pažeidimo šalinimo prioritetas (toliau – prioritetas). Prioritetas nustatomas remiantis šia lentele.

Kritiškumas / Skubumas	Didelis 1 lygis	Vidutinis 2 lygis	Mažas 3 lygis
Didelis / 1 lygis	**A**	**B**	**C**
Vidutinis / 2 lygis	**B**	**C**	**D**
Mažas / 3 lygis	**C**	**D**	**E**

18. Prioriteto reikšmių pagal Aprašo 17 punkte pateikiamą lentelę apibūdinimas:

18.1. A – aukščiausio lygio pažeidimas, darantis didžiausią poveikį duomenų subjekto teisėms bei laisvėms ir apimantis didelę duomenų subjektų imtį (didelio masto pažeidimas);

18.2. B – aukšto lygio pažeidimas, darantis 1 arba 2 lygio poveikį duomenų subjekto teisėms bei laisvėms ir apimantis didelę duomenų subjektų imtį (didelio masto pažeidimas);

18.3. C – vidutinio lygio pažeidimas, darantis didelį poveikį duomenų subjekto teisėms bei laisvėms ir turintis įtakos nedidelei duomenų subjektų imčiai arba turintis mažą poveikį duomenų subjekto teisėms ir laisvėms bei apimantis didelę duomenų subjektų imtį (didelio masto pažeidimas);

18.4. D – žemo lygio pažeidimas, darantis mažą arba vidutinį poveikį duomenų subjekto teisėms bei laisvėms ir turintis įtakos nedidelei duomenų subjektų imčiai;

18.5. E – žemiausio lygio pažeidimas, darantis mažą poveikį duomenų subjekto teisėms bei laisvėms ir turintis įtakos nedidelei duomenų subjektų imčiai.

19. Esant bet kokiam saugumo pažeidimui, komisija arba tyrimą atliekantys darbuotojai privalo nedelsdami taikyti būtinas technines ir organizacines saugumo užtikrinimo priemones, kad būtų suvaldytas saugumo pažeidimas ir sumažinti neigiami jo padariniai.

20. Prireikus komisija pasitelkia kitus darbuotojus ar duomenų tvarkytojus.

21. Nustačius aukščiausią kritiškumo lygį ir didelį incidento padarinių šalinimo skubumą, saugumo pažeidimui suteikiamas aukščiausias „A“ pažeidimo šalinimo prioritetas. Tokiu atveju apie (galimą) saugumo pažeidimą turi būti nedelsiant informuojamas VLK direktorius. Prireikus sudaroma komisija incidentui spręsti ir jo pasekmėms šalinti.

22. Komisija (jei yra sudaryta) įvertina, ar būtina pranešti apie saugumo pažeidimą asmens duomenų subjektui (-ams), atsižvelgiant Bendrojo duomenų apsaugos reglamento 34 straipsnio reikalavimus.

23. Duomenų saugos pareigūnas arba VLK direktoriaus įgaliotas asmuo privalo informuoti Priežiūros instituciją Aprašo 5 skyriuje nustatyta tvarka.

24. VLK direktoriaus įgaliotas asmuo arba duomenų savininkas informuoja duomenų subjektą (-us) apie saugumo pažeidimą Aprašo 6 skyriuje nustatyta tvarka. Duomenų subjektai turi būti nedelsiant informuojami tais atvejais, kai saugumo pažeidimas gali kelti didelį pavojų jų teisėms ir laisvėms.

V SKYRIUS
PRIEŽIŪROS INSTITUCIJOS INFORMAVIMAS APIE SAUGUMO PAŽEIDIMĄ

25. Jeigu apie įvykusį saugumo pažeidimą būtina pranešti Priežiūros institucijai, tai atliekama nedelsiant, praėjus ne daugiau kaip 72 (septyniasdešimt dviem) valandoms nuo tada, kai darbuotojas įtarė, suprato ar sužinojo, kad yra padarytas / įvykęs saugumo pažeidimas. Priežiūros institucija apie saugumo pažeidimą informuojama jos nustatytos formos pranešimu (toliau – pranešimas Priežiūros institucijai).

26. Pranešimą Priežiūros institucijai, kuris yra derinamas su duomenų apsaugos pareigūnu, pildo duomenų savininkas.

27. Išimtiniais atvejais, kai duomenų apsaugos pareigūnas kartu su komisija (jei ji yra sudaryta) arba kitas direktoriaus įgaliotas asmuo, ar duomenų savininkas, įvertinę (galimo) saugumo pažeidimo pobūdį ir keliamą riziką, nusprendžia, kad saugumo pažeidimas nekelia ir ateityje nekels pavojaus duomenų subjektų teisėms ir laisvėms, apie tokį saugumo pažeidimą galima nepranešti Priežiūros institucijai.

28. Jeigu Priežiūros institucijai apie saugumo pažeidimą reikia pranešti, bet nepranešama per 72 (septyniasdešimt dvi) valandas nuo tada, kai darbuotojas įtarė, suprato ar sužinojo apie šį pažeidimą, pranešime Priežiūros institucijai turi būti nurodomos vėlavimo priežastys.

29. Pranešime Priežiūros institucijai nurodoma:

29.1. saugumo pažeidimo data ir laikas;

29.2. saugumo pažeidimo pobūdis, taip pat, jei įmanoma, atitinkamų duomenų subjektų kategorijos ir apytikslis jų skaičius bei atitinkamų asmens duomenų įrašų kategorijos ir apytikslis jų skaičius;

29.3. duomenų apsaugos pareigūno vardas, pavardė ir kontaktiniai duomenys;

29.4. tikėtinos saugumo pažeidimo pasekmės;

29.5. priemonės saugumo pažeidimui pašalinti, kurių ėmėsi ar pasiūlė imtis VLK, įskaitant priemones galimoms neigiamoms pasekmėms sumažinti.

30. Jeigu negalima visos Aprašo 29 punkte nurodytos informacijos pateikti Priežiūros institucijai tuo pačiu metu, informacija apie saugumo pažeidimą gali būti nedelsiant teikiama etapais. Informacijos teikimas etapais yra pateisinamas sudėtingesnių pažeidimų atveju (pavyzdžiui, įvykus kai kuriems kibernetinio saugumo incidentams), kai gali būti reikalingas nuodugnus tyrimas, siekiant išsamiai nustatyti saugumo pažeidimo pobūdį ir tai, kokia apimtimi asmens duomenys buvo pažeisti.

31. Pateikus pranešimą Priežiūros institucijai, bet kuriuo metu galima papildomai informuoti šią instituciją apie tolesnio tyrimo metu atskleistus įrodymus, kad saugumo pažeidimo faktiškai nebuvo. Tokiu atveju ši papildoma informacija yra įtraukiama į Priežiūros institucijai pateiktą pirminę informaciją ir incidentas atitinkamai nėra laikomas saugumo pažeidimu.

32. Jeigu įtariama, kad saugumo pažeidimas turi nusikalstamos veikos požymių, VLK direktoriaus įgaliotas darbuotojas informaciją apie galimą nusikalstamą veiką pateikia Lietuvos Respublikos teisėsaugos institucijoms pagal galiojančius teisės aktus.

33. Jeigu padarytas / įvykęs saugumo pažeidimas yra susijęs su kibernetiniu incidentu, VLK direktoriaus įgaliotas darbuotojas informaciją apie kibernetinį incidentą pateikia Lietuvos Respublikos kibernetinio saugumo įstatyme nurodytoms valstybės institucijoms šio įstatymo nustatyta tvarka.

34. Tais atvejais, kai VLK yra kitų trečiųjų asmenų (duomenų valdytojų) duomenų tvarkytoja, vos tik sužinojusi apie saugumo pažeidimą, susijusį su duomenų valdytojų asmens duomenimis, ir įvertinusi tai, kad duomenų valdytojas turi informuoti Priežiūros instituciją (tam

tikrais atvejais ir duomenų subjektus) praėjus ne daugiau kaip 72 (septyniasdešimt dviem) valandoms nuo tada, kai sužinoma apie saugumo pažeidimą, ji privalo nedelsdama informuoti duomenų valdytojus apie (galimai) padarytą / įvykusį saugumo pažeidimą.

VI SKYRIUS
DUOMENŲ SUBJEKTO INFORMAVIMAS APIE SAUGUMO PAŽEIDIMĄ

35. Tais atvejais, kai dėl saugumo pažeidimo gali kilti didelis pavojus duomenų subjektų teisėms ir laisvėms, Aprašo 24 punkte numatyti darbuotojai pateikia pranešimą apie duomenų saugumo pažeidimą (Aprašo priedas) patiems duomenų subjektams (toliau – pranešimas duomenų subjektams), kad šie galėtų imtis visų įmanomų priemonių apsisaugoti nuo neigiamų padarinių.

36. Pranešime duomenų subjektams aiškiai aprašomas duomenų saugumo pažeidimo pobūdis ir pateikiama Aprašo 29.1–29.5 papunkčiuose nurodyta informacija.

37. Pranešimo duomenų subjektams pateikti nereikalaujama, jeigu įvykdomos toliau nurodytos sąlygos:

37.1. jei buvo įgyvendintos tinkamos techninės ir organizacinės apsaugos priemonės ir jos buvo taikytos asmens duomenims, kuriems saugumo pažeidimas turėjo poveikį (pirmiausia tos priemonės, kuriomis užtikrinama, kad asmeniui, neturinčiam leidimo susipažinti su asmens duomenimis, jie būtų nesuprantami, pavyzdžiui, šifravimo priemonės);

37.2. jei iškart po saugumo pažeidimo buvo imtasi priemonių, kuriomis užtikrinama, kad nebekils didelis pavojus duomenų subjektų teisėms ir laisvėms;

37.3. jei duomenų subjektams informuoti prireiktų neproporcingai daug pastangų – tokiu atveju apie saugumo pažeidimą paskelbiama viešai interneto puslapyje arba taikoma panašaus efektyvumo informavimo priemonė (pavyzdžiui, informuojama elektroniniu paštu ar trumposiomis žinutėmis).

38. Jeigu VLK dar nėra pranešusi duomenų subjektams apie saugumo pažeidimą, tačiau Priežiūros institucija, numatydama, kad dėl saugumo pažeidimo kils didelis pavojus, reikalauja tai padaryti, VLK nedelsdama praneša duomenų subjektams apie įvykusį saugumo pažeidimą.

VII SKYRIUS
SAUGUMO PAŽEIDIMŲ DOKUMENTAVIMAS

39. Gavęs pranešimą apie saugumo pažeidimą, duomenų apsaugos pareigūnas IS „Enablor“ Incidentų valdymo modulyje užregistruoja saugumo pažeidimą. Visi saugumo pažeidimai (įskaitant tuos, apie kuriuos neprivaloma pranešti Priežiūros institucijai, o tam tikrais atvejais – ir duomenų subjektams) privalo būti registruojami, nurodant su saugumo pažeidimu susijusius faktus, jų poveikį ir veiksmus, kurių buvo imtasi.

40. Duomenys apie saugumo pažeidimus IS „Enablor“ Incidentų valdymo modulyje registruojami nedelsiant, atlikus Aprašo 16–24 punktuose išvardytus veiksmus. Šie duomenys prireikus turi būti pildomi ir (ar) koreguojami.

41. Tam, kad Priežiūros institucija galėtų patikrinti, ar laikomasi teisės aktų reikalavimų, registruojant saugumo pažeidimą IS „Enablor“ Incidentų valdymo modulyje reikia įvesti šiuos duomenis:

41.1. duomenis apie saugumo pažeidimą;

41.2. duomenis apie saugumo pažeidimo pasekmių šalinimą;

41.3. kitus svarbius duomenis.

42. Darbuotojai informuojami apie saugumo pažeidimo dokumentavimo būtinumą ir privalo nurodyti reikiamą informaciją, registruodami saugos incidentą NAT IS.

43. IS „Enablor“ Incidentų valdymo modulyje padaryti įrašai yra periodiškai peržiūrimi. Prireikus numatomos atitinkamos prevencijos priemonės ir jų vykdymo kontrolė, siekiant, kad ateityje saugumo pažeidimai nesikartotų.

44. IS „Enablor“ Incidentų valdymo modulyje daromi įrašai saugomi 5 (penkerius) metus.

VIII SKYRIUS
BAIGIAMOSIOS NUOSTATOS

45. Jei dėl saugumo pažeidimo laiku nesiimama tinkamų priemonių, duomenų subjektai gali patirti materialinę ar nematerialinę žalą, pavyzdžiui, prarasti savo asmens duomenų kontrolę, patirti teisių apribojimą, diskriminaciją, gali būti pavogta ar suklastota asmens tapatybė, padaryta finansinių nuostolių, neleistinai panaikinti pseudonimai, pakenkta jų reputacijai, prarastas asmens duomenų, kurie laikomi profesine paslaptimi, konfidencialumas arba padaryta kita ekonominė ar socialinė žala.

46. Aprašo nuostatų nesilaikymas traktuojamas kaip darbo pareigų pažeidimas, už kurį darbuotojui gali būti taikoma atsakomybė.

47. Aprašas peržiūrimas ne rečiau kaip kartą per 2 (dvejus) metus arba pasikeitus teisės aktams.

48. Aprašo nuostatų privalo laikytis visi darbuotojai.

_____

Valstybinės ligonių kasos prie Sveikatos apsaugos ministerijos tvarkomų asmens duomenų saugumo pažeidimų valdymo tvarkos aprašo
priedas

(Pranešimo apie duomenų saugumo pažeidimą forma)

PRANEŠIMAS APIE DUOMENŲ SAUGUMO PAŽEIDIMĄ

_____
(Data)

Gerb._____,
(duomenų subjektas)

apgailestaudami pranešame, kad Valstybinėje ligonių kasoje prie Sveikatos apsaugos ministerijos (VLK) įvyko asmens duomenų saugumo pažeidimas ir tam tikri Jūsų asmens duomenys buvo (arba galėjo būti) neleistinai pasiekiami, nukopijuoti ar kitu būdu pažeisti. Stengiamės kuo labiau sumažinti šio asmens duomenų saugumo pažeidimo pasekmes ir nustatyti jo priežastį.

Vadovaudamiesi Bendrojo duomenų apsaugos reglamento (ES) 2016/679 34 straipsniu, informuojame Jus apie įvykusį duomenų saugumo pažeidimą ir pateikiame visą su juo susijusią informaciją:

1. Asmens duomenų saugumo pažeidimo data ir laikas (laikas gali būti nurodomas minučių tikslumu):
2. Asmens duomenų saugumo pažeidimo pobūdis: (Pvz., neleistina prieiga prie VLK duomenų bazės, kurioje saugomi klientų kontaktiniai duomenys).
3. Galima asmens duomenų saugumo pažeidimo priežastis: (Pvz., tiriama, darbuotojo klaida ar pan.).
4. Jūsų asmens duomenys, kurie buvo ar galėjo būti neleistinai pasiekiami, nukopijuoti ar kitaip pažeisti: (pvz.: 1. vardas; 2. pavardė; 3. gimimo data ir pan.).
5. Galimos asmens duomenų saugumo pažeidimo pasekmės: (Pvz., leidimo neturinčios trečiosios šalys pažeidė (galėjo pažeisti) asmens duomenis, su jais susipažinti, juos nukopijuoti ar pan.).
6. Priemonės, kurių imtasi siekiant sumažinti galimą žalą ir pašalinti asmens duomenų saugumo pažeidimą: (Pvz., siekdami pašalinti šį asmens duomenų saugumo pažeidimą, pradėjome vidinį tyrimą, kurį atlikus bus nustatyta pažeidimo priežastis. Taip pat ėmėmės šių techninių priemonių: ..... .)
7. Rekomenduojame Jums imtis šių priemonių: (Pvz., pakeiskite savo slaptažodį ir kitus prisijungimo prie mūsų duomenų bazės / sistemos duomenis).

Visais klausimais dėl asmens duomenų saugumo pažeidimo kreipkitės į nurodytą atsakingąjį asmenį (vardas, pavardė, kontaktinis telefono numeris, elektroninio pašto adresas) arba duomenų apsaugos pareigūną elektroninio pašto adresu duomenusauga@vlk.lt.

Imamės visų priemonių, kad užtikrintume Jūsų privatumą ir duomenų apsaugą.

_____
(Paskirto kontaktinio asmens / duomenų apsaugos pareigūno vardas, pavardė, pareigos)

_____

Nuorašas tikras
Valstybinė ligonių kasa prie Sveikatos apsaugos ministerijos
2025-04-22

DETALŪS METADUOMENYS	
Dokumento sudarytojas (-ai)	Valstybinė ligonių kasa prie Sveikatos apsaugos ministerijos
Dokumento pavadinimas (antraštė)	DĖL VALSTYBINĖS LIGONIŲ KASOS PRIE SVEIKATOS APSAUGOS MINISTERIJOS DIREKTORIAUS 2021 M. KOVO 23 D. ĮSAKYMO NR. 1K-94 „DĖL VALSTYBINĖS LIGONIŲ KASOS PRIE SVEIKATOS APSAUGOS MINISTERIJOS IR TERITORINIŲ LIGONIŲ KASŲ TVARKOMŲ ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ
Dokumento registracijos data ir numeris	2025-04-22 Nr. 1K-179
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	Gytis Bendorius, direktorius, ADMINISTRACIJA
Parašo sukūrimo data ir laikas	2025-04-22 09:44:06
Parašo formatas	XAdES-T
Laiko žymoje nurodytas laikas	2025-04-22T09:44:11+03:00
Informacija apie sertifikavimo paslaugų teikėją	EID-SK 2016, AS Sertifitseerimiskeskus
Sertifikato galiojimo laikas	2023-10-26 14:24:42 - 2026-10-26 14:24:42
Parašo paskirtis	Registravimas
Parašą sukūrusio asmens vardas, pavardė ir pareigos	Dokumentų valdymo sistema, DVS System, Valstybinė ligonių kasa, į.k. 191351679
Parašo sukūrimo data ir laikas	2025-04-22 10:10:35
Parašo formatas	XAdES
Laiko žymoje nurodytas laikas	-
Informacija apie sertifikavimo paslaugų teikėją	RCSC IssuingCA-2, VI Registru Centras - i.k. 124110246
Sertifikato galiojimo laikas	2024-12-11 08:40:07 - 2025-12-11 08:40:07
Informacija apie būdus, naudotus metaduomenų vientisumui užtikrinti	"Registravimas" paskirties metaduomenų vientisumas užtikrintas naudojant "RCSC IssuingCA-2, VI Registru Centras - i.k. 124110246" išduotą sertifikatą "CN=Dokumentų valdymo informacinė sistema, O="Valstybinė ligonių kasa, į.k. 191351679", L=Vilnius, S=Lietuva, C=LT", kuris galioja nuo 2024-12-11 08:40:07 iki 2025-12-11 08:40:07
Pagrindinio dokumento priedų skaičius	1
Pagrindinio dokumento pridedamų dokumentų skaičius	0

Pridedamo dokumento sudarytojas (-ai)	-
Pridedamo dokumento pavadinimas (antraštė)	-
Pridedamo dokumento registracijos data ir numeris	-
Programinės įrangos, kuria naudojantis sudarytas elektroninis dokumentas, pavadinimas	Elpako v.20250417.1
Informacija apie elektroninio dokumento ir elektroninio (-ių) parašo (-ų) tikrinimą (tikrinimo data)	Atitinka specifikacijos keliamus reikalavimus. Visi dokumente esantys elektroniniai parašai galioja (2025-04-22 10:11:52)
Elektroninio dokumento nuorašo atspausdinimo data ir ją atspausdinęs darbuotojas	2025-04-22 10:11:52 nuorašą suformavo VLK Dokumentų valdymo sistema
Paieškos nuoroda	–
Papildomi metaduomenys	-