PATVIRTINTA
Viešosios įstaigos Kauno miesto
greitosios pagalbos stoties
direktoriaus
2022 m. kovo 2 d.
įsakymu Nr. V-62

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ VALDYMO TAISYKLĖS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Asmens duomenų saugumo pažeidimų valdymo taisyklės (toliau – Taisyklės) nustato asmens duomenų saugumo pažeidimų (toliau – pažeidimas) ir jų priežasčių klasifikavimą, pranešimo apie pažeidimus viešajai įstaigai Kauno miesto greitosios medicinos pagalbos stočiai (toliau – Kauno m. GMPS), Valstybinei duomenų apsaugos inspekcijai (toliau – Inspekcija) ir duomenų subjektams, pažeidimų tyrimo, jų ir jų pasekmių pašalinimo ir mažinimo, pažeidimų prevencijos ir dokumentavimo tvarką.

2. Taisyklės taikomos Kauno m. GMPS, registrų bei valstybės informacinių sistemų, kurių duomenų valdytojas yra Kauno m. GMPS, duomenų tvarkytojams bei juridiniams asmenims, su kuriais sudaryta asmens duomenų tvarkymo sutartis tvarkyti asmens duomenis pagal Kauno m. GMPS nurodymus (toliau kartu – duomenų tvarkytojai).

3. Taisyklės parengtos atsižvelgiant į 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) (OL 2016 L 119, p. 1) (toliau – Reglamentas (ES) 2016/679).

4. Taisyklėse vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos Reglamente (ES) 2016/679 ir Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme.

II SKYRIUS
PAŽEIDIMŲ IR JŲ PRIEŽASČIŲ KLASIFIKAVIMAS

5. Pažeidimai pagal pobūdį (tipą) yra:

5.1. konfidencialumo pažeidimas – netyčinis arba neteisėtas asmens duomenų laikinas ar nuolatinis atskleidimas ar prieigos prie asmens duomenų suteikimas asmenims, kurie neturi teisės susipažinti su asmens duomenimis;

5.2. prieinamumo pažeidimas – neteisėtas, laikinas ar nuolatinis prieigos prie asmens duomenų praradimas arba asmens duomenų sunaikinimas;

5.3. vientisumo pažeidimas – neteisėtas asmens duomenų laikinas ar nuolatinis pakeitimas;

5.4. mišraus pobūdžio (tipo) pažeidimas – asmens duomenų konfidencialumo, prieinamumo ir vientisumo pažeidimas ar bet kurių Taisyklių 5.1–5.3 papunkčiuose nurodytų pažeidimų derinys.

6. Pažeidimai gali būti nulemti šių priežasčių:

6.1. netyčiniai veiksmai, kai asmens duomenų saugumas pažeidžiamas neturint tikslo tai padaryti (dėl duomenų tvarkymo klaidos, informacijos laikmenų, duomenų įrašų ištrynimo, sunaikinimo ar sistemų sutrikimų dėl elektros tiekimo nutrūkimo, įvykusio dėl asmens veiklos, kompiuterinio viruso, paskleisto dėl asmens veiklos, vidaus taisyklių pažeidimo, sistemos priežiūros trūkumo, programinės įrangos testų atlikimo, netinkamos duomenų laikmenų priežiūros, netinkamo ryšio linijų pajėgumo ir apsaugos nustatymo, kompiuterių integravimo į tinklą, netinkamos kompiuterinių programų apsaugos parinkimo ir kt.);

6.2. tyčiniai veiksmai, kai asmens duomenų saugumas pažeidžiamas sąmoningai turint tikslą tai padaryti (neteisėtas įsibrovimas į asmens duomenų tvarkytojo patalpas, asmens duomenų

laikmenų saugyklas, informacines sistemas, kompiuterių tinklą, tyčinis nustatytų taisyklių tvarkant asmens duomenis pažeidimas, sąmoningas kompiuterinio viruso platinimas, asmens duomenų vagystė, neteisėtas naudojimasis kito Kauno m. GMPS darbuotojo teisėmis ir kt.);

6.3. *force majeure* ir kiti netikėti įvykiai, kurių negalima kontroliuoti, numatyti ir užkirsti kelio jų atsiradimui (žaibas, gaisras, potvynis, užliejimas, audros, elektros instaliacijos degimas, temperatūros ir (ar) drėgmės pakitimų poveikis, purvo, dulkių ir magnetinių laukų įtaka, techninės avarijos, išskyrus nurodytas Taisyklių 6.1 papunktyje, ir kt.).

III SKYRIUS
PRANEŠIMAS APIE GALIMĄ PAŽEIDIMĄ IR JO NAGRINĖJIMAS

7. Kauno m. GMPS, sužinojęs ar pats nustatęs galimą pažeidimą arba kai informacija apie galimą pažeidimą gaunama iš duomenų tvarkytojo, žiniasklaidos ar kito šaltinio (toliau – galimo pažeidimo paaiškėjimas), privalo:

7.1. nedelsiant, bet ne vėliau kaip per 2 darbo valandas nuo galimo pažeidimo paaiškėjimo momento informuoti žodžiu, raštu ar elektroninėmis priemonėmis savo tiesioginį vadovą, Kauno m. GMPS saugos įgaliotinį ir Kauno m. GMPS duomenų apsaugos pareigūną;

7.2. užpildyti Taisyklių 1 priede nustatytos formos pranešimą apie galimą asmens duomenų saugumo pažeidimą ir nedelsiant, bet ne vėliau kaip per 4 darbo valandas nuo galimo pažeidimo paaiškėjimo momento perduoti jį Kauno m. GMPS saugos įgaliotiniui ir jo kopiją – duomenų apsaugos pareigūnui;

7.3. jei įmanoma, imtis priemonių pašalinti galimą pažeidimą ir priemonių galimoms neigiamoms jo pasekmėms sumažinti.

8. Duomenų tvarkytojas paaiškėjus galimam pažeidimui privalo:

8.1. nedelsdamas, bet ne vėliau kaip per 24 valandas nuo galimo pažeidimo paaiškėjimo momento, apie tai pranešti Kauno m. GMPS, raštu pateikdamas pranešimą, kuriame nurodyta Reglamento (ES) 2016/679 33 straipsnio 3 dalyje nustatyta informacija, kiek tos informacijos įmanoma pateikti tuo metu, taip pat teikti Kauno m. GMPS šiame punkte nurodytą informaciją, jei ji nebuvo pateikta per šiame punkte nurodytą terminą nedelsiant po jos paaiškėjimo;

8.2. Taisyklių V skyriuje nustatytais atvejais ir tvarka Kauno m. GMPS vardu pranešti apie galimą pažeidimą Inspekcijai ir Taisyklių VI skyriuje nustatytais atvejais ir tvarka – duomenų subjektams;

8.3. kai asmens duomenų, tvarkomų registruose ir valstybinėse informacinėse sistemose, kurių duomenų valdytojas yra Kauno m. GMPS, arba pagal Kauno m. GMPS nurodymus, galimas saugumo pažeidimas yra susijęs su kibernetiniu incidentu, informaciją apie galimą pažeidimą kartu su informacija apie kibernetinį incidentą pateikti Lietuvos Respublikos kibernetinio saugumo įstatyme (toliau – Kibernetinio saugumo įstatymas) nurodytoms valstybės institucijoms Kibernetinio saugumo įstatymo nustatyta tvarka ir atvejais;

8.4. kuo greičiau imtis priemonių pašalinti pažeidimus ir (ar) sumažinti ar pašalinti jų pasekmes, siekiant atkurti padėtį, kuri buvo prieš pažeidimą;

8.5. bendradarbiauti su Kauno m. GMPS tiriant pažeidimą ir per Kauno m. GMPS nurodytą terminą teikti Kauno m. GMPS visą jos prašomą informaciją, susijusią su informavimu apie pažeidimą ir jo tyrimu.

9. Kauno m. GMPS saugos įgaliotinis gavęs Taisyklių 7.2 ar 8.1 papunktyje nurodytą pranešimą (toliau kartu – pranešimas) privalo:

9.1. atlikti pažeidimo tyrimą Taisyklių IV skyriaus nustatyta tvarka;

9.2. pasitelkti Kauno m. GMPS darbuotojus pagal kompetenciją (asmens duomenų, tvarkomų Kauno m. GMPS, saugumo pažeidimo atveju) ar duomenų tvarkytojų darbuotojus pagal kompetenciją (asmens duomenų, tvarkomų registruose ir valstybės informacinėse sistemose, kurių duomenų valdytojas yra Kauno m. GMPS saugumo pažeidimo ir asmens duomenų, tvarkomų pagal Kauno m. GMPS nurodymus, saugumo pažeidimo atveju), jei pažeidimas yra susijęs su elektroninės informacijos saugos ir (ar) kibernetiniu incidentu;

9.3. asmens duomenų, tvarkomų Kauno m. GMPS, saugumo galimo pažeidimo atveju, kai galimas pažeidimas yra susijęs su kibernetiniu incidentu, informaciją apie galimą pažeidimą kartu su informacija apie kibernetinį incidentą pateikti Kibernetinio saugumo įstatyme nurodytoms valstybės institucijoms Kibernetinio saugumo įstatymo nustatyta tvarka ir atvejais;

9.4. teikti rekomendacijas Kauno m. GMPS darbuotojams, atsakingiems už pažeidimo ir (ar) jo pasekmių pašalinimą ir (ar) sumažinimą, ir (ar) duomenų tvarkytojui dėl tinkamų techninių ir organizacinių priemonių, kad pažeidimas būtų išsamiai ištirtas ir jis ir (ar) jo pasekmės būtų pašalintos ir (ar) sumažintos ir pažeidimas ateityje nepasikartotų, taikymo ir (arba) pats imtis šių veiksmų.

10. Kauno m. GMPS duomenų apsaugos pareigūnas, gavęs pranešimą privalo:

10.1. informaciją apie galimą pažeidimą fiksuoti Asmens duomenų saugumo pažeidimų registracijos žurnale (Taisyklių 2 priedas) (toliau – Žurnalas);

10.2. saugos įgaliotiniui ir Kauno m. GMPS direktoriui patarti dėl pažeidimo tyrimo ir teikti išvadas dėl pranešimų Inspekcijai ir (ar) duomenų subjektui;

10.3. bendradarbiauti su Inspekcija dėl pažeidimų;

10.4. stebėti, kaip vykdomos Reglamente (ES) 2016/679 ir Taisyklėse nustatytos Kauno m. GMPS pareigos, susijusios su pažeidimų valdymu.

11. Kai yra įtariama, kad pažeidimas turi nusikalstamos veikos požymių, informacija apie galimą nusikalstamą veiką pateikiama valstybės institucijoms, įgaliotoms atlikti ikiteisminį tyrimą, teisės aktų, reguliuojančių tokios informacijos teikimą, nustatyta tvarka. Asmens duomenų, tvarkomų registruose ir valstybinėse informacinėse sistemose, kurių duomenų valdytojas yra Kauno m. GMPS, arba pagal Kauno m. GMPS nurodymus, saugumo pažeidimo atveju tokį pranešimą pateikia duomenų tvarkytojas, o asmens duomenų, tvarkomų Kauno m. GMPS, saugumo pažeidimo atveju – saugos įgaliotinis.

IV SKYRIUS
PAŽEIDIMO TYRIMAS

12. Saugos įgaliotinis nedelsiant, bet ne vėliau kaip per 24 valandas nuo pranešimo gavimo momento, išnagrinėja pranešime nurodytas aplinkybes, įvertina, ar padarytas pažeidimas, jei pažeidimas padarytas, nustato, kokio pobūdžio (tipo) pažeidimas padarytas, asmens duomenų, kurių saugumas pažeistas, kategorijas, įskaitant specialių kategorijų asmens duomenis, pažeidimo priežastis, pažeidimo apimtis (duomenų subjektų kategorijos ir jų skaičius), esamas ir (ar) galimas pasekmes ir žalą, padarytą duomenų subjektui (-ams), įvertina pavojų duomenų subjekto teisėms ir laisvėms (toliau – rizika), kuris gali atsirasti dėl galimo pažeidimo, Taisyklių 14-15 punktuose nustatyta tvarka ir pateikia Kauno m. GMPS duomenų apsaugos pareigūnui ir Kauno GMPS direktoriui (ar jo įgaliotam asmeniui) išvadą dėl pažeidimo buvimo ir rizikos.

13. Pažeidimo tyrimo metu darbuotojai ir duomenų tvarkytojas privalo operatyviai teikti saugos įgaliotiniui visą jo paprašytą su pažeidimu susijusią informaciją ir dokumentus.

14. Rizika vertinama objektyviai įvertinus pažeidimo aplinkybes ir atsižvelgiant į:

14.1. pažeidimo pobūdį (tipą);

14.2. asmens duomenų pobūdį, kategoriją (pvz., specialių kategorijų asmens duomenys), asmens duomenų, kurių saugumas pažeistas pažeidimu, apimtį;

14.3. duomenų subjekto identifikavimo galimybę tiesiogiai ar netiesiogiai pasinaudojant pažeidimo objektu esančiais duomenimis;

14.4. padarinių duomenų subjektui sunkumą. Vertinant riziką turi būti laikoma, kad pažeidimas, galintis kelti pavojų duomenų subjektų teisėms ir laisvėms, yra toks, dėl kurio, laiku nesiėmus tinkamų priemonių, kyla grėsmė duomenų subjektų sveikatai ir (ar) gyvybei ar grėsmė patirti 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.

14.5. Preziumuojama, kad pažeidimas kelia riziką, kai pažeidimas yra susijęs su specialių kategorijų asmens duomenimis:

14.5.1. duomenų subjekto savybes (pvz., vaikas ar kitas pažeidžiamas asmuo);

14.5.2. duomenų subjektų, kurių asmens duomenų saugumas buvo pažeistas, skaičių;

14.5.3. duomenų valdytojo savybes (pvz., veiklos pobūdį).

15. Įvertinus riziką nustatoma, kad yra:

15.1 maža rizika, kai nustatoma, kad pavojaus duomenų subjekto teisėms ir laisvėms nėra;

15.2 vidutinė rizika, kai nustatoma, kad dėl asmens duomenų saugumo pažeidimo yra / gali kilti nedidelis pavojus duomenų subjektų teisėms ir laisvėms;

15.3 didelė rizika, kai nustatoma, kad dėl asmens duomenų saugumo pažeidimo yra/gali kilti didelis pavojus duomenų subjektų teisėms ir laisvėms.

16. Jeigu per 24 val. nuo pranešimo gavimo momento dėl objektyvių priežasčių nebuvo nustatytos visos aplinkybės, nurodytos Taisyklių 14 punkte, saugos įgaliotinis atlieka tolesnį pažeidimo tyrimą. Šiame punkte nurodytas tyrimas turi būti atliktas ir Taisyklių 3 priede nustatytos formos Asmens duomenų saugumo pažeidimo ataskaita (toliau – Ataskaita) parengta ir pateikta Kauno m. GMPS direktoriui, duomenų apsaugos pareigūnui ir duomenų tvarkytojo vadovui, jei tai susiję su duomenų tvarkytojo atliekamais asmens duomenų tvarkymo veiksmais, ne vėliau kaip per 20 darbo dienų nuo pažeidimo paaiškėjimo dienos.

17. Jeigu išvadoje dėl pažeidimo buvimo ir rizikos nurodyta, kad rizikos nėra, tačiau Taisyklių 16 punkte nurodyto pažeidimo tyrimo metu nustatoma, kad rizika gali kilti, arba jo metu pasikeitė rizikos laipsnis, saugos įgaliotinis turi riziką vertinti iš naujo Taisyklių 14–16 punktuose nustatyta tvarka.

V SKYRIUS
PRANEŠIMAS INSPEKCIJAI

18. Taisyklių 15.2 ir 15.3 papunkčiuose nurodytais atvejais asmens duomenų, tvarkomų Kauno m. GMPS, saugumo pažeidimo atveju Kauno m. GMPS, o asmens duomenų, tvarkomų registruose ir valstybės informacinėse sistemose, kurių duomenų valdytojas yra Kauno m. GMPS, arba pagal Kauno m. GMPS nurodymus, saugumo pažeidimo atveju Kauno m. GMPS vardu duomenų tvarkytojas, ne vėliau kaip per 72 valandas nuo galimo pažeidimo paaiškėjimo momento, Inspekcijos nustatyta tvarka ir sąlygomis praneša apie pažeidimą Inspekcijai (toliau – pranešimas Inspekcijai) ir pranešimo Inspekcijai kopiją pateikia Kauno m. GMPS.

19. Kai sužinojus apie galimai įvykusį pažeidimą nėra objektyvių galimybių per 72 valandas nustatyti, ar pažeidimas tikrai įvyko, Inspekcijai per 72 valandas nuo sužinojimo apie galimai įvykusį pažeidimą pateikti pranešimą apie pažeidimą, nurodant tiek informacijos, kiek tuo metu yra žinoma. Jeigu, įvertinus riziką, abejojama, ar ji yra ir ar reikia pranešti apie Pažeidimą Inspekcijai, būtina pranešti.

20. Duomenų apsaugos pareigūnas per 24 val. nuo saugos įgaliotinio išvados dėl pažeidimo buvimo ir rizikos gavimo momento, pateikia išvadą Kauno m. GMPS direktoriui (ar jo įgaliotam asmeniui) dėl pranešimo apie pažeidimą Inspekcijai bei Taisyklių 15.2 ir 15.3 papunkčiuose nurodytais atvejais parengia pranešimo dėl asmens duomenų, tvarkomų Kauno m. GMPS, saugumo pažeidimo projektą, išskyrus 18 punkte nurodytą atvejį, kai pranešimą Inspekcijai Kauno m. GMPS vardu pateikia duomenų tvarkytojas.

21. Kauno m. GMPS direktorius (ar jo įgaliotas asmuo) per 24 val. nuo Taisyklių 20 punkte nurodytos Kauno m. GMPS duomenų apsaugos pareigūno išvados gavimo momento priima sprendimą dėl pranešimo teikimo Inspekcijai ir informuoja apie priimtą sprendimą saugos įgaliotinį ir duomenų apsaugos pareigūną. Jeigu abejojama dėl rizikos priskyrimo Taisyklių 15.2 ar 15.3 papunkčiuose nurodytam rizikos lygiui, apie pažeidimą Inspekcijai pranešama.

22. Jeigu atliekamas Taisyklių 16 punkte nurodytas tyrimas, Inspekcijai informacija gali būti teikiama etapais. Apie informacijos teikimą etapais Kauno m. GMPS arba duomenų tvarkytojas Inspekciją informuoja pranešime Inspekcijai.

23. Jeigu po pranešimo Inspekcijai pateikimo, atlikus Taisyklių 16 punkte nurodytą tolesnį tyrimą, yra nustatoma, kad saugumo incidentas buvo sustabdytas ir nebuvo pažeidimo, apie tai ne vėliau kaip per 3 darbo dienas nuo šios informacijos paaiškėjimo momento Kauno m. GMPS arba duomenų tvarkytojas informuoja Inspekciją ir pažymi Žurnale.

VI SKYRIUS
PRANEŠIMAS DUOMENŲ SUBJEKTUI

24. Taisyklių 15.3 papunktyje nurodytu atveju asmens duomenų, tvarkomų Kauno m. GMPS, saugumo pažeidimo atveju Kauno m. GMPS, o asmens duomenų, tvarkomų registruose ir valstybės informacinėse sistemose, kurių duomenų valdytojas yra Kauno m. GMPS, arba pagal Kauno m. GMPS nurodymus, saugumo pažeidimo atveju Kauno m. GMPS vardu duomenų tvarkytojas privalo nedelsdamas (rekomenduojama per 72 val. nuo galimo pažeidimo paaiškėjimo momento) apie tai raštu pranešti duomenų subjektui, kurio teisėms ir laisvėms dėl šio pažeidimo kyla didelė rizika. Pranešimas rengiamas ir teikiamas šio skyriaus ir Taisyklių 18–21 punktuose *mutatis mutandis* nustatyta tvarka.

25. Pranešime duomenų subjektui aiškia ir paprasta kalba pateikiama:

25.1. pažeidimo pobūdžio aprašymas;

25.2. duomenų tvarkytojo duomenų apsaugos pareigūno arba kito kontaktinio asmens vardas, pavardė (pavadinimas) ir kontaktiniai duomenys;

25.3. galimų pažeidimo pasekmių aprašymas;

25.4. priemonių, kurių ėmėsi Kauno m. GMPS ir (ar) duomenų tvarkytojas arba siūlo imtis duomenų subjektui, kad būtų pašalintas pažeidimas ir (ar) pašalintos ar sumažintos galimos neigiamos jo pasekmės, aprašymas (pvz., kad apie pažeidimą yra informuota Inspekcija ir kad yra gautas patarimas dėl pažeidimo pasekmių pašalinimo ar sumažinimo; siūlymas duomenų subjektui pasikeisti slaptažodžius ir kt.);

25.5 kita reikšminga informacija, susijusi su pažeidimu, kuri, Kauno m. GMPS ar duomenų tvarkytojo manymu, turėtų būti pateikta duomenų subjektui.

26. Pranešimo pateikimo būdas pasirenkamas atsižvelgiant į tai, kokius duomenų subjekto kontaktinius duomenis tvarko Kauno m. GMPS ir (ar) duomenų tvarkytojas, ir į tai, kuris būdas geriausiai užtikrintų, kad pranešimas pasiektų adresatą. Šis pranešimas turi būti atskirtas nuo kitos siunčiamos informacijos, tokios kaip nuolatiniai atnaujinimai, naujienlaiškiai ar standartiniai pranešimai. Gali būti taikomi keli pranešimo duomenų subjektui apie pažeidimą būdai.

27. Pranešimas duomenų subjektui apie pažeidimą neteikiamas, išskyrus, jei teikti pranešimą reikalauja Inspekcija, šiais atvejais:

27.1. Kauno m. GMPS ir (ar) duomenų tvarkytojas įgyvendino tinkamas technines ir organizacines asmens duomenų apsaugos priemones, kurios užtikrino, kad įvykus pažeidimui nekils rizika, ir tos priemonės taikytos asmens duomenims, kuriems pažeidimas turėjo poveikio (pvz., asmens duomenys buvo šifruoti);

27.2. iš karto po pažeidimo Kauno m. GMPS ir (ar) duomenų tvarkytojas ėmėsi priemonių, kuriomis užtikrinama, kad nebegalėtų kilti rizika;

27.3. reikėtų neproporcingai daug pastangų susisiekti su duomenų subjektais (pvz., kai jų kontaktiniai duomenys buvo prarasti dėl pažeidimo arba nežinomi). Tokiu atveju Taisyklių 25 punkte nurodyta informacija apie pažeidimą paskelbiama viešai arba taikoma panaši priemonė, kuria duomenų subjektai būtų informuojami taip pat efektyviai, pvz., pranešimas interneto svetainėje, spaudoje ar pan.

28. Jeigu Kauno m. GMPS ar duomenų tvarkytojas pranešimo duomenų subjektui apie pažeidimą neteikė, asmens duomenų tvarkomų Kauno m. GMPS, saugumo pažeidimo atveju Kauno m. GMPS, o asmens duomenų, tvarkomų registruose ir valstybės informacinėse sistemose, kurių

duomenų valdytojas yra Kauno m. GMPS, arba pagal Kauno m. GMPS nurodymus, saugumo pažeidimo atveju Kauno m. GMPS vardu duomenų tvarkytojas turi pagrįsti Inspekcijai, kad įvykdė vieną iš Taisyklių 27 punkte nurodytų sąlygų.

VII SKYRIUS
ŽURNALO DUOMENŲ TVARKYMAS

29. Kauno m. GMPS ir duomenų tvarkytojai tvarko atskirus Žurnalus.

30. Žurnale nurodoma:

30.1. Visi su pažeidimu susiję faktai – pažeidimo priežastis, kas įvyko ir kokie asmens duomenys pažeisti;

30.2. pažeidimo poveikis ir pasekmės;

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

30.3. su pažeidimu susijusių sprendimų priėmimo priežastys (pvz., kodėl duomenų valdytojas nusprendė nepranešti apie pažeidimą Inspekcijai ir (ar) duomenų subjektui, t. y. kodėl nusprendė, kad rizika žema, arba kokią Taisyklių 27 punkte nurodytą sąlygą įvykdė);

30.4. pranešimo Inspekcijai pateikimo vėlavimo priežastys (jeigu pranešimą vėluojama pateikti ar pranešimas teikiamas etapais);

30.5. informacija, susijusi su pranešimu duomenų subjektui (pvz., ar buvo pranešta, kodėl nepranešta ir pan.);

30.6. kita reikšminga informacija, susijusi su pažeidimu (pvz., kad tyrimo metu nustatyta, jog Pažeidimo nebuvo, o buvo tik saugumo incidentas).

31. Už Žurnalo pildymą ir saugojimą atsakingas duomenų apsaugos pareigūnas. Žurnale registruojami visi pažeidimai, nepaisant to, ar apie juos pranešta Inspekcijai ir (ar) duomenų subjektui, ar tokie pažeidimai kelia riziką. Žurnalas yra elektroninės formos, pildomas dokumentų valdymo sistemoje. Užpildytas Žurnalas saugomas 5 metus nuo paskutinio įrašo Žurnale padarymo.

32. Informacija apie pažeidimą į Žurnalą turi būti įvedama nedelsiant, kai tik paaiškėja galimas pažeidimas, bet ne ilgiau kaip per 5 darbo dienas nuo galimo pažeidimo paaiškėjimo momento. Kai pasikeičia Žurnale nurodyta informacija arba paaiškėja nauja informacija, Žurnale esanti informacija turi būti papildoma ir (ar) koreguojama.

33. Žurnalas yra pateikiamas Inspekcijai jai pareikalavus.

34. Duomenų apsaugos pareigūnas kartą per ketvirtį peržiūri Žurnale esančius įrašus ir pasiūlo Kauno m. GMPS direktoriui, kokios prevencijos priemonės turėtų būti įgyvendintos bei kaip turėtų būti kontroliuojamas šių prevencijos priemonių įdiegimas, kad ateityje tokie patys pažeidimai nesikartotų.

VIII SKYRIUS
BAIGIAMOSIOS NUOSTATOS

35. Kauno m. GMPS darbuotojai ir duomenų tvarkytojai privalo išsaugoti esamos situacijos, susijusios su galimu pažeidimu, įrodymus, kad vėliau naudojant technines ir organizacines priemones (pvz., duomenų srauto ir prisijungimų analizės įrankius ar kt.) galima būtų tirti pažeidimą.

36. Prireikus Kauno m. GMPS gali būti sudaryta komisija tirti pažeidimus (įskaitant jų priežastis, pasekmes) bei teikti pasiūlymus Kauno m. GMPS direktoriui dėl pažeidimų išvengimo ateityje.

37. Atsižvelgęs į Ataskaitą Kauno m. GMPS direktorius prireikus tvirtina priemonių planą, kuriame numatomos būtinos techninės, organizacinės, administracinės ir kitos priemonės, reikalingos užkirsti kelią pažeidimams, jų pasekmėms pašalinti ar sumažinti, atsakingi priemonių vykdytojai ir įgyvendinimo terminai.

_____

Asmens duomenų saugumo pažeidimų
valdymo taisyklių
1 priedas

(Pranešimo apie galimą asmens duomenų saugumo pažeidimą forma)

VIEŠOJI ĮSTAIGA KAUNO MIESTO GREITOSIOS MEDICINOS PAGALBOS STOTIS

_____
(struktūrinio padalinio pavadinimas)

_____
(pareigų pavadinimas)

_____
(vardas, pavardė)

PRANEŠIMAS APIE GALIMĄ ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ

_____ Nr. _____

Kaunas

Informuoju apie galimą asmens duomenų saugumo pažeidimą, pateikdamas man turimą informaciją apie jį:

1. Galimo asmens duomenų saugumo pažeidimo nustatymo data, valanda (minučių tikslumu) ir vieta: _____

2. Galimo asmens duomenų saugumo pažeidimo padarymo data, laikas ir vieta: _____
_____

3. Galimo asmens duomenų saugumo pažeidimo pobūdis, esmė ir aplinkybės _____
_____
_____
_____
_____
_____

4. Duomenų subjektų, kurių asmens duomenų saugumas galimai pažeistas, kategorijos (pvz., darbuotojai, asmenys, pateikę prašymus, skundus ir pan.) ir jų skaičius (jei žinoma)) _____
_____
_____

5. Asmens duomenų kategorijos, susijusios su galimu asmens duomenų saugumo pažeidimu:

5.1. Asmens duomenys

Vardas	
Pavardė	

Asmens kodas	
Adresas	
Telefono ryšio numeris	
Elektroninio pašto adresas	
Banko sąskaitos numeris	
Banko kortelės numeris	
Prisijungimo duomenys (vartotojo vardas, slaptažodis)	
Asmens dokumento (-ų) duomenys	
Duomenys apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas	
Kiti duomenys	

5.2. Specialių kategorijų asmens duomenys

Duomenys, susiję su asmens sveikata	
Biometriniai duomenys	
Duomenys, susiję su asmens politinėmis pažiūromis, religiniais, filosofiniais įsitikinimais	
Duomenys, susiję su asmens naryste profesinėse sąjungose	
Duomenys, susiję su asmens rasine ar etnine kilme	
Duomenys, susiję su asmens lytiniu gyvenimu ir lytine orientacija	

6. Kokių veiksmų / priemonių buvo imtasi sužinojus apie padarytą asmens duomenų saugumo pažeidimą (pvz., pakeisti kompiuterio slaptažodžiai, nutraukta neteisėta prieiga prie tvarkomų asmens duomenų, panaudotos atsarginės kopijos, siekiant atkurti prarastus ar sugadintus duomenis, atnaujinta programinė įranga, surinkti ne saugojimui skirtoje vietoje palikti dokumentai su asmens duomenimis ir pan.) _____

_____

_____

_____

_____

_____

(parašas)