LIETUVOS POLICIJOS GENERALINIS KOMISARAS

ĮSAKYMAS
DĖL LIETUVOS POLICIJOS GENERALINIO KOMISARO 2019 M. KOVO 12 D. ĮSAKYMO NR. 5-V-202 „DĖL ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ NUSTATYMO, TYRIMO, PRANEŠIMO APIE JUOS IR DOKUMENTAVIMO TVARKOS APRAŠO PATVIRTINIMO“ PAKEITIMO

Nr.
Vilnius

P a k e i č i u Asmens duomenų saugumo pažeidimų nustatymo, tyrimo, pranešimo apie juos ir dokumentavimo tvarkos aprašą, patvirtintą Lietuvos policijos generalinio komisaro 2019 m. kovo 12 d. įsakymu Nr. 5-V-202 „Dėl Asmens duomenų saugumo pažeidimų nustatymo, tyrimo, pranešimo apie juos ir dokumentavimo tvarkos aprašo patvirtinimo“, ir jį išdėstau nauja redakcija (pridedama).

Policijos generalinis komisaras Renatas Požėla

1123299 2023-07-03

PATVIRTINTA
Lietuvos policijos generalinio komisaro
2019 m. kovo 12 d. įsakymu Nr. 5-V-202
(Lietuvos policijos generalinio komisaro
2023 m. d. įsakymo Nr. 5-V-
redakcija)

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ NUSTATYMO, TYRIMO, PRANEŠIMO APIE JUOS IR DOKUMENTAVIMO TVARKOS APRAŠAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Asmens duomenų saugumo pažeidimų nustatymo, tyrimo, pranešimo apie juos ir dokumentavimo tvarkos aprašas (toliau – Tvarkos aprašas) nustato asmens duomenų saugumo pažeidimų nustatymo, tyrimo, pranešimo apie juos ir dokumentavimo tvarką, už šių veiksmų atlikimą atsakingus asmenis ir (ar) padalinius.

2. Tvarkos aprašas taikomas visose policijos įstaigose.

3. Tvarkos aprašas parengtas vadovaujantis 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) (toliau – Reglamentas (ES) 2016/679) 33 ir 34 straipsniais, 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 ir 30 straipsniais, Europos Parlamento ir Tarybos direktyvos 95/46/EB 29 straipsnio darbo grupės 2017 m. spalio 3 d. patvirtintomis gairėmis dėl pranešimo apie asmens duomenų saugumo pažeidimą pagal Reglamentą (ES) 2016/679 (toliau – 29 straipsnio darbo grupės gairės) ir susijusiomis Valstybinės duomenų apsaugos inspekcijos rekomendacijomis.

4. Tvarkos apraše vartojamos sąvokos:

4.1. **Priežiūros institucija** – Valstybinė duomenų apsaugos inspekcija.

4.2. **Duomenų apsaugos pareigūnas** – Policijos departamento prie Lietuvos Respublikos vidaus reikalų ministerijos (toliau – Policijos departamentas) Duomenų apsaugos skyriaus vedėjas, kuriam visų policijos įstaigų mastu pavesta atlikti duomenų apsaugos pareigūno funkcijas ir užduotis. Duomenų apsaugos pareigūno funkcijas ir užduotis padeda atlikti duomenų apsaugos pareigūno komanda – Policijos departamento Duomenų apsaugos skyriaus darbuotojai.

5. Kitos Tvarkos apraše vartojamos sąvokos atitinka Reglamente (ES) 2016/679 ir Įstatyme apibrėžtas sąvokas. Šiuose teisės aktuose jos apibrėžtos taip:

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

5.2. **Asmens duomenų saugumo pažeidimas** – 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.

6. Apie asmens duomenų saugumo pažeidimą privaloma pranešti Valstybinei duomenų apsaugos inspekcijai visais atvejais, išskyrus, kai labiausiai tikėtina, kad toks pažeidimas nekels pavojaus fizinių asmenų teisėms ir laisvėms. Kai dėl asmens duomenų saugumo pažeidimo

pobūdžio kyla didelės grėsmės rizika fizinių asmenų teisėms ir laisvėms, apie asmens duomenų saugumo pažeidimą privaloma pranešti ir duomenų subjektams.

II SKYRIUS
PRANEŠIMAS APIE GALIMĄ ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ

7. Kiekvienas darbuotojas, nustatęs pats arba sužinojęs iš kitų šaltinių apie galimą asmens duomenų saugumo pažeidimą ar dėl bet kokių kitokių priežasčių įtardamas, kad toks pažeidimas galėjo būti padarytas, nedelsdamas (ne vėliau kaip tą pačią darbo dieną) privalo apie tai pranešti duomenų apsaugos pareigūnui, išskyrus Tvarkos aprašo 10 punkte nustatytą atvejį.

8. Pranešimas duomenų apsaugos pareigūnui siunčiamas elektroninio pašto adresu dap@policija.lt ir (arba) jo tarnybinio elektroninio pašto adresu. Kartu su pranešimu pateikiama turima medžiaga, susijusi su galimo asmens duomenų saugumo pažeidimo aplinkybėmis.

9. Priklausomai nuo aplinkybių, informacija apie galimą asmens duomenų saugumo pažeidimą duomenų apsaugos pareigūnui gali būti teikiama ir kitais būdais (pavyzdžiui, perduodant susijusį dokumentą per Policijos dokumentų valdymo sistemą (toliau – DVS) ir pan.).

10. Kai informacija apie galimą asmens duomenų saugumo pažeidimą gaunama Policijos departamento Imuniteto valdyboje, pranešimas apie galimą asmens duomenų saugumo pažeidimą duomenų apsaugos pareigūnui siunčiamas atlikus gautos informacijos patikslinimą ir surinktų duomenų pagrindu nustačius asmens duomenų saugumo pažeidimo požymius (gavus policijos įstaigos darbuotojo policijos veikloje naudojamose duomenų bazėse atliktų asmens duomenų tvarkymo veiksmų audito išrašą, užfiksuotą vaizdo, garso medžiagą ir pan.), išskyrus atvejus, kai tokia informacija jau turima (tokiu atveju pranešimas teikiamas nedelsiant). Surinkti duomenys kartu su pranešimu perduodami duomenų apsaugos pareigūnui. Jei Policijos departamento Imuniteto valdyboje atlikus gautos informacijos patikslinimą informacija apie galimą asmens duomenų saugumo pažeidimą nepasitvirtina, pranešimas duomenų apsaugos pareigūnui nesiunčiamas.

11. Duomenų apsaugos pareigūnas turi teisę iš kitų Policijos departamento struktūrinių padalinių, o taip pat iš kitų policijos įstaigų darbuotojų gauti asmens duomenų saugumo pažeidimui nustatyti ir tyrimui atlikti reikalingą informaciją ir techninę bei metodinę pagalbą. Gavę duomenų apsaugos pareigūno prašymą ar paklausimą, darbuotojai privalo suteikti prašomą informaciją ar pagalbą ne vėliau kaip tą pačią darbo dieną.

III SKYRIUS
ASMENS DUOMENŲ SAUGUMO PAŽEIDIMO TYRIMAS

12. Duomenų apsaugos pareigūnas, gavęs pranešimą apie galimą asmens duomenų saugumo pažeidimą, nedelsdamas, bet ne vėliau kaip tą pačią darbo dieną, įvertina pateiktą informaciją. Jei pateiktos informacijos nepakanka asmens duomenų saugumo pažeidimui nustatyti ir reikalingos informacijos negalima gauti per vieną darbo dieną, ne vėliau kaip kitą darbo dieną nuo pranešimo gavimo surašomas tarnybinis pranešimas, kuriuo užfiksuojamas pranešimo apie galimą asmens duomenų saugumo pažeidimą gavimo faktas ir atsakingi policijos įstaigos padaliniai įpareigojami surinkti bei duomenų apsaugos pareigūnui teikti reikalingą informaciją. Asmens duomenų saugumo pažeidimo tyrimas pradedamas gavus reikalingą informaciją ir atliekamas Tvarkos aprašo 14 punkte nustatyta tvarka.

13. Asmens duomenų saugumo pažeidimo tyrimas nepradedamas, jei įvertinus pateiktą informaciją akivaizdžiai matyti, jog nėra asmens duomenų saugumo pažeidimo sudėties arba yra pakankamai požymių, kad policijos įstaigos darbuotojas, tvarkydamas policijos įstaigos valdomus ir (ar) tvarkomus asmens duomenis, veikė kaip savarankiškas duomenų valdytojas. Vertinant, ar

policijos įstaigos darbuotojas, tvarkydamas policijos įstaigos valdomus ir (ar) tvarkomus asmens duomenis, veikė kaip savarankiškas duomenų valdytojas, visų pirma atsižvelgiama į šiuos kriterijus:

13.1. kokiu tikslu konkrečioje situacijoje buvo tvarkomi asmens duomenys ir kas nusprendė, kad duomenys būtų tvarkomi tuo tikslu;

13.2. ar policijos įstaiga taikė tinkamas technines ir organizacines priemones, siekdama užtikrinti, kad būtų laikomasi Reglamento (ES) 2016/679, Įstatymo ir kitų asmens duomenų tvarkymą reglamentuojančių teisės aktų reikalavimų.

Vertinimo, kad policijos įstaigos darbuotojas, netinkamai tvarkydamas policijos įstaigos valdomus ir (ar) tvarkomus asmens duomenis, veikė kaip savarankiškas duomenų valdytojas, išvada užfiksuojama ne vėliau kaip kitą darbo dieną nuo pranešimo gavimo surašant tarnybinį pranešimą. Tarnybiniame pranešime gali būti teikiamas siūlymas policijos įstaigos darbuotojo veiksmus, tvarkant policijos įstaigos valdomus ir (ar) tvarkomus asmens duomenis kaip savarankiškam duomenų valdytojui, įvertinti Policijos departamento Imuniteto valdyboje siekiant nustatyti, ar nebuvo padarytas tarnybinis nusižengimas, taip pat gali būti teikiamos rekomendacijos policijos įstaigos vadovui ar jo įgaliotam asmeniui dėl siūlomų techninių ir (ar) organizacinių priemonių taikymo.

14. Duomenų apsaugos pareigūnas, gavęs pranešimą apie galimą asmens duomenų saugumo pažeidimą ir įvertinęs, kad pateiktos informacijos pakanka tyrimui dėl galimo asmens duomenų saugumo pažeidimo pradėti, ne vėliau kaip per kitą darbo dieną atlieka tyrimą, kurio tikslas – išsiaiškinti ir nustatyti:

14.1. ar pažeidimas iš tikrųjų buvo padarytas;

14.2. jeigu pažeidimas iš tikrųjų buvo padarytas, koks yra pažeidimo tipas ir kokios galimos jo pasekmės (įvertinti grėsmės riziką).

15. Asmens duomenų saugumo pažeidimų tipai:

15.1. konfidencialumo pažeidimas – neleistinas arba netyčinis asmens duomenų atskleidimas arba prieigos prie asmens duomenų suteikimas;

15.2. vientisumo pažeidimas – neleistinas arba netyčinis asmens duomenų pakeitimas;

15.3. prieinamumo pažeidimas – neleistinas arba netyčinis prieigos prie asmens duomenų praradimas arba asmens duomenų sunaikinimas.

16. Priklausomai nuo aplinkybių, asmens duomenų saugumo pažeidimas gali būti priskiriamas vienam iš nurodytų tipų arba atitikti jų derinį.

17. Grėsmės rizikos vertinimas atliekamas vadovaujantis Tvarkos aprašu ir 29 straipsnio darbo grupės gairėmis, atsižvelgiant į konkrečias su asmens duomenų saugumo pažeidimu susijusias aplinkybes.

18. Vertinant grėsmės riziką fizinių asmenų teisėms ir laisvėms, siekiama nustatyti pavojaus atsiradimo tikimybę ir rimtumą. Tai vertinama atsižvelgiant į šiuos kriterijus:

18.1. asmens duomenų saugumo pažeidimo tipą;

18.2. asmens duomenų pobūdį (jautrumą) ir apimtį;

18.3. duomenų subjektų skaičių ir ypatumus;

18.4. kaip lengvai, remiantis asmens duomenimis, gali būti nustatyta duomenų subjekto tapatybė;

18.5. kokios pasekmės dėl įvykusio asmens duomenų saugumo pažeidimo kilo arba gali kilti duomenų subjektams;

18.6. ar imtasi priemonių asmens duomenų saugumo pažeidimo pasekmėms pašalinti arba sumažinti.

19. Vertinant grėsmės riziką fizinių asmenų teisėms ir laisvėms, laikoma, kad asmens duomenų pažeidimas, galintis kelti pavojų fizinių asmenų teisėms ir laisvėms, yra toks pažeidimas, dėl kurio, laiku nesiėmus tinkamų priemonių, fiziniai asmenys gali patirti kūno sužalojimą, materialinę ar nematerialinę žalą, teisių apribojimą, diskriminaciją, gali būti pavogta ar suklastota asmens tapatybė, padaryta finansinių nuostolių, pakenkta reputacijai, prarastas asmens duomenų, kurie saugomi profesine paslaptimi, konfidencialumas arba padaryta kita ekonominė ar socialinė žala atitinkamam fiziniam asmeniui.

20. Vertinant pavojaus fizinių asmenų teisėms ir laisvėms rimtumą, esminės reikšmės turi asmens duomenų jautrumas, todėl visų pirma atsižvelgiama į tai, ar pažeidimas yra susijęs su asmens duomenimis, kurie atskleidžia duomenų subjekto rasinę arba etninę kilmę, politines pažiūras, religinius arba filosofinius įsitikinimus, priklausymą profesinėms sąjungoms arba kuriuose yra genetinių duomenų, duomenų apie sveikatą arba lytinį gyvenimą, apkaltinamuosius nuosprendžius ir nusikalstamas veikas arba susijusias apsaugos priemones.

21. Įvertinus grėsmės riziką, nustatoma, kad rizikos tikimybė yra:

21.1. žema;

21.2. vidutinė;

21.3. didelė.

22. Jei, įvertinus grėsmės riziką fizinių asmenų teisėms ir laisvėms, grėsmė nenustatoma ir, atsižvelgiant į asmens duomenų saugumo pažeidimo padarymo aplinkybes ir pritaikytas priemones, mažai tikėtina, kad ji galėtų kilti ateityje, laikoma, kad rizikos tikimybė yra itin žema ir pavojus fizinių asmenų teisėms ir laisvėms nekyla.

23. Duomenų apsaugos pareigūnas, atlikdamas tyrimą, lygiagrečiai turi imtis veiksmų (arba nurodyti jų imtis kitiems padaliniams ar darbuotojams pagal kompetenciją) dėl pažeidimo pašalinimo (sustabdymo, ištaisymo).

24. Atlikęs tyrimą, tą pačią darbo dieną duomenų apsaugos pareigūnas tarnybinio pranešimo forma surašo išvadą dėl asmens duomenų saugumo pažeidimo fakto nustatymo ir rizikos fizinių asmenų teisėms bei laisvėms įvertinimo ir pateikia susijusius siūlymus (dėl taisomųjų veiksmų vykdymo, pranešimo pateikimo priežiūros institucijai, duomenų subjektams ir pan.). Tarnybinis pranešimas adresuojamas policijos įstaigos vadovui ir perduodamas jam ar jo įgaliotam asmeniui rezoliucijai įrašyti.

25. Nustačius, kad asmens duomenų saugumo pažeidimas buvo padarytas arba kad policijos įstaigos darbuotojas, tvarkydamas policijos įstaigos valdomus ir (ar) tvarkomus asmens duomenis, veikė kaip savarankiškas duomenų valdytojas, tarnybinis pranešimas DVS priemonėmis perduodamas Policijos departamento Imuniteto valdybos viršininkui spręsti dėl tarnybinio patikrinimo pradėjimo.

26. Duomenų apsaugos pareigūnas turi teisę gauti informaciją apie tai, kaip buvo įgyvendinti išvadoje pateikti siūlymai. Už išvadoje pateiktų siūlymų įgyvendinimą atsakingas Policijos departamento ar policijos įstaigos struktūrinis padalinys, gavęs duomenų apsaugos pareigūno paklausimą pateikti informaciją apie tai, kaip buvo įgyvendinti išvadoje pateikti siūlymai, šią informaciją duomenų apsaugos pareigūnui pateikia per vieną darbo dieną arba per duomenų apsaugos pareigūno paklausime nurodytą terminą.

IV SKYRIUS
PRANEŠIMO PATEIKIMAS PRIEŽIŪROS INSTITUCIJAI

27. Nustačius, kad asmens duomenų saugumo pažeidimas buvo padarytas ir kad yra Tvarkos aprašo 21.1–21.3 papunkčiuose nustatyto lygio rizika fizinių asmenų teisėms ir laisvėms, apie tai nedelsiant, ne vėliau kaip per 72 valandas nuo sužinojimo apie padarytą pažeidimą, turi būti pranešama Valstybinei duomenų apsaugos inspekcijai.

28. Pranešimą apie policijos įstaigoje padarytą asmens duomenų saugumo pažeidimą ir nustatytą riziką fizinių asmenų teisėms ir laisvėms rengia ir pasirašo duomenų apsaugos pareigūnas.

29. Pranešimas rengiamas vadovaujantis Pranešimo apie asmens duomenų saugumo pažeidimą rekomenduojama forma, patvirtinta Valstybinės duomenų apsaugos inspekcijos direktoriaus 2018 m. rugpjūčio 29 d. įsakymu Nr. 1T-82(1.12.E) „Dėl Pranešimo apie asmens duomenų saugumo pažeidimą rekomenduojamos formos patvirtinimo“. Bet kuriuo atveju pranešime turi būti nurodoma ši informacija:

29.1. asmens duomenų saugumo pažeidimo pobūdis, asmens duomenų ir duomenų subjektų kategorijos ir apytikslis skaičius;

29.2. tikėtinos asmens duomenų saugumo pažeidimo pasekmės;

29.3. priemonės, kurių buvo imtasi arba siūloma imtis, kad būtų pašalintas asmens duomenų saugumo pažeidimas;

29.4. duomenų apsaugos pareigūno, kitų asmenų, galinčių suteikti daugiau informacijos, vardai, pavardės ir kontaktiniai duomenys.

30. Jeigu, atsižvelgiant į asmens duomenų saugumo pažeidimo pobūdį ar kitas aplinkybes, yra būtina atlikti išsamesnį tyrimą tam, kad būtų nustatyti visi svarbūs su pažeidimu susiję faktai, ir per 72 valandas nuo sužinojimo apie pažeidimą dėl objektyvių aplinkybių to padaryti neįmanoma, informacija Valstybinei duomenų apsaugos inspekcijai gali būti teikiama etapais. Tokiu atveju apie informacijos teikimą etapais Valstybinė duomenų apsaugos inspekcija yra informuojama teikiant pirmąjį pranešimą apie asmens duomenų saugumo pažeidimą.

31. Visi iš Valstybinės duomenų apsaugos inspekcijos gauti paklausimai ir kitokie raštai, susiję su duomenų apsaugos pareigūno teiktu pranešimu apie padarytą asmens duomenų saugumo pažeidimą, DVS priemonėmis perduodami duomenų apsaugos pareigūnui susipažinti ir (ar) pagal kompetenciją nagrinėti bei teikti atsakymą.

V SKYRIUS
PRANEŠIMO PATEIKIMAS DUOMENŲ SUBJEKTUI

32. Nustačius, kad asmens duomenų saugumo pažeidimas buvo padarytas ir kad yra didelė rizika fizinių asmenų teisėms ir laisvėms, duomenų apsaugos pareigūnas nedelsdamas, ne vėliau kaip per 72 valandas nuo sužinojimo apie padarytą pažeidimą, parengia, pasirašo ir teikia pranešimą duomenų subjektui, kurio teisėms ir laisvėms gali kilti didelis pavojus.

33. Pranešime duomenų subjektui pateikiama ši informacija:

33.1. asmens duomenų saugumo pažeidimo aprašymas;

33.2. duomenų apsaugos pareigūno, esant poreikiui, kitų kontaktinių asmenų vardai, pavardės ir kontaktiniai duomenys;

33.3. tikėtinų pasekmių aprašymas;

33.4. priemonių, kurių buvo imtasi ar kurių siūloma imtis, kad būtų pašalintas pažeidimas ir sumažintos galimos neigiamos pasekmės, aprašymas;

33.5. kita reikšminga informacija, susijusi su pažeidimu.

34. Duomenų subjektai apie asmens duomenų saugumo pažeidimą informuojami tiesiogiai, išskyrus atvejus, kai tai pareikalautų neproporcingai daug pastangų, pavyzdžiui, kai duomenų subjektų yra labai daug arba konkretus duomenų subjektų ratas nėra apibrėžtas ir pan. Tokiu atveju apie asmens duomenų saugumo pažeidimą gali būti paskelbiamas viešas pranešimas. Turi būti parenkama tokia viešo pranešimo paskelbimo priemonė, kuria būtų užtikrinta didžiausia tikimybė, kad informacija pasieks visus asmenis, kuriems pažeidimas turi (gali turėti) poveikį. Siekiant šio tikslo, gali būti parenkamos kelios pranešimo priemonės.

35. Pranešimas duomenų subjektams gali būti neteikiamas, jeigu iki jo pateikimo yra vykdomos tinkamos techninės ir organizacinės apsaugos priemonės, kurios leidžia sumažinti didelę riziką fizinių asmenų teisėms ir laisvėms iki priimtino lygio, tai yra rizikos tikimybė tampa ne aukštesnė nei vidutinė.

36. Jei pranešimą apie galimą asmens duomenų saugumo pažeidimą pateikė duomenų subjektas, jis apie atlikto asmens duomenų saugumo pažeidimo tyrimo rezultatus informuojamas visais atvejais, nepriklausomai nuo to, ar asmens duomenų saugumo pažeidimas buvo padarytas ir, jei buvo padarytas, kokio lygio rizika kyla duomenų subjekto teisėms ir laisvėms.

VI SKYRIUS
ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ DOKUMENTAVIMAS

37. Visi asmens duomenų saugumo pažeidimai, nepriklausomai nuo to, ar apie juos buvo pranešta Valstybinei duomenų apsaugos inspekcijai ar ne, registruojami Asmens duomenų saugumo pažeidimų žurnale (toliau – Žurnalas). Žurnalas tvarkomas elektronine forma.

38. Informacija apie asmens duomenų saugumo pažeidimą į Žurnalą įvedama nedelsiant, kai tik nustatomas pažeidimo faktas. Įvesta informacija pagal poreikį pildoma ir (ar) koreguojama.

39. Žurnale nurodoma ši informacija:

39.1. su asmens duomenų saugumo pažeidimu susiję faktai, pažeidimo tipas ir pasekmės;

39.2. taisomieji veiksmai, kurių buvo imtasi;

39.3. pranešimo Valstybinei duomenų apsaugos inspekcijai pateikimo aplinkybės (pranešimo pateikimo vėlavimo priežastys, etapai ar sprendimo nepranešti motyvai ir pan.);

39.4. pranešimo duomenų subjektams pateikimo aplinkybės;

39.5. kita reikšminga informacija.

40. Registruojant asmens duomenų saugumo pažeidimą, nurodomi su pažeidimu susijusių dokumentų registracijos datos ir numeriai. Kita informacija Žurnale pateikiama nenurodant asmens duomenų, tiesiogiai atskleidžiančių asmens tapatybę (vardai, pavardės, pareigos ir pan.).

41. Asmens duomenų saugumo pažeidimus registruoja, Žurnalą pildo ir (ar) įvestą informaciją koreguoja Policijos departamento Duomenų apsaugos skyriaus darbuotojai ir kontroliuoja duomenų apsaugos pareigūnas.

VII SKYRIUS
BAIGIAMOSIOS NUOSTATOS

42. Darbuotojai su Tvarkos aprašu ir jo pakeitimais supažindinami pasirašytinai. Supažindinimą vykdo Policijos departamento Dokumentų administravimo valdybos darbuotojai, atsakingi už dokumentų valdymą policijos įstaigoje, o už naujai priimamų darbuotojų supažindinimą atsako jų tiesioginiai vadovai.

_____

DETALŪS METADUOMENYS	
Dokumento sudarytojas (-ai)	Policijos departamentas prie Lietuvos Respublikos vidaus reikalų ministerijos 188785847, Saltoniškių g. 19, LT-08105 Vilnius
Dokumento pavadinimas (antraštė)	DĖL LIETUVOS POLICIJOS GENERALINIO KOMISARO 2019 M. KOVO 12 D. ĮSAKYMO NR. 5-V-202 „DĖL ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ NUSTATYMO, TYRIMO, PRANEŠIMO APIE JUOS IR DOKUMENTAVIMO TVARKOS APRAŠO PATVIRTINIMO“ PAKEITIMO
Dokumento registracijos data ir numeris	2023-07-10 Nr. 5-V-578
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	Renatas Požėla, Policijos generalinis komisaras
Sertifikatas išduotas	RENATAS POŽĖLA LT
Parašo sukūrimo data ir laikas	2023-07-10 16:47:51 (GMT+03:00)
Parašo formatas	XAdES-T
Laiko žymoje nurodytas laikas	2023-07-10 16:48:04 (GMT+03:00)
Informacija apie sertifikavimo paslaugų teikėją	EID-SK 2016, AS Sertifitseerimiskeskus EE
Sertifikato galiojimo laikas	2019-11-14 11:07:15 – 2024-11-12 23:59:59
Informacija apie būdus, naudotus metaduomenų vientisumui užtikrinti	"Registravimas" paskirties metaduomenų vientisumas užtikrintas naudojant "RCSC IssuingCA, VI Registru centras - i.k. 124110246 LT" išduotą sertifikatą "Dokumentų valdymo sistema Avilys, Policijos departamentas prie LR VRM, į.k.188785847 L=Vilnius LT", sertifikatas galioja nuo 2022-05-26 08:52:31 iki 2025-05-25 08:52:31
Pagrindinio dokumento priedų skaičius	1
Pagrindinio dokumento pridedamų dokumentų skaičius	–
Pridedamo dokumento sudarytojas (-ai)	–
Pridedamo dokumento pavadinimas (antraštė)	–
Pridedamo dokumento registracijos data ir numeris	–
Programinės įrangos, kuria naudojantis sudarytas elektroninis dokumentas, pavadinimas	Dokumentų valdymo sistema Avilys, versija 3.5.68.1
Informacija apie elektroninio dokumento ir elektroninio (-ių) parašo (-ų) tikrinimą (tikrinimo data)	Atitinka specifikacijos keliamus reikalavimus. Visi dokumente esantys elektroniniai parašai galioja (2023-07-10 16:55:03)
Paieškos nuoroda	–
Papildomi metaduomenys	Nuorašą suformavo 2023-07-10 16:55:04 Dokumentų valdymo sistema Avilys