PATVIRTINTA
Asmens su negalia teisių apsaugos agentūros
prie Lietuvos Respublikos socialinės apsaugos
ir darbo ministerijos direktoriaus
2026 m. d. įsakymu Nr. V-

PRANEŠIMO APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ ASMENS SU NEGALIA TEISIŲ APSAUGOS AGENTŪROJE PRIE LIETUVOS RESPUBLIKOS SOCIALINĖS APSAUGOS IR DARBO MINISTERIJOS PATEIKIMO TVARKOS APRAŠAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Pranešimo apie asmens duomenų saugumo pažeidimą Asmens su negalia teisių apsaugos agentūroje prie Lietuvos Respublikos socialinės apsaugos ir darbo ministerijos pateikimo tvarkos aprašas (toliau – Tvarkos aprašas) nustato asmens duomenų saugumo pažeidimo aptikimo, sustabdymo (pašalinimo) ir pranešimo apie asmens duomenų saugumo pažeidimą Asmens su negalia teisių apsaugos agentūroje prie Lietuvos Respublikos socialinės apsaugos ir darbo ministerijos (toliau – Agentūra) tvarką.

2. Šis Tvarkos aprašas taikomas Agentūroje tvarkant duomenų subjektų asmens duomenis.

3. Šis Tvarkos aprašas parengtas 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 (toliau – Bendrasis duomenų apsaugos reglamentas).

4. Šiame Tvarkos apraše vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos Bendrajame duomenų apsaugos reglamente.

5. Galimi šie asmens duomenų saugumo pažeidimai:

5.1. konfidencialumo pažeidimas – neteisėtas arba netyčinis asmens duomenų atskleidimas arba gauta prieiga prie jų;

5.2. vientisumo pažeidimas – neteisėtas arba netyčinis asmens duomenų pakeitimas;

5.3. prieinamumo pažeidimas – neteisėtas arba netyčinis prieigos prie asmens duomenų praradimas arba asmens duomenų sunaikinimas.

6. Atsižvelgiant į aplinkybes, asmens duomenų saugumo pažeidimas vienu metu gali būti susijęs su asmens duomenų konfidencialumu, vientisumu ir prieinamumu, taip pat su bet kokiu jų deriniu.

7. Asmens duomenų saugumo pažeidimas gali įvykti dėl šių priežasčių:

7.1. žmogiškosios klaidos (pvz., asmens duomenys, perduoti ar persiųsti ne tam adresatui (asmeniui), kuriam jie buvo skirti; ne saugojimui skirtoje vietoje ar byloje palikti (įkelti) dokumentai, kuriuose yra asmens duomenų; pamesti nešiojami / mobilieji įrenginiai (telefonas, nešiojamasis kompiuteris, išorinės duomenų laikmenos), kuriuose saugomi asmens duomenys ir kt.);

7.2. vagystės (pvz., pavogti nešiojami / mobilieji įrenginiai, kuriuose saugomi asmens duomenys; pavogtos neautomatiniu būdu susistemintos bylos, kuriose yra asmens duomenų ir kt.);

7.3. kibernetinės atakos (pvz., duomenų bazėje ar informacinėje sistemoje esantys asmens duomenys užšifruojami, naudojant išpirkos reikalaujančią programą; internete paskelbiami informacinių sistemų naudotojų vardai ir slaptažodžiai ir kt.);

7.4. neleistinos (neautorizuotos) prieigos prie asmens duomenų (pvz., įgaliojimų neturintys asmenys patenka į patalpas, kuriose saugomos bylos su asmens duomenimis; įgaliojimų neturintys asmenys prisijungia prie duomenų bazių ar informacinių sistemų ir kt.);

7.5. įrenginių ar programinės įrangos gedimo, saugos sistemos spragų (pvz., energijos tiekimo nutrūkimas, dėl kurio negalima prieiga prie asmens duomenų; programos kodo, kuriuo kontroliuojamas prieigos teisių suteikimas informacinių sistemų naudotojams, klaida ir kt.);

7.6. nenugalimos jėgos (force majeure) aplinkybių ir kitų priežasčių (gaisras, vandens užliejimas, dėl kurių sugadinami arba prarandami asmens duomenys ir kt.).

8. Asmens duomenų saugumo pažeidimas, galintis kelti pavojų asmenų teisėms ir laisvėms yra toks, dėl kurio, laiku nesiėmus tinkamų priemonių, fiziniai asmenys gali patirti kūno sužalojimą, materialinę ar nematerialinę žalą (pvz., asmuo gali patirti teisių apribojimą, diskriminaciją, gali būti pavogta ar suklastota jo asmens tapatybė, jam padaryta finansinių nuostolių, pakenkta jo reputacijai, prarastas duomenų, kurie laikomi profesine paslaptimi, konfidencialumas ir kt.).

II SKYRIUS
PRANEŠIMAS APIE GALIMĄ ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ AGENTŪRAI

9. Agentūros valstybės tarnautojai ar darbuotojai, dirbantys pagal darbo sutartį (toliau kartu – darbuotojai), sužinoję ar patys nustatę galimą asmens duomenų saugumo pažeidimą arba kai informacija apie galimą asmens duomenų saugumo pažeidimą gaunama iš duomenų tvarkytojo, žiniasklaidos ar kito šaltinio:

9.1. nedelsdami, bet ne vėliau kaip per 2 darbo valandas nuo asmens duomenų saugumo pažeidimo paaiškėjimo momento, informuoja savo tiesioginį vadovą ir Agentūros duomenų apsaugos pareigūną;

9.2. užpildo šio Tvarkos aprašo 1 priede nustatytos formos, skelbiamos Agentūros intraneto svetainės skyriuje „Asmens duomenų apsauga“, tarnybinį pranešimą apie galimą asmens duomenų saugumo pažeidimą ir nedelsiant, bet ne vėliau kaip per 2 darbo valandas nuo pažeidimo paaiškėjimo momento, perduoda šį tarnybinį pranešimą Agentūros duomenų apsaugos pareigūnui elektroniniu paštu dap@anta.lt arba užregistruoja dokumentų valdymo bendrojoje informacinėje sistemoje (toliau – DBSIS), o pranešimas DBSIS priemonėmis nukreipiamas Agentūros duomenų apsaugos pareigūnui susipažinti;

9.3. jei įmanoma, nedelsiant imasi priemonių pašalinti asmens duomenų saugumo pažeidimą ir priemonių galimoms neigiamoms jo pasekmėms sumažinti;

9.4. kartu su darbuotojo tarnybiniu pranešimu apie galimą asmens duomenų saugumo pažeidimą gali būti pateikiami šio pranešimo priedai: rašytinė informacija, nurodanti galimo asmens duomenų saugumo pažeidimo aplinkybes ir/ar kiti faktiniai duomenys, patvirtinantys priemones ir veiksmus, kurių buvo imtasi galimo asmens duomenų saugumo pažeidimo neigiamoms pasekmėms sumažinti.

10. Duomenų tvarkytojai, sužinoję apie asmens duomenų saugumo pažeidimą, nedelsdami, bet ne vėliau kaip per 3 darbo valandas, apie tai praneša Agentūros duomenų apsaugos pareigūnui, elektroniniu paštu dap@anta.lt pateikdami pranešimą, numatytą Bendrojo duomenų apsaugos reglamento 33 straipsnio 3 dalyje, tiek, kiek tos informacijos įmanoma pateikti tuo metu.

11. Agentūros darbuotojai ar duomenų tvarkytojai turėtų būti laikomi žinančiais apie pažeidimą nuo to momento, kai yra pagrįstų įtarimų, kad įvyko saugumo incidentas, dėl kurio kilo realus pavojus asmens duomenų saugumui.

III SKYRIUS
ASMENS DUOMENŲ SAUGUMO PAŽEIDIMO TYRIMAS IR PAŠALINIMAS

12. Agentūros duomenų apsaugos pareigūnas, gavęs Agentūros darbuotojo užpildytą tarnybinį pranešimą dėl galimo asmens duomenų saugumo pažeidimo ar duomenų tvarkytojo pranešimą dėl asmens duomenų saugumo pažeidimo (toliau kartu – pranešimas):

12.1. nedelsdamas nagrinėja pranešime nurodytas aplinkybes;

12.2. įvertina, ar padarytas asmens duomenų saugumo pažeidimas;

12.3. jei asmens duomenų saugumo pažeidimas padarytas, nustato, kokio tipo pažeidimas padarytas; asmens duomenų kategorijas, įskaitant specialių kategorijų asmens duomenis, kurios buvo susijusios su pažeidimu; pažeidimo priežastis, lėmusias asmens duomenų saugumo pažeidimą; apimtis (duomenų subjektų kategorijos ir skaičius), žalą, padarytą asmeniui;

12.4. prireikus pasitelkia Informacinių technologijų skyriaus darbuotoją, kurį paskiria jo tiesioginis vadovas, aplinkybių tyrimui ir taikytinų techninių ir organizacinių priemonių nustatymui, jeigu galimas asmens duomenų saugumo pažeidimas susijęs su elektroninės informacijos saugos ir kibernetinio saugumo incidentu (kompiuterių, terminalų, serverių, laikmenų, kitų Agentūros nuosavybės teise, nuomos ar kitais pagrindais valdomos kompiuterinės įrangos ir joje esančios programinės įrangos, taip pat elektroninės pašto dėžutės, bendravimo interneto tinklu programų, debesų kompiuterijos paslaugų, interneto prieigos, kitų informacinių technologijų naudojimu);

12.5. nustato, kokių skubių ir tinkamų priemonių būtina imtis, kad būtų pašalintas asmens duomenų saugumo pažeidimas (pvz., naudoti atsargines kopijas, siekiant atkurti prarastus ar sugadintus duomenis ar kt.);

12.6. nustato, ar būtina apie įvykusį asmens duomenų saugumo pažeidimą pranešti Valstybinei duomenų apsaugos inspekcijai (toliau – Inspekcija) ir duomenų subjektui.

13. Agentūros duomenų apsaugos pareigūnas, vertindamas rizikos lygį, atsižvelgia į konkrečias pažeidimo aplinkybes, pavojaus duomenų subjektų teisėms ir laisvėms atsiradimo tikimybę ir rimtumą bei veikia kaip nepriklausomas konsultantas ir ekspertas, teikiantis išvadas bei rekomendacijas, o galutiniai sprendimai dėl asmens duomenų saugumo pažeidimo kvalifikavimo, rizikos lygio nustatymo ir pranešimo Inspekcijai ar duomenų subjektams priimami Agentūros direktoriaus ar jo įgalioto asmens. Rizikos lygis vertinamas atsižvelgiant į šiuos kriterijus:

13.1. saugumo pažeidimo pobūdį (konfidencialumo, vientisumo ar prieinamumo pažeidimas) – nustatomas saugumo pažeidimo pobūdis, nuo kurio gali priklausyti pavojaus duomenų subjektams dydis;

13.2. asmens duomenų pobūdį, jautrumą ir kiekį – nustatomas asmens duomenų, kurių saugumas buvo pažeistas, pobūdis, jautrumas ir jų kiekis: kuo jautresni asmens duomenys ir kuo didesnis jų kiekis, tuo didesnis žalos pavojus;

13.3. galimybę identifikuoti fizinį asmenį – įvertinama, ar neįgaliotiems asmenims, kuriems tapo prieinami asmens duomenys, bus lengva nustatyti konkrečių asmenų tapatybę arba susieti tuos duomenis su kita informacija (pvz., tinkamai užšifruoti asmens duomenys nebus suprantami neįgaliotiems asmenims, todėl pažeidimas padarys mažesnį poveikį duomenų subjektams);

13.4. fizinio asmens specifinius ypatumus – nustatomi fizinių asmenų, kurių asmens duomenims kilo pavojus, specifiniai ypatumai: kuo asmenys yra labiau pažeidžiami (pvz., vaikai, negalią turintys asmenys), tuo didesnį poveikį pažeidimas gali jiems padaryti;

13.5. nukentėjusių duomenų subjektų skaičių – nustatomas nukentėjusių asmenų skaičius: kuo daugiau yra asmenų, kuriems pažeidimas turi poveikio, tuo didesnis žalos pavojus;

13.6. pasekmes, sukeltas fiziniams asmenims – įvertinamos visos galimos pažeidimo pasekmės bei jų rimtumas; taip pat atsižvelgiama į pasekmių ilgalaikiškumą: jei pažeidimo pasekmės yra ilgalaikės, tai poveikis fiziniams asmenims bus didesnis.

14. Agentūros duomenų apsaugos pareigūnas, įvertinęs riziką, nustato vieną iš trijų rizikos tikimybių lygių – mažą, vidutinį ar didelį.

15. Atliekant asmens duomenų saugumo pažeidimo tyrimą ir siekiant nustatyti, ar pažeidimas iš tikrųjų įvyko, esamos situacijos įrodymai privalo būti fiksuojami dokumentuose ir užtikrinamas jų atsekamumas.

16. Agentūros duomenų apsaugos pareigūnas, atlikęs asmens duomenų saugumo pažeidimo tyrimą, surašo šio Tvarkos aprašo 2 priede nustatytos formos Asmens duomenų saugumo pažeidimo ataskaitą ir ją užregistruoja Agentūros DBSIS.

17. Asmens duomenų saugumo pažeidimo ataskaita yra pateikiama Agentūros direktoriui ir duomenų tvarkytojo vadovui, jei tai susiję su duomenų tvarkytojo atliekamais asmens duomenų tvarkymo veiksmais.

18. Asmens duomenų saugumo pažeidimo ataskaitą ir, jeigu būtina, parengtą priemonių planą, kuriame numatomas techninių, organizacinių, administracinių ir kitų priemonių poreikis dėl asmens duomenų saugumo pažeidimo, tvirtina, atsakingus vykdytojus paskiria ir įgyvendinimo terminus nustato Agentūros direktorius.

Galutinį sprendimą dėl pranešimo apie asmens duomenų saugumo pažeidimą Inspekcijai ir (ar) duomenų subjektams, atsižvelgdamas į Agentūros duomenų apsaugos pareigūno pateiktas išvadas ir rekomendacijas, priima Agentūros direktorius arba jo įgaliotas asmuo.

IV SKYRIUS
PRANEŠIMAS APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ PRIEŽIŪROS INSTITUCIJAI IR DUOMENŲ SUBJEKTUI

19. Agentūros duomenų apsaugos pareigūnas nedelsdamas ir, jei įmanoma, nepraėjus 72 valandoms nuo to laiko, kai buvo sužinota apie asmens duomenų saugumo pažeidimą, pateikia Inspekcijai pranešimą apie asmens duomenų saugumo pažeidimą, vadovaujantis Pranešimo apie asmens duomenų saugumo pažeidimą pateikimo Valstybinei duomenų apsaugos inspekcijai tvarkos aprašo, patvirtinto Inspekcijos direktoriaus 2018 m. liepos 27 d. įsakymu Nr. 1T-72(1.12.E) „Dėl pranešimo apie asmens duomenų saugumo pažeidimą pateikimo Valstybinei duomenų apsaugos inspekcijai tvarkos aprašo patvirtinimo“ nustatyta tvarka. Pranešimas apie asmens duomenų saugumo pažeidimą Inspekcijai teikiamas pagal formą, patvirtintą 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“.

20. Kai apie padarytą asmens duomenų saugumo pažeidimą privaloma informuoti Inspekciją, tačiau per 72 valandas yra neįmanoma šio pažeidimo ištirti, pranešime Inspekcijai yra pateikiama tuo metu prieinama informacija, nurodyta Bendrojo duomenų apsaugos reglamento 33 straipsnio 3 dalyje, vėlavimo priežastys ir kada bus pateikta kita detalesnė informacija. Informacija gali būti teikiama etapais, apie tai Inspekciją informuojant pirminiame pranešime.

21. Tuo atveju, jei po pranešimo apie asmens duomenų saugumo pažeidimą pateikimo Inspekcijai, atlikus tolesnį tyrimą, yra nustatoma, kad pažeidimas buvo sustabdytas ir faktiškai neįvyko, Agentūros duomenų apsaugos pareigūnas nedelsdamas apie tai informuoja Inspekciją.

22. Agentūros duomenų apsaugos pareigūnas nedelsdamas ir, jei įmanoma, nepraėjus 72 valandoms nuo to laiko, kai buvo sužinota apie asmens duomenų saugumo pažeidimą, elektroniniu paštu, paštu, SMS žinute ar kitu būdu praneša apie asmens duomenų saugumo pažeidimą duomenų subjektui, kai dėl asmens duomenų saugumo pažeidimo gali kilti didelis pavojus

fizinių asmenų teisėms ir laisvėms, Bendrojo duomenų apsaugos reglamento 34 straipsnyje nustatyta tvarka, išskyrus šiame straipsnyje numatytas išimtis.

23. Duomenų subjektas gali būti informuojamas apie asmens duomenų saugumo pažeidimą vėliau, nesilaikant šio Aprašo 22 punkte nustatyto termino, kai tenkinamos Bendrojo duomenų apsaugos reglamento 34 straipsnio 3 dalies sąlygos, kuriomis siekiama užkirsti kelią besikartojantiems ar panašiems asmens duomenų saugumo pažeidimams.

24. Duomenų tvarkytojai suteikia Agentūrai pagalbą, kurios reikia, kad būtų tinkamai pranešta apie asmens duomenų saugumo pažeidimą duomenų subjektui.

25. Tuo atveju, kai asmens duomenų saugumo pažeidimas nekelia pavojaus fizinių asmenų teisėms ir laisvėms, apie padarytą asmens duomenų saugumo pažeidimą Inspekcija ir duomenų subjektai nėra informuojami.

26. Tuo atveju, kai yra įtariama, kad asmens duomenų saugumo pažeidimas turi nusikalstamos veikos požymių, informacija apie galimą nusikalstamą veiką pateikiama atitinkamoms valstybės institucijoms, įgaliotoms atlikti ikiteisminį tyrimą. Sprendimą dėl kreipimosi į teisėsaugos institucijas priima Agentūros direktorius.

27. Kai padarytas asmens duomenų saugumo pažeidimas yra susijęs su kibernetiniu incidentu, informacija apie kibernetinį incidentą, susijusį su asmens duomenų saugumo pažeidimu, pateikiama Lietuvos Respublikos kibernetinio saugumo įstatyme nurodytoms valstybės institucijoms šio įstatymo nustatyta tvarka ir atvejais.

V SKYRIUS
ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ REGISTRAVIMAS

28. Visi asmens duomenų saugumo pažeidimai, nepriklausomai nuo jų reikšmingumo ir nuo to, ar apie juos buvo pranešta Inspekcijai ir duomenų subjektui, registruojami Agentūros Asmens duomenų saugumo pažeidimų registravimo žurnale (toliau – Asmens duomenų saugumo pažeidimų registravimo žurnalas) (Tvarkos aprašo 3 priedas).

29. Agentūros duomenų apsaugos pareigūnas nedelsdamas, bet ne ilgiau kaip per 5 darbo dienas, įrašo informaciją apie asmens duomenų saugumo pažeidimą į Asmens duomenų saugumo pažeidimų registravimo žurnalą, kuriame nurodoma:

29.1. pažeidimo nustatymo aplinkybės (pažeidimo nustatymo data, laikas, vieta, subjektas, pranešęs apie pažeidimą);

29.2. pažeidimo aplinkybės (pažeidimo data, vieta, pažeidimo pobūdis, priežastys, asmens duomenų, kurių saugumas pažeistas, kategorijos ir apytikslis skaičius, duomenų subjektų, kurių asmens duomenų saugumas pažeistas, kategorijos ir apytikslis skaičius);

29.3. tikėtinos pažeidimo pasekmės ir pavojus duomenų subjekto teisėms ir laisvėms;

29.4. priemonės, kurių buvo imtasi, kad būtų pašalintas pažeidimas, įskaitant priemones galimoms neigiamoms pažeidimo pasekmėms sumažinti;

29.5. informacija apie pranešimą ar nepranešimą Inspekcijai:

29.5.1. jeigu apie asmens duomenų saugumo pažeidimą buvo nepranešta Inspekcijai, nurodomi tokio sprendimo motyvai; jeigu apie asmens duomenų saugumo pažeidimą buvo pranešta Inspekcijai, nurodoma pranešimo data ir numeris, taip pat, ar informacija teikiama etapais;

29.5.2. jeigu apie asmens duomenų saugumo pažeidimą buvo vėluojama pranešti Inspekcijai, nurodomos tokio vėlavimo priežastys;

29.6. informacija apie pranešimą ar nepranešimą duomenų subjektui (subjektams):

29.6.1. jeigu apie asmens duomenų saugumo pažeidimą buvo nepranešta duomenų subjektui (subjektams), nurodomi tokio sprendimo motyvai; jeigu apie asmens duomenų saugumo pažeidimą buvo pranešta duomenų subjektui (subjektams), nurodoma pranešimo (pranešimų) data (datos) ir būdas (būdai);

29.6.2. jeigu apie asmens duomenų saugumo pažeidimą buvo vėluojama pranešti duomenų subjektui (subjektams), nurodomos tokio vėlavimo priežastys;

29.7. kita reikšminga informacija, susijusi su asmens duomenų saugumo pažeidimu.

30. Asmens duomenų saugumo pažeidimų registravimo žurnalą elektroninėmis priemonėmis tvarko ir saugo Agentūros duomenų apsaugos pareigūnas. Asmens duomenų saugumo pažeidimų registravimo žurnalo įrašai saugomi 3 metus nuo paskutinio įrašo žurnale padarymo.

VI SKYRIUS
BAIGIAMOSIOS NUOSTATOS

31. Agentūros darbuotojai su šiuo Tvarkos aprašu yra supažindinami DBSIS priemonėmis.

32. Agentūros darbuotojai, pažeidę šio Tvarkos aprašo reikalavimus, atsako Lietuvos Respublikos teisės aktų, reglamentuojančių atsakomybę už tarnybinius nusižengimus ir darbo pareigų pažeidimus, nustatyta tvarka.

_____

Pranešimo apie asmens duomenų saugumo pažeidimą Asmens su negalia teisių apsaugos agentūroje prie Lietuvos Respublikos socialinės apsaugos ir darbo ministerijos pateikimo tvarkos aprašo
1 priedas

(Tarnybinio pranešimo apie galimą asmens duomenų saugumo pažeidimą forma)

ASMENS SU NEGALIA TEISIŲ APSAUGOS AGENTŪROS
PRIE LIETUVOS RESPUBLIKOS SOCIALINĖS APSAUGOS IR DARBO MINISTERIJOS
_____ SKYRIAUS
(skyriaus pavadinimas)

_____
(pareigų pavadinimas)

Asmens su negalia teisių apsaugos agentūros
prie Lietuvos Respublikos socialinės apsaugos ir darbo ministerijos
direktoriui

TARNYBINIS PRANEŠIMAS
APIE GALIMĄ ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ

_____ Nr. _____
(data)

_____
(vieta)

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

1. Asmens duomenų saugumo pažeidimo data ir laikas:
1.1. Asmens duomenų saugumo pažeidimo data ir tikslus laikas _____
1.2. Asmens duomenų saugumo pažeidimo nustatymo data ir tikslus laikas _____
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 _____
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)

4. Apytikslis duomenų subjektų, kurių asmens duomenų saugumas pažeistas, skaičius: _____

5. Duomenų subjektų, kurių asmens duomenų saugumas pažeistas, kategorijos (atskiriamos pagal jai būdingą požymį):

_____

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):

_____

☐ Prisijungimo duomenys ir (ar) asmens identifikaciniai numeriai (pavyzdžiui, asmens kodas, slaptažodžiai):

_____

☐ Kiti:

_____

☐ Nežinomi (pranešimo teikimo metu):

_____

1.7. Apytikslis asmens duomenų, kurių saugumas pažeistas, skaičius:

_____

1.8. Kita reikšminga informacija apie asmens duomenų saugumo pažeidimą:

_____

_____

_____

_____

_____

_____	_____	_____
(pareigos)	(parašas)	(vardas, pavardė)

_____

Pranešimo apie asmens duomenų saugumo pažeidimą Asmens su negalia teisių apsaugos agentūroje prie Lietuvos Respublikos socialinės apsaugos ir darbo ministerijos pateikimo tvarkos aprašo
2 priedas

(Asmens duomenų saugumo pažeidimo ataskaitos forma)

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMO ATASKAITA

_____ Nr. _____
(data)

1. Asmens duomenų saugumo pažeidimo aprašymas	
1.1. Asmens duomenų saugumo pažeidimo nustatymo data, valanda (minučių tikslumu) ir vieta	
1.2. Darbuotojas, pranešęs apie asmens duomenų saugumo pažeidimą (vardas, pavardė, Asmens su negalia teisių apsaugos agentūros prie Lietuvos Respublikos socialinės apsaugos ir darbo ministerijos struktūrinio padalinio, kuriame dirba darbuotojas, pavadinimas, telefono Nr., elektroninio pašto adresas)	
1.3. Duomenų tvarkytojo, pranešusio apie asmens duomenų saugumo pažeidimą, pavadinimas, jo kontaktinio asmens duomenys (vardas, pavardė, telefono Nr., elektroninio pašto adresas)	
1.4. Asmens duomenų saugumo pažeidimo padarymo data ir vieta	
1.5. Asmens duomenų saugumo pažeidimo pobūdis, esmė ir aplinkybės	
1.5.1. Asmens duomenų konfidencialumo praradimas (kai asmens duomenys netyčia arba neteisėtai atskleidžiami arba gaunama prieiga prie jų)	
1.5.2. Asmens duomenų vientisumo praradimas (kai asmens duomenys netyčia arba neteisėtai pakeičiami)	
1.5.3. Asmens duomenų prieinamumo praradimas (kai netyčia arba neteisėtai prarandama prieiga prie asmens duomenų arba jie sunaikinami)	
1.6. Duomenų subjektų kategorijos ir jų skaičius	
1.7. Kaip ilgai tęsėsi asmens duomenų saugumo pažeidimas?	
1.8. Asmens duomenų kategorijos, susijusios su asmens duomenų saugumo pažeidimu:	

1.8.1. Asmens duomenys	
1.8.2. Specialių kategorijų asmens duomenys	
1.9. Apytikslis asmens duomenų, kurių saugumas pažeistas, skaičius	
2. Asmens duomenų saugumo pažeidimo rizikos įvertinimas	
2.1. Priežastys, lėmusios asmens duomenų saugumo pažeidimą (pvz., duomenų ar įrangos, kurioje yra saugomi asmens duomenys, vagystė, netinkamos prieigos kontrolės priemonės, leidžiančios neteisėtai naudotis asmens duomenimis, įrangos gedimas, žmogiška klaida, įsilaužimo ataka ir pan.)	
2.2. Asmens duomenų saugumo pažeidimo pasekmės:	
2.2.1. Atsitiktinai arba neteisėtai sunaikinti asmens duomenys	
2.2.2. Atsitiktinai arba neteisėtai prarasti asmens duomenys	
2.2.3. Atsitiktinai arba neteisėtai pakeisti asmens duomenys	
2.2.4. Be duomenų subjekto sutikimo atskleisti asmens duomenys	
2.2.5. Sudaryta galimybė naudotis asmens duomenimis	
2.2.6. Asmens duomenų išplitimas labiau nei tai yra būtina ir duomenų subjekto kontrolės praradimas savo asmens duomenų atžvilgiu	
2.2.7. Skirtingos informacijos susiejimas	
2.2.8. Asmens duomenų panaudojimas neteisėtais tikslais	
2.2.9. Dėl asmens duomenų trūkumo negalima teikti paslaugų	
2.2.10. Dėl klaidų asmens duomenų tvarkymo procesuose negalima teikti tinkamos paslaugos	
2.2.11. Kita	
2.3. Ar pažeistų asmens duomenų pobūdis kelia didesnę žalos riziką?	
2.4. Dėl asmens duomenų saugumo pažeidimo nėra pavojaus fizinių asmenų teisėms ir laisvėms (žema rizikos tikimybė)	
2.5. Dėl asmens duomenų saugumo pažeidimo yra / gali kilti pavojus fizinių asmenų teisėms ir laisvėms (būtina pranešti Inspekcijai) (vidutinė rizikos tikimybė)	
2.6. Dėl asmens duomenų saugumo pažeidimo yra / gali kilti didelis pavojus fizinių asmenų teisėms ir laisvėms (būtina pranešti Inspekcijai ir duomenų subjektams) (didelė (aukšta) rizikos tikimybė)	
2.7. Kas turėjo prieigą prie pažeistų asmens duomenų iki asmens duomenų saugumo pažeidimo padarymo?	
2.8. Kas gavo prieigą prie pažeistų asmens duomenų?	
2.9. Ar buvo kokių kitų įvykių, kurie galėjo turėti poveikį asmens duomenų saugumo pažeidimo padarymui?	

2.10. Ar iki asmens duomenų saugumo pažeidimo asmens duomenys buvo tinkamai užkoduoti, anonimizuoti ar kitaip lengvai neprieinami?	
2.11. IT sistemos, įrenginiai, įranga, įrašai, susiję su asmens duomenų saugumo pažeidimu	
2.12. Ar tai yra sisteminė klaida ar vienetinis incidentas?	
2.13. Kokia žala buvo padaryta duomenų subjektui ar Agentūrai (tapatybės vagystė, grėsmė fiziniam saugumui ir emocinei gerovei, žala reputacijai, teisinė atsakomybė, konfidencialumo, saugumo nuostatų pažeidimas ir pan.)?	
2.14. Kokių veiksmų / priemonių buvo imtasi sužinojus apie padarytą asmens duomenų saugumo pažeidimą?	
2.15. Kokios taikytos priemonės, siekiant sumažinti poveikį duomenų subjektams?	
2.16. Kokios techninės priemonės buvo taikomos asmens duomenų saugumo pažeidimo paveiktiems asmens duomenims, užtikrinant, kad asmens duomenys nebūtų prieinami neįgaliotiems asmenims?	
2.17. Techninės ir / ar organizacinės saugumo priemonės, kurios įgyvendintos dėl asmens duomenų saugumo pažeidimo, taip pat siekiant, kad pažeidimas nepasikartotų	
2.18. Techninės ir / ar organizacinės saugumo priemonės, kurios ketinamos įgyvendinti dėl asmens duomenų saugumo pažeidimo, įskaitant ir priemones sumažinti asmens duomenų saugumo pažeidimo pasekmėms	
3. Pranešimų pateikimas	
3.1. Ar pranešta duomenų subjektui apie asmens duomenų saugumo pažeidimą:	
3.1.1. Taip	
3.1.2. Ne	
3.1.3. Bus informuota vėliau	
3.1.4. Duomenų subjektas tokią informaciją jau turi	
3.2. Pranešimo duomenų subjektui būdas (paštu, elektroninio pašto pranešimu ar SMS pranešimu ir kt.)	
3.3. Informuotų duomenų subjektų skaičius	
3.4. Ar pranešta Inspekcijai apie asmens duomenų saugumo pažeidimą:	
3.4.1. Taip	
3.4.2. Ne	
3.5. Ar pranešta valstybės institucijoms, įgaliotoms atlikti ikiteisminį tyrimą, apie asmens duomenų saugumo pažeidimą, galimai turintį nusikalstamos veikos požymių:	
3.5.1. Taip	
3.5.2. Ne	
3.6. Ar pranešta valstybės institucijoms, nurodytoms Lietuvos Respublikos kibernetinio saugumo įstatyme, apie kibernetinį incidentą, susijusį su asmens duomenų saugumo pažeidimu:	

3.6.1. Taip	
3.6.2. Ne	
3.7. Nepranešimo apie asmens duomenų saugumo pažeidimą duomenų subjektui priežastys:	
3.7.1. ne, nes nekyla didelis pavojus duomenų subjektų teisėms ir laisvėms (nurodomos priežastys)	
3.7.2. ne, nes įgyvendintos tinkamos techninės ir organizacinės priemonės, užtikrinančios, kad asmeniui, neturinčiam leidimo susipažinti su asmens duomenimis, jie būtų nesuprantami (nurodomos kokios)	
3.7.3. ne, nes įgyvendintos tinkamos techninės ir organizacinės priemonės, užtikrinančios, kad nekiltų didelis pavojus duomenų subjektų teisėms ir laisvėms (nurodomos kokios)	
3.7.4. 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)	
3.7.5. ne, nes dar neidentifikuoti duomenų subjektai, kurių asmens duomenų saugumas pažeistas	
3.8. Vėlavimo pranešti duomenų subjektui apie asmens duomenų saugumo pažeidimą priežastys	
3.9. Nepranešimo apie asmens duomenų saugumo pažeidimą Inspekcijai priežastys	
3.10. Vėlavimo pranešti Valstybinei duomenų apsaugos inspekcijai apie asmens duomenų saugumo pažeidimą priežastys	

_____ _____ _____

(pareigos) (parašas) (vardas, pavardė)

_____

Pranešimo apie asmens duomenų saugumo pažeidimą Asmens su negalia teisių apsaugos agentūroje prie Lietuvos Respublikos socialinės apsaugos ir darbo ministerijos pateikimo tvarkos aprašo
3 priedas

(Asmens su negalia teisių apsaugos agentūros prie Lietuvos Respublikos socialinės apsaugos ir darbo ministerijos asmens duomenų saugumo pažeidimų registravimo žurnalo forma)

ASMENS SU NEGALIA TEISIŲ APSAUGOS AGENTŪRA
PRIE LIETUVOS RESPUBLIKOS SOCIALINĖS APSAUGOS IR DARBO MINISTERIJOS

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ REGISTRAVIMO ŽURNALAS

Eil. Nr.	**Asmens duomenų saugumo pažeidimo aprašymas**	**Pradžia *(*metai, mėnuo, diena, valanda*)***	**Pabaiga (metai, mėnuo, diena, valanda*)***	**Pašalino (vardas, pavardė, parašas)**	**Asmens duomenų saugumo pažeidimo ataskaitos data ir numeris**	**Asmens su negalia teisių apsaugos agentūros prie Lietuvos Respublikos socialinės apsaugos ir darbo ministerijos direktoriaus įgaliotas asmuo (vardas, pavardė, parašas)**

_____