

## **ASMENS DUOMENŲ TVARKYMO TAISYKLĖS**

### **I SKYRIUS BENDROSIOS NUOSTATOS**

1. Asmens duomenų tvarkymo taisyklių (toliau – Taisyklės) tikslas – reglamentuoti asmens duomenų tvarkymą Nacionaliniame transplantacijos biure prie Sveikatos apsaugos ministerijos (toliau – NTB). Jomis siekiama užtikrinti 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), Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo ir kitų teisės aktų, reglamentuojančių asmens duomenų tvarkymą ir apsaugą, laikymąsi ir įgyvendinimą.

2. Šios Taisyklės privalomos visiems NTB valstybės tarnautojams ir darbuotojams, dirbantiems pagal darbo sutartis (toliau – darbuotojai). Darbuotojai su Taisyklėmis supažindinami per Dokumentų valdymo sistemą.

3. NTB, veikdamas kaip asmens duomenų valdytojas ir tvarkytojas, užtikrina, kad asmens duomenys NTB būtų tvarkomi laikantis Reglamento (ES) 2016/679, Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo ir kitų teisės aktų nustatytą asmens duomenų tvarkymo reikalavimų.

4. NTB direktoriaus įsakymu skiriamas duomenų apsaugos pareigūnas, kuris vykdo Reglamento (ES) 2016/679 39 straipsnyje jam nustatytas užduotis. Asmens duomenų pareigūnu gali būti paskirtas NTB valstybės tarnautojas arba darbuotojas, dirbantis pagal darbo sutartį, taip pat dėl asmens duomenų pareigūno funkcijų vykdymo gali būti sudaryta paslaugų teikimo sutartis su asmeniu iš išorės.

5. Šiose Taisyklėse vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos Reglamente (ES) 2016/679 ir Lietuvos Respublikos teisės aktuose.

### **II SKYRIUS PAGRINDINIAI ASMENS DUOMENŲ TVARKYMO REIKALAVIMAI**

6. NTB asmens duomenys tvarkomi vadovaujantis Reglamento (ES) 2016/679 5 straipsnyje numatytais asmens duomenų tvarkymo principais ir tik esant Reglamento (ES) 2016/679 6 straipsnio 1 dalyje nurodytoms sąlygoms.

7. Asmens duomenys tvarkomi duomenų subjektui sutikus, kai tai tiesiogiai numatyta teisės aktuose arba, kai atsižvelgiant į duomenų tvarkymo tikslą ar duomenų apimtį NTB neturi kito teisinio pagrindo tvarkyti asmens duomenis ar įvykdyti kitus Reglamente (ES) 2016/679 nustatytus įpareigojimus visa apimtimi. Jeigu asmens duomenys atsižvelgiant į jų apimtį ir tvarkymo tikslus gali būti tvarkomi pagal bent vieną iš Reglamente (ES) 2016/679 įtvirtintų sąlygų, papildomo duomenų subjekto sutikimo neprašoma. Duomenų subjekto sutikimas gali būti gaunamas šiais būdais: raštu, įskaitant gautus elektroninėmis priemonėmis, žodžiu ar veiksmais, jeigu yra galimybė įrodyti, kad toks sutikimas buvo duotas, ir jeigu duomenų subjektas savo veiksmais aiškiai sutinka su siūlomu jo asmens duomenų tvarkymu. Visais atvejais sutikimas kaip asmens duomenų tvarkymo pagrindas turi atitikti Reglamento (ES) 2016/679 7 straipsnyje numatytas sąlygas.

8. Asmens duomenys NTB renkami tik teisės aktų nustatyta tvarka juos gaunant iš duomenų subjekto ar iš kitų asmenų, taip pat iš reikalingą informaciją tvarkančių ir turinčių teisę ją teikti subjektų

pagal prašymą (vienkartinio asmens duomenų rinkimo atveju) arba pagal asmens duomenų teikimo sutartį (daugkartinio asmens duomenų rinkimo atveju).

9. Asmens duomenys tvarkomi neautomatiniu (susistemintose rinkmenose) ir (arba) automatiniu būdu.

10. NTB dokumentai, kuriuose yra asmens duomenų, valdomi Dokumentų valdymo sistemoje vadovaujantis NTB direktoriaus įsakymu patvirtintu darbo reglamentu.

11. Asmens duomenys saugomi ne ilgiau, negu to reikalauja duomenų tvarkymo tikslai. Dokumentų su asmens duomenimis saugojimo terminai nustatomi NTB direktoriaus patvirtintame kasmetiniame dokumentacijos plane. Asmens duomenų, esančių informacinėse sistemose, saugojimo terminus nustato informacinių sistemų nuostatai. Kai asmens duomenys neberekalingi jų tvarkymo tikslams, jie yra sunaikinami, išskyrus tuos, kurie įstatymų nustatytais atvejais turi būti perduoti Lietuvos valstybės naujajam archyvui.

12. NTB įgyvendina ir užtikrina organizacines ir technines priemones, skirtas asmens duomenims apsaugoti nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, taip pat nuo bet kokio kito neteisėto tvarkymo.

13. Konkretūs asmens duomenų tvarkymo tikslai, teisiniai pagrindai, tvarkomi asmens duomenys, jų saugojimo terminai, organizacinės ir techninės saugumo priemonės nurodomi Duomenų tvarkymo veiklos, už kurią NTB atsako, įrašuose.

14. Reglamento (ES) 2016/679 35 straipsnyje nustatytais atvejais ir tvarka prieš pradėdant tvarkyti asmens duomenis NTB atliekamas poveikio asmens duomenų apsaugai vertinimas. Atlikdami poveikio duomenų apsaugai vertinimą darbuotojai (struktūriniai padaliniai), atsakingi už asmens duomenų tvarkymą, konsultuojasi su duomenų apsaugos pareigūnu. Jeigu pagal Reglamento (ES) 2016/679 35 straipsnį atliktame poveikio duomenų apsaugos vertinime nurodyta, kad tvarkant asmens duomenis kiltų didelis pavojus fizinių asmenų teisėms ir laisvėms NTB nesiėmus priemonių pavojui sumažinti, taip pat kitais įstatymų numatytais atvejais, NTB, prieš pradėdama tvarkyti asmens duomenis, konsultuojasi su Valstybine duomenų apsaugos inspekcija jos nustatyta tvarka.

15. Teisės aktų nustatytais atvejais ir tvarka NTB teikia jos tvarkomus asmens duomenis valstybės registrų ir valstybės informacinių sistemų valdytojams ir (arba) tvarkytojams, valstybės ir savivaldybių institucijoms, įstaigoms, organizacijoms ir kitiems asmenims, kuriems asmens duomenis teikti NTB įpareigoja įstatymai ar kiti teisės aktai arba kuriems NTB teisės aktų nustatyta tvarka vykdydama savo funkcijas teikia asmens duomenis, taip pat pagal duomenų gavėjų prašymus (vienkartinio teikimo atveju) arba NTB ir duomenų gavėjų sudarytas asmens duomenų teikimo sutartis (daugkartinio teikimo atveju). Sutartyje turi būti nurodytas asmens duomenų naudojimo tikslas, teikimo ir gavimo teisinis pagrindas, sąlygos, tvarka ir teikiamų asmens duomenų apimtis. Prašyme turi būti nurodytas asmens duomenų naudojimo tikslas, teikimo bei gavimo teisinis pagrindas ir prašomų pateikti asmens duomenų apimtis. Kai asmens duomenys tvarkomi automatiniu būdu ir taikomos tinkamos duomenų saugumą užtikrinančios priemonės, teikiant asmens duomenis pagal NTB ir duomenų gavėjo sudarytą asmens duomenų teikimo sutartį prioritetą turi būti teikiamas automatiniame duomenų teikime, o teikiant asmens duomenis pagal duomenų gavėjo prašymą, – duomenų teikimui elektroninėmis priemonėmis.

### **III SKYRIUS**

#### **REIKALAVIMAI ASMENIMS, TVARKANTIEMS ASMENS DUOMENIS**

16. Prieiga prie asmens duomenų gali būti suteikta tik tam NTB darbuotojui, kuriam asmens duomenys yra reikalingi jo funkcijoms vykdyti.

17. Su asmens duomenimis galima atlikti tik tuos veiksmus, kuriems atlikti NTB darbuotojui yra suteiktos teisės.

18. NTB darbuotojas, tvarkantis asmens duomenis, privalo:

18.1. laikytis pagrindinių asmens duomenų tvarkymo principų ir saugumo reikalavimų, įtvirtintų Reglamente (ES) 2016/679, Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatyme, šiose Taisyklėse ir kituose teisės aktuose;

18.2. laikytis konfidencialumo principo ir laikyti paslapyje bet kokią su asmens duomenimis susijusią informaciją, su kuria jis susipažino vykdydamas savo funkcijas, išskyrus atvejus, kai tokia informacija pagal galiojančių įstatymų ar kitų teisės aktų nuostatas buvo vieša. Pareiga saugoti asmens duomenų paslaptį galioja ir perėjus dirbti į kitas pareigas ar pasibaigus įgaliojimams, valstybės tarnybos ar darbo santykiams NTB;

18.3. laikytis organizacinių ir techninių asmens duomenų saugumo priemonių, kad būtų užkirstas kelias netyčiniam ar neteisėtam tvarkomų asmens duomenų sunaikinimui, praradimui, pakeitimui, atskleidimui, taip pat bet kokiam kitam neteisėtam tvarkymui, saugoti dokumentus, duomenų rinkmenas bei duomenų bazėse saugomus duomenis ir vengti perteklinių jų kopijų darymo;

18.4. neatskleisti, neperduoti ir nesudaryti sąlygų bet kokiomis priemonėmis susipažinti su asmens duomenimis asmeniui, kuris nėra įgaliotas tvarkyti asmens duomenų;

18.5. nedelsiant pranešti NTB direktoriui ir duomenų apsaugos pareigūnui apie bet kokią įtartina situaciją, kuri gali kelti grėsmę NTB tvarkomų asmens duomenų saugumui;

18.6. laikytis kitų šiose Taisyklėse ir asmens duomenų apsaugą reglamentuojančiuose teisės aktuose nustatytų reikalavimų.

19. NTB darbuotojas netenka teisės tvarkyti asmens duomenų, kai pasibaigia NTB darbuotojo įgaliojimai, valstybės tarnybos ar darbo santykiai su NTB arba kai jam pavedama vykdyti su duomenų tvarkymu nesusijusias funkcijas.

#### **IV SKYRIUS ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ VALDYMAS**

26. Už asmens duomenų saugumo pažeidimų valdymą NTB atsakingas NTB direktorius ir duomenų apsaugos pareigūnas.

27. NTB darbuotojas, sužinojęs arba pats nustatęs galimą asmens duomenų saugos pažeidimą, nedelsdamas informuoja NTB direktorių ir raštu ar elektroninėmis priemonėmis praneša duomenų apsaugos pareigūnui užpildydamas Taisyklėse patvirtintą Pranešimo apie duomenų saugumo pažeidimą formą (Taisyklių 3 priedas).

28. Duomenų apsaugos pareigūnas, sužinojęs apie galimą asmens duomenų saugumo pažeidimą, nedelsdamas išnagrinėja pranešime nurodytas aplinkybes, atlieka galimai padaryto asmens duomenų saugumo pažeidimo tyrimą, įvertina, ar buvo padarytas asmens duomenų saugumo pažeidimas.

29. Jei asmens duomenų saugumo pažeidimas buvo padarytas, nustato pažeidimo pobūdį, tipą (asmens duomenų konfidencialumo, vientisumo ir (arba) prieinamumo pažeidimas), aplinkybes, apytikslį duomenų subjektų, kurių asmens duomenų saugumas pažeistas, skaičių, asmens duomenų, kurių saugumas pažeistas, kategorijas (asmens tapatybę patvirtinantys asmens duomenys, specialių kategorijų asmens duomenys, prisijungimo duomenys ir (arba) asmens identifikaciniai numeriai ir kt.) ir apimtis, tikėtinas asmens duomenų saugumo pažeidimo pasekmės, pavojus fizinių asmenų teisėms ir laisvėms, imasi priemonių pažeidimui pašalinti ir (arba) neigiamoms pažeidimo pasekmėms sumažinti.

30. Duomenų apsaugos pareigūnas turi teisę pasitelkti ne tik su asmens duomenų saugumo pažeidimu susijusius darbuotojus, bet ir kitus darbuotojus (informacinių technologijų specialistus ir pan.), jei tai būtina. Per duomenų apsaugos pareigūno nurodytą terminą darbuotojai pateikia duomenų apsaugos pareigūnui jo prašomą informaciją, susijusią su asmens duomenų saugos pažeidimu ir jo tyrimu.

31. Atlikęs asmens duomenų saugumo pažeidimo tyrimą duomenų apsaugos pareigūnas surašo išvadą (Taisyklių 4 priedas), kurioje įvertinamas asmens duomenų pažeidimo faktas ir jo keliamas pavojus fizinių asmenų teisėms bei laisvėms. Išvada pateikiama NTB direktoriui, kuris priima sprendimą dėl tolesnių veiksmų, susijusių su asmens duomenų saugumo pažeidimu.

32. Duomenų apsaugos pareigūnas nedelsdamas ir, jei įmanoma, ne vėliau kaip per 72 valandas nuo sužinojimo apie asmens duomenų saugumo pažeidimą, praneša Valstybinei duomenų apsaugos inspekcijai, išskyrus atvejus, kai, jo vertinimu, asmens duomenų saugumo pažeidimas neturėtų kelti pavojaus fizinių asmenų teisėms ir laisvėms. Jeigu po pranešimo Valstybinei duomenų apsaugos inspekcijai apie asmens duomenų saugumo pažeidimą pateikimo atlikus tolesnį tyrimą yra nustatoma, kad saugumo pažeidimo

incidentas buvo sustabdytas ir faktiškai nebuvo jokio asmens duomenų saugumo pažeidimo, apie tai informuojama Valstybinė duomenų apsaugos inspekcija ir pažymima Asmens duomenų saugumo pažeidimų žurnale.

33. Tais atvejais, kai atsižvelgiant į asmens duomenų pažeidimo pobūdį yra būtina atlikti išsamesnį tyrimą ir nustatyti svarbius faktus, susijusius su asmens duomenų pažeidimu ir per 72 val. nuo sužinojimo apie asmens duomenų pažeidimą neįmanoma pranešti Valstybinei duomenų apsaugos inspekcijai, duomenų apsaugos pareigūnas informaciją apie asmens duomenų pažeidimą teikia Valstybinei duomenų apsaugos inspekcijai nurodydamas vėlavimo priežastis ir etapais paaiškindamas, kodėl visos informacijos neįmanoma pateikti iš karto.

34. Pranešimas apie asmens duomenų saugumo pažeidimą pateikiamas Valstybinės duomenų apsaugos inspekcijai vadovaujantis Pranešimo apie asmens duomenų saugumo pažeidimą pateikimo Valstybinei duomenų apsaugos inspekcijai tvarkos aprašo, patvirtinto Valstybinės duomenų apsaugos 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<sup>1</sup> užpildant Pranešimo apie asmens duomenų saugumo pažeidimą rekomenduojamą 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“.<sup>2</sup>

35. Vertinant asmens duomenų saugumo pažeidimą laikoma, kad asmens duomenų saugumo pažeidimas, galintis kelti didelį pavojų fizinių asmenų teisėms ir laisvėms, yra toks, dėl kurio laiku nesiėmus tinkamų priemonių fizinis asmuo gali patirti kūno sužalojimą, materialinę ar nematerialinę žalą (gali kilti diskriminacija, būti pavogta ar suklastota tapatybė, būti padaryta finansinių nuostolių, pakenkta reputacijai, prarastas asmens duomenų, kurie saugomi profesine paslaptimi, konfidencialumas, padaryta didelė ekonominė ar socialinė žala, kai duomenų subjektai gali netekti galimybės naudotis savo teisėmis ir laisvėmis ar jiems užkertamas kelias kontroliuoti savo asmens duomenis, gali būti paviešinti specialiu kategorijų, pažeidžiamų fizinių asmenų asmens duomenys ir (ar) asmens duomenys apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas arba susijusias saugumo priemones ir kt.)

36. Tyrimo metu, įvertinus visas asmens duomenų saugumo pažeidimo aplinkybes ir nustačius, kad asmens duomenų saugumo pažeidimas kelia pavojų fizinių asmenų teisėms ir laisvėms, nustatoma rizikos tikimybė: maža (žema); vidutinė; didelė (aukšta).

37. Duomenų apsaugos pareigūnas nustatęs didelį pavojų fizinių asmenų teisėms ir laisvėms, apie pažeidimą nedelsdamas praneša duomenų subjektui: duomenų subjektui aiškia ir paprasta kalba aprašomas duomenų saugumo pažeidimo pobūdis, nurodomas duomenų apsaugos pareigūno arba kito kontaktinio asmens, galinčio suteikti daugiau informacijos, vardas, pavardė ir kontaktiniai duomenys (telefono numeris, elektroninio pašto adresas), aprašomos tikėtinos asmens duomenų saugumo pažeidimo pasekmės ir priemonės, kurių buvo imtasi arba pasiūlyta imtis, kad būtų pašalintas asmens duomenų saugumo pažeidimas, taip pat priemonės galimoms neigiamoms jo pasekmėms sumažinti bei pagal galimybes atitinkamam fiziniam asmeniui skirtos rekomendacijos, kaip sumažinti galimą neigiamą poveikį (pasikeisti prisijungimo slaptažodžius neteisėtos prieigos prie asmens duomenų atveju ir kt.).

38. Apie asmens duomenų saugumo pažeidimą duomenų subjektui pranešti neprivaloma, jei:

38.1. NTB įgyvendino tinkamas technines ir organizacines apsaugos priemones ir tos priemonės taikytos asmens duomenims, kuriems asmens duomenų saugumo pažeidimas turėjo poveikio;

38.2. iš karto po asmens duomenų saugumo pažeidimo NTB ėmėsi priemonių, kuriomis užtikrinama, kad nebegalėtų kilti didelis pavojus duomenų subjektų teisėms ir laisvėms;

38.3. tai pareikalautų neproporcingai daug pastangų. Tokiu atveju apie asmens duomenų saugumo pažeidimą paskelbiama viešai arba taikoma panaši priemonė, kuria duomenų subjektai būtų informuojami taip pat efektyviai.

39. Jeigu NTB veikia tik kaip duomenų tvarkytojas, sužinojęs apie asmens duomenų saugumo pažeidimus turi nedelsdamas apie tai raštu pranešti duomenų valdytojui. Pranešimą Valstybinei duomenų

<sup>1</sup> <https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/42316db191d411e8aa33fe8f0fea665f/asr>

<sup>2</sup> <https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/78750ef0abc311e8aa33fe8f0fea665f?positionInSearchResults=0&searchModelUUID=bfad13c1-7790-4de9-bf77-7d783a8d513d>

apsaugos inspekcijai ir (ar) duomenų subjektams NTB teikia tokiu atveju, jeigu turi duomenų valdytojo įgaliojimą arba jeigu tokia pareiga nustatyta sutartyje, pagal kurią duomenys yra tvarkomi.

41. Asmens duomenų pareigūnas visus asmens duomenų saugumo pažeidimo atvejus registruoja Asmens duomenų saugumo pažeidimų žurnale (elektroninė forma) pagal šiose Taisyklėse patvirtintą formą (Taisyklių 2 priedas). Informacija apie asmens duomenų saugumo pažeidimą į Asmens duomenų saugumo pažeidimų žurnalą įvedama ne vėliau kaip per 5 darbo dienas nuo išvados įregistravimo. Esant būtinybei, Asmens duomenų saugumo pažeidimų žurnale esanti informacija turėtų būti papildoma ir (ar) koreguojama. Duomenų apsaugos pareigūnas periodiškai peržiūri Asmens duomenų saugumo pažeidimų žurnale esančius įrašus ir kartu su NTB direktoriumi sprendžia, kokios prevencijos priemonės turėtų būti įgyvendintos bei kaip bus kontroliuojamas šių prevencijos priemonių įdiegimas, kad ateityje analogiški asmens duomenų saugumo pažeidimai nesikartotų.

## **VI SKYRIUS BAIGIAMOSIOS NUOSTATOS**

42. Jeigu įtariama, kad asmens duomenų saugos pažeidimas turi nusikalstamos veikos požymių, informacija apie galimą nusikalstamą veiką pateikiama valstybės institucijoms, įgaliotoms atlikti ikiteisminį tyrimą.

43. Taisyklės duomenų apsaugos pareigūno peržiūros įvykus organizacinių, sisteminių ar kitų pokyčių arba pasikeitus teisės aktų reikalavimams.

---

(Duomenų tvarkymo veiklos įrašų formos)

**DUOMENŲ TVARKYMO VEIKLOS, UŽ KURIAŲ ATSAKO NTB, ĮRAŠAI**

<b>Duomenų valdytojas:</b>											
Duomenų valdytojo (jei taikoma, ir bendro duomenų valdytojo) pavadinimas											
Pašto adresas			Telefono ryšio numeris			Elektroninio pašto adresas		Kitos ryšių priemonės (pvz., interneto svetainės adresas, el. siuntos pristatymo dėžutės adresas)			
<b>Duomenų apsaugos pareigūnas:</b>											
Duomenų apsaugos pareigūno vardas ir pavardė											
Pašto adresas			Telefono ryšio numeris			Elektroninio pašto adresas		Kitos ryšių priemonės			
Eil. Nr.	Duomenų tvarkymo tikslas	Asmens duomenų tvarkymo teisinis pagrindas	Duomenų subjektų kategorijos	Asmens duomenų kategorijos	Duomenų gavėjų kategorijos*	Asmens duomenų saugojimo, ištrynimo terminai	Bendras duomenų saugumo priemonių (nurodytų Reglamento (ES) 2016/679 32 str. 1 d.) aprašymas		Duomenų šaltiniai	Darbuotojai (struktūriniai padaliniai), atsakingi už asmens duomenų tvarkymą	Duomenų įvedimo, keitimo data (datos)
							Techninės saugumo priemonės	Organizacinės saugumo priemonės			
1.											
2.											
3.											
4.											
5.											
....											

\*Kai taikoma, asmens duomenų perdavimas trečiajai valstybei arba tarptautinei organizacijai, įskaitant tos trečiosios valstybės arba tarptautinės organizacijos pavadinimą, ir Reglamento (ES) 2016/679 49 straipsnio 1 dalies antroje pastraipoje nurodytais duomenų perdavimų atvejais tinkamų apsaugos priemonių dokumentai.

**SU VISŲ KATEGORIJŲ SU DUOMENŲ TVARKYMO VEIKLA, VYKDOMA DUOMENŲ VALDYTOJO VARDU, SUSIJĘ ĮRAŠAI**

<b>Duomenų tvarkytojas:</b>			
Duomenų tvarkytojo pavadinimas			
Pašto adresas	Telefono ryšio numeris	Elektroninio pašto adresas	Kitos ryšių priemonės <i>(pvz., interneto svetainės adresas, el. siuntos pristatymo dėžutės adresas)</i>
<b>Kiekvienas duomenų valdytojas (jei taikoma – ir jo atstovas), kurio vardu veikia duomenų tvarkytojas:</b>			
Duomenų valdytojo pavadinimas			
Pašto adresas	Telefono ryšio numeris	Elektroninio pašto adresas	Kitos ryšių priemonės <i>(pvz., interneto svetainės adresas, el. siuntos pristatymo dėžutės adresas)</i>
<b>Duomenų apsaugos pareigūnas (jei taikoma):</b>			
Duomenų apsaugos pareigūno vardas ir pavardė			
Pašto adresas	Telefono ryšio numeris	Elektroninio pašto adresas	Kitos ryšių priemonės
<b>Asmens duomenų perdavimas trečiajai valstybei arba tarptautinei organizacijai (kai taikoma):</b>			
Trečiosios valstybės arba tarptautinės organizacijos, kuriai perduodami asmens duomenys, pavadinimas:		Reglamento (ES) 2016/679 49 straipsnio 1 dalies antroje pastraipoje nurodytais duomenų perdavimų atvejais tinkamų apsaugos priemonių dokumentai:	
Kita informacija, susijusi su asmens duomenų perdavimu			
<b>Bendras duomenų saugumo priemonių (nurodytų Reglamento (ES) 2016/679 32 straipsnio 1 dalyje) aprašymas (kai įmanoma):</b>			
Techninės saugumo priemonės: <i>(pvz., programinė įranga yra nuolat atnaujinama, aprūpinta ugniasienėmis ir antivirusinėmis programomis, daromos atsarginės duomenų kopijos, atliekamas duomenų šifravimas ir t. t.)</i>		Organizacinės saugumo priemonės: <i>(pvz., informacinių sistemų ir duomenų bazių vartotojų teisių ribojimas ir kontrolė, asmenys, dirbantys su asmens duomenimis, yra saistomi teisės aktuose nustatytų konfidencialumo pareigų ir t. t.)</i>	
<b>Kita informacija</b> <i>(pvz., darbuotojai (skyriai), atsakingi už duomenų tvarkymą, nuorodos į kitus su duomenų apsauga susijusius dokumentus ir t. t.)</i>			
<b>Duomenų įvedimo, keitimo data (-os)</b>			



**(Pranešimo apie duomenų saugumo pažeidimą forma)**

**NACIONALINIO TRANSPLANTACIJOS BIURO PRIE LIETUVOS RESPUBLIKOS SVEIKATOS APSAUGOS MINISTERIJOS**

\_\_\_\_\_  
(skyriaus pavadinimas)

\_\_\_\_\_  
(pareigų pavadinimas)

\_\_\_\_\_  
(vardas, pavardė)

**PRANEŠIMAS**

**APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ**

1.	Asmens duomenų saugumo pažeidimo data, laikas ir vieta	(Nurodoma asmens duomenų saugumo pažeidimo data, laikas ir vieta)
2.	Asmens duomenų saugumo pažeidimo nustatymo data ir laikas	(Nurodoma asmens duomenų saugumo pažeidimo nustatymo data ir laikas)
3.	Asmens duomenų saugumo pažeidimo aplinkybės	(Nurodomos asmens duomenų saugumo pažeidimo aplinkybės: nurodoma, ar tai konfidencialumo pažeidimas, ar prieinamumo pažeidimas, ar vientisumo pažeidimas ir pateikiamas platesnis pažeidimo aplinkybių paaiškinimas)
4.	Apytikslis duomenų subjektų, kurių asmens duomenų saugumas pažeistas, skaičius ir kategorijos	(Nurodomas apytikslis fizinių asmenų, kurių asmens duomenų saugumas pažeistas, skaičius.
5.	Apytikslis asmens duomenų, kurių saugumas pažeistas, skaičius ir kategorijos	(Nurodomas apytikslis asmens duomenų, kurių saugumas pažeistas, skaičius. Nurodoma viena ar daugiau asmens duomenų, kurių saugumas pažeistas, kategorijų: 1. asmens identifikavimo duomenys;

		<p>2. asmens charakteristikos duomenys (fizinės charakteristikos duomenys; elgsenos duomenys; istoriniai duomenys; demografiniai duomenys);</p> <p>3. finansiniai duomenys (sąskaitos duomenys; duomenys apie nuosavybę; duomenys apie finansinius sandorius ir pajamas; kredito duomenys);</p> <p>4. socialiniai duomenys (profesiniai duomenys; viešojo gyvenimo duomenys; šeimos duomenys; komunikacijos duomenys; socialinių ryšių duomenys; dalyvavimo duomenys; duomenys apie socialines paslaugas);</p> <p>5. vietos nustatymo ir kontaktiniai duomenys (technologinių prietaisų duomenys; kontaktiniai duomenys; vietos nustatymo duomenys);</p> <p>6. specialių kategorijų duomenys (informacija, atskleidžianti asmens rasinę ar etninę kilmę, politines pažiūras, religinius ar filosofinius įsitikinimus ar narystę profesinėse sąjungose, taip pat genetiniai duomenys, biometriniai duomenys, sveikatos duomenys arba duomenys apie asmens lytinį gyvenimą ir lytinę orientaciją);</p> <p>7. kiti duomenys.</p>
6.	Tikėtinos asmens duomenų saugumo pažeidimo pasekmės	(Nurodomos tikėtinos asmens duomenų saugumo pažeidimo pasekmės, pavyzdžiui: kūno sužalojimas; turtinė ar neturtinė žala; diskriminacija; pavogta ar suklastota tapatybė; finansiniai nuostoliai; pakenkta reputacijai; atskleista profesinė paslaptis; prarasta galimybė naudotis savo teisėmis; užkertamas kelias kontroliuoti savo duomenis ir t. t.)
7.	Priemonės, kurių jau imtasi arba siūloma imtis, kad būtų pašalintas asmens duomenų saugumo pažeidimas arba kad būtų sumažintos jo sukeltos pasekmės	(Nurodomos priemonės, kurių jau imtasi pašalinti asmens duomenų saugumo pažeidimą arba sumažinti jo sukeltas pasekmes; jeigu priemonių nebuvo imtasi, nurodyti, kokių priemonių siūloma imtis)
8.	Kita reikšminga informacija	

(pareigos)

(parašas)

(vardas ir pavardė)

(Asmens duomenų saugumo pažeidimo išvados forma)

**ASMENS DUOMENŲ SAUGUMO PAŽEIDIMO IŠVADA**

\_\_\_\_\_ Nr. \_\_\_\_\_  
(data) \_\_\_\_\_  
\_\_\_\_\_ (vieta)

<b>1. Asmens duomenų saugumo pažeidimo aprašymas</b>	
1.1. Asmens duomenų saugumo pažeidimo nustatymo data, laikas (valanda, minutės)	
1.2. Darbuotojas, pranešęs apie pažeidimą (vardas ir pavardė, telefono numeris, elektroninio pašto adresas)	
1.3. Duomenų tvarkytojo, pranešusio apie pažeidimą, pavadinimas, jo kontaktinio asmens duomenys (vardas ir pavardė, telefono Nr., elektroninio pašto adresas)	
1.4. Pažeidimo data, laikas (valanda, minutės)	
1.5. Pažeidimo vieta (adresas, informacinės sistemos pavadinimas, duomenų bazė, įrenginys ir pan.)	
1.6. Pažeidimo esmė ir aplinkybės	
1.6.1. Susijusios faktinės aplinkybės:	

1.6.2. Asmens duomenų konfidencialumo praradimas (be leidimo ar neteisėtai atskleidžiami asmens duomenys arba gaunama prieiga prie jų)	
1.6.3. Asmens duomenų vientisumo praradimas (kai asmens duomenys pakeičiami be leidimo ar netyčia)	
1.6.4. Asmens duomenų prieinamumo praradimas (kai netyčia arba neteisėtai prarandama prieiga prie jų arba sunaikinami asmens duomenys)	
1.7. Duomenų subjektų, kurių duomenų saugumas pažeistas, kategorijos ir šių duomenų subjektų apytikslis skaičius (jei įmanoma)	
1.8. Pažeidimo trukmė	
1.9. Asmens duomenų, kurių saugumas pažeistas, kategorijos (jei įmanoma):	
1.9.1. Asmens duomenys (išvardyti kategorijas)	
1.9.2. Specialių kategorijų asmens duomenys (išvardyti kategorijas)	
1.9.3. Asmens duomenų įrašų apytikslis skaičius	
<b>2. Pažeidimo rizikos įvertinimas</b>	
2.1. Priežastys bei įvykiai, turėję įtakos įvykti pažeidimui (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. Pažeidimo pasekmės (aprašyti tinkamas):	
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. Atsitiktinai arba neteisėtai atskleisti asmens duomenys teisės susipažinti su jais neturintiems asmenims (jei įmanoma, nurodomi neteisėtą priegią gavę asmenys)	
2.2.5. Asmens duomenų išplitimas labiau nei tai yra būtina ir duomenų subjekto kontrolės praradimas savo asmens duomenų atžvilgiu, pavyzdžiui, asmens duomenys išplito internete)	
2.2.6. Asmens duomenų panaudojimas neteisėtais tikslais	
2.2.7. Dėl asmens duomenų trūkumų negalima vykdyti funkcijų	
2.2.8. Dėl klaidų asmens duomenų tvarkymo procesuose negalima tinkamai vykdyti funkcijų	
2.2.9. Kita	
2.3. Rizikos tikimybė fizinių asmenų teisėms ir laisvėms (nurodyti tinkamą ir pateikti pagrindžiančius argumentus):	
2.3.1. Dėl pažeidimo nėra pavojaus fizinių asmenų teisėms ir laisvėms (maža tikimybė)	
2.3.2. Dėl pažeidimo yra ar gali kilti pavojus fizinių asmenų teisėms ir laisvėms (vidutinė tikimybė)	
2.3.3. Dėl Pažeidimo yra ar gali kilti didelis pavojus fizinių asmenų teisėms ir laisvėms (didelė tikimybė)	
2.4. Duomenų subjektui ir (ar) NTB padaryta žala (tapatybės vagystė, grėsmė fiziniam saugumui ir emocinei gerovei, žala reputacijai, teisinė atsakomybė, konfidencialumo, saugumo nuostatų pažeidimas ir pan.)	

2.5. Techninės ir (ar) organizacinės duomenų saugumo priemonės:	
2.5.1. Techninės ir (ar) organizacinės priemonės, kurios buvo taikomos asmens duomenims, kurių saugumas buvo pažeistas siekiant užtikrinti šių duomenų saugumą (aprašoma arba pridedami patvirtinantys dokumentai; išvada dėl tinkamumo)	
2.5.2. Techninės ir (ar) organizacinės saugumo priemonės, kurios įgyvendintos dėl įvykusio pažeidimo, taip pat siekiant, kad pažeidimas nepasikartotų ir būtų sumažintos pasekmės duomenų subjektui (aprašoma arba pridedami patvirtinantys dokumentai)	
2.5.3. Techninės ir (ar) organizacinės saugumo priemonės, kurias planuojama įgyvendinti dėl įvykusio pažeidimo, taip pat siekiant, kad pažeidimas nepasikartotų ir būtų sumažintos pasekmės duomenų subjektui (aprašoma arba pridedami patvirtinantys dokumentai)	
2.6. Pažeidimo pakartotinumai:	
2.6.1. Tokio pobūdžio pažeidimas įvyko pirmą kartą	
2.6.2. Pakartotinis tokio pobūdžio pažeidimas	
<b>3. Pranešimų pateikimas</b>	
3.1. Pranešimas duomenų subjektui apie įvykusį pažeidimą;	
3.1.1. Pranešimo data, būdas, trumpas turinio aprašymas, informuotų duomenų subjektų skaičius	
3.1.2. Priežastys, dėl kurių nepranešta duomenų subjektui:	

3.1.2.1. Nekyla didelio pavojaus duomenų subjektų teisėms ir laisvėms	
3.1.2.2. Įgyvendintos tinkamos techninės ir organizacinės apsaugos priemonės ir tos priemonės taikytos asmens duomenims, kuriems asmens duomenų saugumo pažeidimas turėjo poveikio, visų pirma, tos priemonės, kuriomis užtikrinama, kad asmeniui, neturinčiam leidimo susipažinti su asmens duomenimis, jie būtų nesuprantami, pavyzdžiui, šifravimo priemonės	
3.1.2.3. Imtasi priemonių, kuriomis užtikrinama, kad nebegalėtų kilti didelio pavojaus duomenų subjektų teisėms ir laisvėms	
3.1.2.4. Pranešimas 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)	
3.2. Pranešimas Valstybės duomenų apsaugos inspekcijai apie pažeidimą:	
3.2.1. Pranešimo data, numeris	
3.2.2. Priežastys, dėl kurių nepranešta Valstybės duomenų apsaugos inspekcijai	
3.2.3. Pranešimo Valstybės duomenų apsaugos inspekcijai vėlavimo priežastys	
3.3. Pranešimas valstybės institucijoms, įgaliotoms atlikti ikiteisminį tyrimą, apie asmens duomenų saugumo pažeidimą, galimai turintį nusikalstamos veikos požymių (jei taikoma) (rašto data, numeris; adresatas)	

3.4. Pranešimas Nacionaliniam kibernetinio saugumo centrui apie NTB valdomose ir (ar) tvarkomose ryšių ir informacinėse sistemose įvykusį kibernetinį incidentą ir taikytas kibernetinių incidentų valdymo priemones (jei taikoma) (rašto data, numeris)	
--	--

---

*(pareigos)*

---

*(parašas)*

---

*(vardas ir pavardė)*