

PATVIRTINTA  
Šiaulių rajono savivaldybės  
priešgaisrinės tarnybos viršininko  
2019 m. liepos 8 d. įsakymu Nr. V-17

## **ŠIAULIŲ RAJONO SAVIVALDYBĖS PRIEŠGAISRINĖS TARNYBOS ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ, TYRIMO, PRANEŠIMO APIE JUOS IR DOKUMENTAVIMO TVARKA**

### **I SKYRIUS BENDROSIOS NUOSTATOS**

1. Šiaulių rajono savivaldybės priešgaisrinės tarnybos (toliau - Tarnyba) asmens duomenų saugumo pažeidimų, tyrimo, pranešimo apie juos ir dokumentavimo tvarka (toliau – Tvarka) parengta vadovaujantis 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamento (ES) 2016/679 dėl fizinių asmens apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (toliau-BDAR) 33 ir 34 straipsniais, Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu (2018-06-30 įstatymo Nr.XIII-1426 redakcija, toliau – Įstatymas) ir kitais galiojančiais teisės aktais.

2. Šioje Tvarkoje vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos Reglamente (ES) 2016/679.

### **II SKYRIUS PRANEŠIMO APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ PROCEDŪRA**

3. Šiaulių rajono savivaldybės priešgaisrinės tarnybos darbuotojas (toliau kartu – darbuotojai), sužinojęs, kad nebuvo užtikrintas asmens duomenų saugumas:

3.1. nedelsiant, bet ne vėliau kaip per 2 darbo valandas nuo asmens duomenų saugumo pažeidimo paaiškėjimo momento informuoja Tarnybos duomenų apsaugos pareigūną;

3.2. užpildo šio Aprašo 1 priede nurodytos formos Pranešimą apie asmens duomenų saugumo pažeidimą ir nedelsiant, bet ne vėliau kaip per 2 darbo valandas nuo pažeidimo paaiškėjimo momento perduoda jį Tarnybos duomenų apsaugos pareigūnui.

3.3. imasi priemonių pašalinti asmens duomenų saugumo pažeidimą ir priemonių galimoms neigiamoms jo pasekmėms sumažinti.

4. Duomenų tvarkytojai, sužinoję apie asmens duomenų saugumo pažeidimą, nedelsiant, bet ne vėliau kaip per 1 darbo dieną, apie tai praneša Tarnybai, pateikdami pranešimą, numatytą Reglamente (ES) 2016/679 33 straipsnio 3 dalyje.

5. Tarnybos duomenų apsaugos pareigūnas, gavęs Tarnybos darbuotojo užpildytą pranešimą ar duomenų tvarkytojo pranešimą (toliau – kartu pranešimas):

5.1. nedelsiant nagrinėja pranešime nurodytas aplinkybes;

5.2. įvertina, ar padarytas asmens duomenų saugumo pažeidimas;

5.3. jei asmens duomenų saugumo pažeidimas padarytas, nustato asmens duomenų kategorijas, įskaitant specialių kategorijų asmens duomenis, kurios buvo susijusios su pažeidimu, pažeidimo priežastys, lėmusios asmens duomenų saugumo pažeidimą, apimtis (duomenų subjektų kategorijos ir skaičius), žala padaryta asmeniui;

5.4. 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);

5.5. nustato, ar būtina nedelsiant pranešti duomenų subjektui apie asmens duomenų saugumo pažeidimą.

6. Duomenų tvarkytojai pateikia Tarnybos viršininkui visą jos prašomą informaciją, susijusią su informavimu apie asmens duomenų saugumo pažeidimą ir jo tyrimu.

7. Tarnybos duomenų apsaugos pareigūnas, atlikęs asmens duomenų saugumo pažeidimo tyrimą, surašo šioje Tvarkoje 2 priede nurodytos formos Asmens duomenų saugumo pažeidimo ataskaitą.

8. Atsižvelgiant į Asmens duomenų saugumo pažeidimo ataskaitą, prireikus priemonių planą, kuriame numatomas būtinų techninių, organizacinių, administracinių ir kitų priemonių poreikis dėl asmens duomenų saugumo pažeidimo, tvirtina, atsakingus vykdytojus paskiria ir įgyvendinimo terminus nustato Tarnybos viršininkas.

9. Tarnybos duomenų apsaugos pareigūnas nedelsiant ir, jei įmanoma, nepraėjus 72 valandoms nuo to laiko, kai buvo sužinota apie asmens duomenų saugumo pažeidimą, informuoja Inspekciją, pateikdamas Reglamento (ES) 2016/679 33 straipsnio 3 dalyje nurodytą informaciją.

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

11. Kai apie padarytą asmens duomenų saugumo pažeidimą privaloma informuoti Inspekciją ir per 72 valandas yra neįmanoma ištirti padarytą asmens duomenų saugumo pažeidimą, pranešime Inspekcijai yra pateikiama tuo metu prieinama informacija, nurodyta Reglamento (ES) 2016/679 33 straipsnio 3 dalyje, vėlavimo priežastys ir kada bus pateikta kita detalesnė informacija.

12. Tarnybos duomenų apsaugos pareigūnas nedelsiant ir, jei įmanoma, nepraėjus 72 valandoms nuo to laiko, kai buvo sužinota apie asmens duomenų saugumo pažeidimą, praneša apie asmens duomenų saugumo pažeidimą duomenų subjektui, kai dėl asmens duomenų saugumo pažeidimo gali kilti didelis pavojus fizinių asmenų teisėms ir laisvėms, Reglamento (ES) 2016/679 34 straipsnyje nustatyta tvarka, išskyrus šiame straipsnyje numatytas išimtis.

13. Duomenų subjektas gali būti informuojamas apie asmens duomenų saugumo pažeidimą vėliau, nesilaikant šio Aprašo 15 punkte nustatyto termino, jei yra įgyvendinamos tinkamos priemonės, kuriomis siekiama užkirsti kelią besikartojantiems ar panašiams asmens duomenų saugumo pažeidimams.

14. 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.

15. Susisiekimo ministerijos duomenų apsaugos pareigūnas informaciją apie asmens duomenų saugumo pažeidimą įrašo į šio Aprašo 3 priede nurodytos formos Asmens duomenų saugumo pažeidimų registravimo žurnalą.

---

Asmens duomenų saugumo pažeidimų, tyrimo,  
pranešimo apie juos ir dokumentavimo tvarkos  
aprašo  
1 priedas

## ŠIAULIŲ RAJONO SAVIVALDYBĖS PRIEŠGAISRINĖ TARNYBA

\_\_\_\_\_  
(pareigų pavadinimas)

\_\_\_\_\_  
(vardas, pavardė)

### PRANEŠIMAS APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ

\_\_\_\_\_ Nr. \_\_\_\_\_

Kuršėnai

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

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

\_\_\_\_\_

2. Asmens duomenų saugumo pažeidimo padarymo data, laikas ir vieta: \_\_\_\_\_

\_\_\_\_\_

3. Asmens duomenų saugumo pažeidimo pobūdis, esmė ir aplinkybės \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

4. Duomenų subjektų kategorijos (pvz., darbuotojai, asmenys, pateikę prašymus, skundus ir pan.)  
ir jų skaičius (jei žinoma) \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

5. Asmens duomenų kategorijos, susijusios su 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	
Genetiniai 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.)

---



---



---



---



---

\_\_\_\_\_  
(pareigos)

\_\_\_\_\_  
(vardas, pavardė)

Pranešimo apie asmens duomenų saugumo  
pažeidimą pateikimo tvarkos aprašo  
2 priedas

## ASMENS DUOMENŲ SAUGUMO PAŽEIDIMO ATASKAITA

\_\_\_\_\_ Nr. \_\_\_\_\_

(data) (rašto numeris)

<b>1. Asmens duomenų saugumo pažeidimo aprašymas</b>	
1.1. Asmens duomenų saugumo pažeidimo nustatymo data, valanda (minučių tikslumu) ir vieta	
1.2. Darbuotojas ar duomenų tvarkytojas, pranešęs apie asmens duomenų saugumo pažeidimą (padalinys, vardas, pavardė, telefonas, adresas)	
1.3. Asmens duomenų saugumo pažeidimo padarymo data ir vieta	
1.4. Asmens duomenų saugumo pažeidimo pobūdis, esmė ir aplinkybės	
1.5. Duomenų subjektų kategorijos ir jų skaičius	
1.6. Kaip ilgai tęsėsi asmens duomenų saugumo pažeidimas?	
1.7. Asmens duomenų kategorijos, susijusios su asmens duomenų saugumo pažeidimu:	
1.7.1. Asmens duomenys	

1.7.2. Specialių kategorijų asmens duomenys	
<b>2. Asmens duomenų saugumo pažeidimo rizikos įvertinimas</b>	
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. Kita	
2.3. Ar pažeistų asmens duomenų pobūdis kelia didesnę žalos riziką?	
2.4. Kas turėjo prieigą prie pažeistų asmens duomenų iki asmens duomenų saugumo pažeidimo padarymo?	

2.5. Kas gavo prieigą prie pažeistų asmens duomenų?	
2.6. Ar buvo kokių kitų įvykių, kurie galėjo turėti poveikį asmens duomenų saugumo pažeidimo padarymui?	
2.7. Ar iki asmens duomenų saugumo pažeidimo asmens duomenys buvo tinkamai užkoduoti, anonimizuoti ar kitaip lengvai neprieinami?	
2.8. IT sistemos, įrenginiai, įranga, įrašai, susiję su asmens duomenų saugumo pažeidimu	
2.9. Ar tai yra sisteminė klaida ar vienetinis incidentas?	
2.10. Kokia žala buvo padaryta duomenų subjektui ar Susisiekimo ministerijai (tapatybės vagystė, grėsmė fiziniam saugumui ir emocinei gerovei, žala reputacijai, teisinė atsakomybė, konfidencialumo, saugumo nuostatų pažeidimas ir pan.)?	
2.11. Kokių veiksmų/priemonių buvo imtasi sužinojus apie padarytą asmens duomenų saugumo pažeidimą?	
2.12. Kokios techninės priemonės buvo taikomos asmens duomenų saugumo pažeidimo paveiktiems asmens duomenims, užtikrinant, kad asmens duomenys nebūtų prieinami neįgaliesiems asmenims?	
2.13. Techninės ir/ar organizacinės saugumo priemonės, kurios įgyvendintos ar ketinamos įgyvendinti dėl asmens duomenų saugumo pažeidimo	
<b>3. Pranešimų pateikimas</b>	
3.1. Ar pranešta duomenų subjektui apie asmens duomenų saugumo pažeidimą:	

3.1.1. Taip	(Pranešimo turinys)
3.1.2. Ne	
3.2. Pranešimo duomenų subjektui būdas (elektroninio pašto pranešimu ar SMS pranešimu ir kt.)	
3.3. Ar pranešta Inspekcijai apie asmens duomenų saugumo pažeidimą:	
3.3.1. Taip	(rašto data ir numeris)
3.3.2. Ne	
3.4. Ar pranešta valstybės institucijoms, įgaliotoms atlikti ikiteisminį tyrimą, apie asmens duomenų saugumo pažeidimą, galimai turintį nusikalstamos veikos požymių:	
3.4.1. Taip	(rašto data ir numeris, adresatas)
3.4.2. Ne	
3.5. Ar pranešta valstybės institucijoms, nurodytoms Lietuvos Respublikos kibernetinio saugumo įstatyme, apie kibernetinį incidentą, susijusį su asmens duomenų saugumo pažeidimu:	
3.5.1. Taip	(rašto data ir numeris, adresatas)
3.5.2. Ne	
3.6. Nepranešimo apie asmens duomenų saugumo pažeidimą duomenų subjektui priežastys	
3.7. Vėlavimo pranešti duomenų subjektui apie asmens duomenų saugumo pažeidimą priežastys	
3.8. Nepranešimo apie asmens duomenų saugumo pažeidimą Inspekcijai priežastys	
3.9. Vėlavimo pranešti Inspekcijai apie asmens duomenų saugumo pažeidimą priežastys	
Susisiekimo ministerijos duomenų apsaugos pareigūnas	(vardas, pavardė, parašas)



