

PATVIRTINTA
Šiaulių miesto savivaldybės viešosios
bibliotekos direktoriaus
2018 m. gruodžio 18 d.
įsakymu Nr. V-134

PRANEŠIMO APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ ŠIAULIŲ MIESTO SAVIVALDYBĖS VIEŠOJOJE BIBLIOTEKOJE PATEIKIMO TVARKOS APRAŠAS

I SKYRIUS BENDROSIOS NUOSTATOS

1. Pranešimo apie asmens duomenų saugumo pažeidimą pateikimo tvarkos aprašas (toliau – Aprašas) nustato pranešimo apie asmens duomenų saugumo pažeidimo turinį, procedūrą, pateikimo duomenų subjektui ir Valstybinei duomenų apsaugos inspekcijai (toliau – Inspekcija) tvarką.
2. Šis Aprašas taikomas Šiaulių miesto savivaldybės viešajai bibliotekai (toliau – Biblioteka), tvarkant duomenų subjektų asmens duomenis.
3. Šis Aprašas parengtas, vadovaujantis 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentu (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (OL 2016 L 119, p. 1–88) (toliau – Reglamentas (ES) 2016/679).
4. Apraše vartojamos sąvokos:
 - 4.1. **Asmens duomenys (toliau – duomenys)** – bet kokia informacija arba jos visuma apie fizinį asmenį, pagal kurią galima nustatyti fizinio asmens tapatybę. Tokia informacija gali būti vardas ir pavardė, asmens kodas, buvimo vietos duomenys, elektroninis paštas, fizinės, fiziologinės, genetinės, psichinės, ekonominės, kultūrinės ar socialinės tapatybės duomenys.
 - 4.2. **Asmens duomenų saugumo pažeidimas** – saugumo pažeidimas, dėl kurio netyčia arba neteisėtai sunaikinami, prarandami, pakeičiami, be leidimo atskleidžiami gauti, saugomi arba kitaip tvarkomi duomenys arba prie jų be leidimo gaunama prieiga.
 - 4.3. **Darbuotojas** – Šiaulių miesto savivaldybės viešosios bibliotekos darbuotojas, dirbantis pagal darbo sutartį.
 - 4.4. **Duomenų subjektas** – fizinis asmuo, kurio duomenis tvarko Biblioteka.
5. Kitos Apraše vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos Reglamente (ES) 2016/679, Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatyme ir kituose teisės aktuose, reglamentuojančiuose asmens duomenų apsaugą.

II SKYRIUS PRANEŠIMO APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ PROCEDŪRA

6. Šiaulių miesto savivaldybės viešosios bibliotekos darbuotojas, dirbantis pagal darbo sutartį (toliau kartu – darbuotojai), sužinojęs, kad nebuvo užtikrintas asmens duomenų saugumas:
 - 6.1. nedelsiant, bet ne vėliau nei per 2 darbo valandas nuo asmens duomenų saugumo pažeidimo paaikšėjimo momento elektroniniu paštu, telefonu arba žodžiu informuoja savo tiesioginį vadovą ir Bibliotekos duomenų apsaugos pareigūną;
 - 6.2. imasi priemonių pašalinti asmens duomenų saugumo pažeidimą ir priemonių galimoms neigiamoms jo pasekmėms sumažinti;
 - 6.3. užpildo šio Aprašo I priede nurodytos formos Pranešimą apie asmens duomenų

saugumo pažeidimą ir nedelsiant perduoda jį Bibliotekos duomenų apsaugos pareigūnui.

7. Duomenų tvarkytojai, sužinoję apie asmens duomenų saugumo pažeidimą, nedelsiant, bet ne vėliau nei per 1 darbo dieną, apie tai praneša Bibliotekos duomenų apsaugos pareigūnui, pateikdami pranešimą, numatytą Reglamento (ES) 2016/679 33 straipsnio 3 dalyje.

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

8.1. nedelsdamas pradeda nagrinėti pranešime nurodytas aplinkybes;

8.2. įvertina, ar buvo padarytas asmens duomenų saugumo pažeidimas;

8.3. 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;

8.4. 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);

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

8.6. nustato, ar būtina pranešti Inspekcijai apie asmens duomenų saugumo pažeidimą.

9. Duomenų tvarkytojai pateikia Bibliotekai visą jos prašomą informaciją, susijusią su informavimu apie asmens duomenų saugumo pažeidimą ir jo tyrimu, per Bibliotekos nurodytą terminą.

10. Bibliotekos duomenų apsaugos pareigūnas, atlikęs asmens duomenų saugumo pažeidimo tyrimą, surašo šio Aprašo 2 priede nurodytos formos Asmens duomenų saugumo pažeidimo ataskaitą.

11. Asmens duomenų saugumo pažeidimo ataskaita yra pateikiama Bibliotekos direktoriui.

12. 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 Bibliotekos direktorius.

13. Tuo atveju, jei yra nustatoma, kad dėl įvykusio asmens duomenų saugumo pažeidimo duomenų tvarkytojas turi imtis papildomų veiksmų ar užtikrinti papildomas asmens duomenų saugumo priemones, Bibliotekos direktorius duoda privalomus nurodymus duomenų tvarkytojui, jei asmens duomenų saugumo pažeidimas susijęs su duomenų tvarkytojo tvarkomais valstybės registrais ar informacinėmis sistemomis.

14. Bibliotekos duomenų apsaugos pareigūnas nedelsiant ir, jei įmanoma, nepraėjus 72 valandoms nuo to laiko, kai buvo sužinota apie asmens duomenų saugumo pažeidimą, informuoja Inspekciją, pateikdamas užpildytą Pranešimo apie asmens duomenų saugumo pažeidimą rekomenduojamą formą, patvirtintą Valstybinės duomenų apsaugos inspekcijos direktoriaus 2018 m. gegužės 24 d. įsakymu Nr. 1T-53 (1.12) „Dėl pranešimo apie asmens duomenų saugumo pažeidimą rekomenduojamos formos patvirtinimo“.

15. Tuo atveju, kai Bibliotekos duomenų apsaugos pareigūnas nustato, kad asmens duomenų saugumo pažeidimas nekelia pavojaus fizinėms asmenų teisėms ir laisvėms, apie padarytą asmens duomenų saugumo pažeidimą Inspekcija nėra informuojama.

16. Kai apie padarytą asmens duomenų saugumo pažeidimą privaloma informuoti Inspekciją ir per 72 valandas yra neįmanoma iširti padaryto asmens duomenų saugumo pažeidimo, pranešime Inspekcijai yra pateikiama tuo metu prieinama informacija, nurodyta nurodomos vėlavimo priežastys ir kada bus pateikta kita detalesnė informacija.

17. Bibliotekos 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 elektroniniu paštu, raštu ar kitu būdu, kai dėl asmens duomenų saugumo pažeidimo gali kilti didelis pavojus fizinėms asmenų teisėms ir

laisvėms, pranešime pateikdamas šią informaciją:

- 17.1. duomenų valdytojo pavadinimas, juridinio asmens kodas, buveinės adresas;
- 17.2. Bibliotekos duomenų apsaugos pareigūno vardas, pavardė ir kontaktiniai duomenys;
- 17.3. pažeidimo pobūdžio ir tikėtinų pažeidimo pasekmių aprašymas;
- 17.4. priemonių, kurių ėmėsi arba pasiūlė imtis Bibliotekai, kad būtų pašalintas pažeidimas, įskaitant priemones galimoms neigiamoms pasekmėms sumažinti, aprašymą;
- 17.5. kitą reikšmingą informaciją, susijusią su pažeidimu, kuri, Bibliotekos manymu, turėtų būti pateikta duomenų subjektui.
18. Atvejai, kada pranešimas duomenų subjektui apie pažeidimą nereikalingas:
 - 18.1. Biblioteka įgyvendino tinkamas technines ir organizacines apsaugos priemones ir tos priemonės taikytos duomenims, kuriems asmens duomenų saugumo pažeidimas turėjo poveikio, visų pirma tas priemones, kuriomis užtikrinamas, kad asmeniui, neturinčiam leidimo susipažinti su duomenimis, jie būtų nesuprantami, pavyzdžiui, šifravimo priemonės.
 - 18.2. Biblioteka ėmėsi priemonių, kuriomis užtikrinama, kad nekiltų didelis pavojus duomenų subjektų teisėms ir laisvėms;
 - 18.3. pranešimas pareikalautų neproporcingai didelių pastangų. Tokiu atveju apie pažeidimą viešai paskelbiama Bibliotekos interneto svetainėje arba taikoma panaši priemonė, kuria duomenų subjektai būtų informuojami taip pat efektyviai.
19. Jei Inspekcija, apsvarsčiusi tikimybę, kad dėl pažeidimo kils didelis pavojus, pareikalauja, kad Biblioteka informuotų duomenų subjektą apie asmens duomenų saugumo pažeidimą, Biblioteka nedelsdama praneša duomenų subjektui apie asmens duomenų saugumo pažeidimą.
20. Duomenų tvarkytojai suteikia Bibliotekai pagalbą, kurios reikia, kad būtų tinkamai pranešta apie asmens duomenų saugumo pažeidimą duomenų subjektui.
21. 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.
22. 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.

III SKYRIUS BAIGIAMOSIOS NUOSTATOS

23. Darbuotojai privalo Bibliotekos asmens duomenų apsaugos pareigūnui pateikti visą informaciją, susijusią su asmens duomenų saugumo pažeidimu, taip pat konsultuoti Bibliotekos duomenų apsaugos pareigūną ir kitais jų kompetencijai priskirtais būdais padėti sustabdyti asmens duomenų saugumo pažeidimą ir (arba) sumažinti jo sukeltus padarinius.

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

25. Asmens duomenų saugumo pažeidimų registravimo žurnalas ir Asmens duomenų saugumo pažeidimo ataskaitos saugo Bibliotekos asmens duomenų apsaugos pareigūnas.

Pranešimo apie asmens duomenų
saugumo pažeidimą pateikimo tvarkos
aprašo
1 priedas

(Pranešimo forma)

ŠIAULIŲ MIESTO SAVIVALDYBĖS VIEŠOJI BIBLIOTEKA

_____ (struktūrinio padalinio pavadinimas)

_____ (pareigų pavadinimas)

_____ (vardas, pavardė)

**PRANEŠIMAS
APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ**

_____ Nr. _____ Vilnius

Informuoju apie 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 _____ Laikas _____

1.2. Asmens duomenų saugumo pažeidimo nustatymo:

Data _____ Laikas _____

2. Asmens duomenų saugumo pažeidimo vieta (pažymėti tinkamą (-us):

- Informacinė sistema
- Duomenų bazė
- Tarnybinė stotis
- Internetinė svetainė
- Debesų kompiuterijos paslaugos
- Nešiojami / mobilūs 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 patvirtinantis 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):

Duomenys apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas:

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

Kiti:

Nežinomi (pranešimo teikimo metu)

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

8. 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 skirtose vietose palikti dokumentai su asmens duomenimis ir pan.)_____:

(pareigos)

(vardas, pavardė, parašas)

Pranešimo apie asmens duomenų saugumo
pažeidimą pateikimo tvarkos aprašo
2 priedas

(Ataskaitos forma)

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMO ATASKAITA

Nr. _____

(data) (rašto numeris)

1. Asmens duomenų saugumo pažeidimo aprašymo kriterijai	Konkreto duomenų saugumo pažeidimo įvertinimas, pagal aprašymo kriterijus
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	
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. 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 Šiaulių miesto savivaldybės viešajai bibliotekai (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	
3. Pranešimų pateikimas	
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	
Šiaulių miesto savivaldybės viešosios bibliotekos duomenų apsaugos pareigūnas	(vardas, pavardė, parašas)

