

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ MOKSLO, INOVACIJŲ IR TECHNOLOGIJŲ AGENTŪROJE TVARKOS APRAŠAS

I SKYRIUS BENDROSIOS NUOSTATOS

1. Asmens duomenų saugumo pažeidimų tyrimo Mokslo, inovacijų ir technologijų agentūroje (toliau – Agentūra) tvarkos aprašas (toliau – Aprašas) nustato asmens duomenų pažeidimų tyrimo, pranešimų apie atliktą tyrimą pateikimo tvarką.

2. Taisyklėse vartojamos sąvokos:

2.1. **Asmens duomenų saugumo pažeidimas** (toliau – pažeidimas) – duomenų tvarkymo saugumo pažeidimas, dėl kurio neteisėtai sunaikinami, prarandami, pakeičiami, be leidimo atskleidžiami gauti, saugomi arba kitaip tvarkomi duomenys arba prie jų be leidimo gaunama prieiga.

2.2. **Agentūros darbuotojas** – Agentūros valstybės tarnautojas ar darbuotojas, dirbantis pagal darbo sutartį.

3. Kitos šiose Taisyklėse vartojamos sąvokos suprantamos taip, kaip jo apibrėžtos 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamente (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (toliau – Reglamentas (ES) 2016/679).

II SKYRIUS PAŽEIDIMŲ TYRIMAS

4. Tyrimas dėl pažeidimo yra pradamas gavus bet kokios pagrįstos informacijos, kurios visuma sudaro pagrindo manyti, jog buvo pažeistas asmens duomenų saugumas.

5. Agentūros darbuotojas, sužinojęs arba pats nustatęs galimą pažeidimą, jeigu įmanoma, imasi visų priemonių pašalinti pažeidimą bei priemonių galimoms neigiamoms jo pasekmėms sumažinti.

6. Agentūros darbuotojas, sužinojęs arba pats nustatęs galimą pažeidimą, nedelsdamas apie pažeidimą ir veiksmus, kurių imtasi siekiant pašalinti pažeidimą bei sumažinti galimas neigiamas jo pasekmes, elektroniniu paštu ar tarnybiniu pranešimu informuoja savo tiesioginį vadovą ir Agentūros duomenų apsaugos pareigūną.

7. Agentūros duomenų apsaugos pareigūnas ar kitas Agentūros direktoriaus įgaliotas darbuotojas, gavęs informaciją apie galimą pažeidimą:

7.1. nedelsdamas nagrinėja gautą informaciją apie galimą pažeidimą bei įvertina, ar jis įvyko;

7.2. jei įvyko pažeidimas:

7.2.1. nedelsdamas tarnybiniu pranešimu informuoja Agentūros direktorių ir jo pavedimu atlieka pažeidimo tyrimą;

7.2.2. prireikus konsultuojasi ar (ir) pasitelkia Agentūros darbuotojus;

7.2.3. įvertina, ar būtina pranešti apie įvykusį pažeidimą Valstybinei duomenų apsaugos inspekcijai (toliau – Inspekcija) atsižvelgiant į Reglamento (ES) 2016/679 33 straipsnio reikalavimus, jei būtina – ne vėliau nei per 48 val. nuo informacijos gavimo parengia pranešimo projektą;

7.2.4. įvertina, ar būtina pranešti apie įvykusį pažeidimą duomenų subjektui atsižvelgiant į Reglamento (ES) 2016/679 34 straipsnio reikalavimus, jei būtina – parengia pranešimo projektą;

7.2.5. nustato, kokių skubių priemonių būtina imtis, kad būtų pašalintas pažeidimas, įskaitant, kai tinkama, priemonės galimoms neigiamoms jo pasekmėms sumažinti (atsarginių kopijų naudojimas siekiant atkurti prarastus ar sugadintus duomenis ir t. t.);

7.2.6. imasi kitų veiksmų, kurie yra būtini galimam pažeidimui nustatyti ir (ar) galimoms neigiamoms jo pasekmėms sumažinti;

7.3. surašo šio Aprašo 1 priede nurodytą Asmens duomenų saugumo pažeidimo ataskaitą (toliau – ataskaita) ir pateikia Agentūros direktoriui.

8. Agentūros duomenų apsaugos pareigūnas ar kitas įgaliotas Agentūros darbuotojas informaciją apie įvykusį pažeidimą įrašo šių Taisyklių 2 priede nurodytame Asmens duomenų saugumo pažeidimų registravimo žurnale (toliau – žurnalas) ne vėliau kaip per 5 darbo dienas nuo ataskaitos įregistravimo. Prireikus žurnale esanti informacija gali būti papildoma ir (ar) koreguojama.

III SKYRIUS

PRANEŠIMŲ APIE ATIKTĄ TYRIMĄ PATEIKIMO TVARKA

9. Jeigu apie įvykusį pažeidimą būtina pranešti Inspekcijai, apie pažeidimą Inspekcijai yra pranešama nedelsiant, ne vėliau kaip per 72 val. nuo informacijos apie pažeidimą gavimo momento, Inspekcijos nustatyta tvarka. Tais atvejais, kai atsižvelgiant į pažeidimo pobūdį būtina atlikti išsamų tyrimą bei nustatyti visus svarbius faktus, susijusius su pažeidimu, ir per 72 val. nuo sužinojimo apie pažeidimą momento dėl objektyvių aplinkybių to padaryti neįmanoma, pranešime Inspekcijai yra pateikiama tuo metu prieinama informacija, nurodomos vėlavimo priežastys ir kada bus pateikta detalesnė informacija.

10. Jeigu apie įvykusį pažeidimą būtina pranešti duomenų subjektui, pranešime apie įvykusį pažeidimą duomenų subjektui pateikiama Reglamento (ES) 2016/679 34 str. nustatyta informacija.

11. Pranešimas apie įvykusį pažeidimą duomenų subjektui neteikiamas, jeigu:

11.1. Agentūra įgyvendino tinkamas technines ir organizacines apsaugos priemonės ir tos priemonės taikytos asmens duomenims, kuriems pažeidimas turėjo poveikio;

11.2. Agentūra iškart po pažeidimo ėmėsi priemonių, kurios užtikrina, kad didelis pavojus asmenų teisėms ir laisvėms nebekils;

11.3. pranešimas pareikalautų neproporcingai daug pastangų; tokiu atveju šio Aprašo 10 punkte nurodyta informacija viešai paskelbiama Agentūros interneto svetainėje arba taikoma panaši priemonė, kuria duomenų subjektai būtų informuojami taip pat efektyviai.

12. Nepranešimo apie įvykusį pažeidimą Inspekcijai ir (ar) duomenų subjektams priežastys nurodomos ataskaitoje.

13. Jei Inspekcija, apsvarsčiusi tikimybę, kad dėl įvykusio pažeidimo kils didelis pavojus, pareikalauja, kad Agentūra informuotų duomenų subjektą apie asmens duomenų saugumo pažeidimą, Agentūra nedelsdama praneša duomenų subjektui apie įvykusį pažeidimą.

14. Tuo atveju, kai yra įtariama, kad pažeidimas turi nusikalstamos veikos požymių, Agentūros direktoriaus įgaliotas darbuotojas informaciją apie galimą nusikalstamą veiką pateikia Agentūros direktoriui.

15. Kai padarytas pažeidimas yra susijęs su kibernetiniu incidentu, informaciją apie kibernetinį incidentą, susijusį su asmens duomenų saugumo pažeidimu, Agentūros direktoriaus įgaliotas darbuotojas pateikia Agentūros darbuotojui, atsakingam už kibernetinę saugą, kuris, jei yra pagrindas, inicijuoja informacijos perdavimą Lietuvos Respublikos kibernetinio saugumo įstatyme nurodytoms valstybės institucijoms šio įstatymo nustatyta tvarka ir atvejais.

IV SKYRIUS

BAIGIAMOSIOS NUOSTATOS

16. Už šių Taisyklių nesilaikymą Agentūros darbuotojai atsako teisės aktų nustatyta tvarka.

(Asmens duomenų saugumo pažeidimo ataskaitos formos pavyzdys)

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMO ATASKAITA

_____ Nr. _____
(data) _____
(vieta)

1. Asmens duomenų saugumo pažeidimo aprašymas	
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. Duomenys apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas (išvardyti kategorijas)	
1.9.4. Asmens duomenų įrašų apytikslis skaičius	
2. Pažeidimo rizikos įvertinimas	
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 prieigą 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. Skirtingos informacijos susiejimas	
2.2.7. Asmens duomenų panaudojimas neteisėtais tikslais	
2.2.8. Dėl asmens duomenų trūkumų negalima vykdyti funkcijų	
2.2.9. Dėl klaidų asmens duomenų tvarkymo procesuose negalima tinkamai vykdyti funkcijų	
2.2.10. Kita	
2.3. Pavojus fizinių asmenų teisėms ir laisvėms (nurodyti tinkamą ir pateikti pagrindžiančius argumentus):	
2.3.1. Dėl pažeidimo nėra pavojaus fizinių asmenų teisėms ir laisvėms	
2.3.2. Dėl pažeidimo yra ar gali kilti pavojus fizinių asmenų teisėms ir laisvėms	
2.3.3. Dėl Pažeidimo yra ar gali kilti dideli pavojus fizinių asmenų teisėms ir laisvėms	
2.4. Duomenų subjektui ir (ar) Agentūrai 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, kurios planuojamos 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	
3. Pranešimų pateikimas	
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 didelis pavojus 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 didelis pavojus 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 Inspekcijai apie pažeidimą:	
3.2.1. Pranešimo data, numeris	
3.2.2. Priežastys, dėl kurių nepranešta Inspekcijai	
3.2.3. Pranešimo 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 Agentūros valdomose ir (ar) tvarkomose ryšių ir informacinėse sistemose įvykusį kibernetinį incidentą ir taikytas kibernetinių incidentų valdymo priemones (jei taikoma) (rašto data, numeris)	

(pareigos)

(vardas ir pavardė)
