

KELMĖS ŠVIETIMO PAGALBOS TARNYBOS ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ VALDYMO IR REAGAVIMO Į JUOS TVARKA

I SKYRIUS BENDROSIOS NUOSTATOS

1. Kelmės švietimo pagalbos tarnybos (toliau – Tarnyba) darbuotojų asmens duomenų saugumo pažeidimo tvarka (toliau – Tvarka) reglamentuoja Tarnybos darbuotojų duomenų rinkimo, naudojimo ir saugojimo principų pažeidimo ir atsakomybės už juos priemonės. Tvarka nustato pranešimo apie galimą asmens duomenų saugumo pažeidimą Tarnybos viduje, asmens duomenų saugumo pažeidimo tyrimo, asmens duomenų saugumo pažeidimo valdymo ir šalinimo, pranešimo apie jį VDAI ir duomenų subjektui, jų registravimo tvarką bei Tarnybos duomenų tvarkytojų pareigas kilus asmens duomenų saugumo pažeidimui.

2. Tikslas – užtikrinti efektyvų Tarnybos ir jos duomenų tvarkytojų reagavimą į galimą asmens duomenų saugumo pažeidimą, nustatyto asmens duomenų saugumo pažeidimo valdymą ir operatyvų jo sukeltų padarinių šalinimą, siekiant kiek įmanoma sumažinti riziką duomenų subjektų teisėms ir laisvėms.

II SKYRIUS SĄVOKOS

3. Pagrindinės Asmens duomenų saugumo pažeidimų valdymo ir reagavimo į juos Tvarkoje naudojamos sąvokos:

3.1. **asmens duomenys** – bet kokia informacija apie fizinį asmenį, kurio tapatybė nustatyta arba kurio tapatybę galima nustatyti;

3.2. **asmens duomenų saugumo pažeidimas** - saugumo pažeidimas, dėl kurio netyčia arba neteisėtai sunaikinami, prarandami, pakeičiami, be leidimo atskleidžiami persiųsti, saugomi arba kitaip tvarkomi asmens duomenys arba prie jų be leidimo gaunama prieiga;

3.3. **duomenų subjektas** – fizinis asmuo, kurio tapatybę tiesiogiai arba netiesiogiai galima nustatyti, visų pirma pagal identifikatorių, kaip antai vardą ir pavardę, asmens identifikavimo numerį, buvimo vietos duomenis ir interneto identifikatorių arba pagal vieną ar kelis to fizinio asmens fizinės, fiziologinės, genetinės, psichinės, ekonominės, kultūrinės ar socialinės tapatybės požymius;

3.4. **duomenų tvarkytojas** – fizinis arba juridinis asmuo, valdžios institucija, agentūra ar kita įstaiga, kuri duomenų valdytojo vardu tvarko asmens duomenis;

3.5. **duomenų valdytojas** – fizinis arba juridinis asmuo, valdžios institucija, agentūra ar kita įstaiga, kuris vienas ar drauge su kitais nustato duomenų tvarkymo tikslus ir priemones;

3.6. **Reglamentas** – Europos Parlamento ir Tarybos 2016 m. balandžio 27 d. Reglamentas (ES) 2016/679.

3.7. **VDAI** – Valstybinė duomenų apsaugos inspekcija.

4. **Kitos sąvokos** kaip jos apibrėžtos Reglamente, ADTAĮ ir kituose teisės aktuose, reguliuojančiuose asmens duomenų tvarkymą ir apsaugą.

III SKYRIUS ASMENS DUOMENŲ PAŽEIDIMAI

5. Asmens duomenų saugumo pažeidimai yra skirstomi į 3 tipus:

5.1. **konfidencialumo pažeidimą** – be Tarnybos leidimo ar neteisėtai tretiesiems asmenims atskleidžiami asmens duomenys arba suteikiama prieiga prie šių duomenų;

5.2. **prieinamumo pažeidimą** – dėl neatsargumo arba neteisėtai prarandama prieiga prie Tarnybos ar jos duomenų tvarkytojų tvarkomų asmens duomenų arba pastarieji asmens duomenys dėl neatsargumo arba neteisėtai yra sunaikinami;

5.3. **vientisumo pažeidimą** – Tarnybos ar jos duomenų tvarkytojų tvarkomi asmens duomenys be Tarnybos leidimo, dėl neatsargumo ar neteisėtai yra pakeičiami.

6. Vienas asmens duomenų saugumo pažeidimas gali atitikti kelis tipus.

7. Reagavimo į galimą asmens duomenų saugumo pažeidimą, nustatyto asmens duomenų saugumo pažeidimo valdymo ir šalinimo procese dalyvauja ir Tarnybos duomenų apsaugos pareigūnas, teikdamas pasiūlymus dėl asmens duomenų saugumo pažeidimo tyrimo ir nustatymo, valdymo, jo sukeltų padarinių šalinimo.

IV SKYRIUS PRANEŠIMAS APIE GALIMĄ ASMENS DUOMENŲ PAŽEIDIMĄ TARNYBOS VIDUJE

8. Bet kuris Tarnybos darbuotojas, pastebėjęs ar sužinojęs apie neteisėtą Tarnybos tvarkomų asmens duomenų perdavimą arba neteisėtą prieigą prie šių asmens duomenų suteikimą tretiesiems asmenims, asmens duomenų perdavimą arba prieigą suteikimą tretiesiems asmenims be Tarnybos direktoriaus ar jo įgalioto asmens leidimo, dėl neatsargumo ar neteisėtai prarastą prieigą prie Tarnybos tvarkomų asmens duomenų, dėl neatsargumo ar neteisėtai sunaikintus, pakeistus asmens duomenis, taip pat pakeistus asmens duomenis be Tarnybos direktoriaus ar jo įgalioto asmens leidimo, privalo nedelsiant pranešti asmenims, atsakingiems už asmens duomenų saugumo pažeidimų tyrimą, nustatymą ir valdymą bei sukeltų padarinių šalinimą (toliau - Atsakingas asmuo).

9. Atsakingą asmenį skiria Tarnybos direktorius.

10. Apie galimą asmens duomenų saugumo pažeidimą Atsakingas asmuo informuojamas jo darbo ir/ar asmeniniu elektroniniu paštu.

V SKYRIUS GALIMO ASMENS DUOMENŲ SAUGUMO PAŽEIDIMO TYRIMAS

11. Atsakingas asmuo, gavęs informaciją apie galimą asmens duomenų saugumo pažeidimą, privalo nedelsiant pradėti tyrimą dėl galimo asmens duomenų saugumo pažeidimo. Tyrimo metu yra įvertinama gauta informacija, jos pakankamumas, patikimumas ir teisingumas. Vykdantis tyrimą asmuo gali pareikalauti Tarnybos darbuotojo, pateikusių informaciją, pateikti papildomus paaiškinimus, apklausti kitus Tarnybos darbuotojus, galinčius turėti informacijos apie galimą asmens duomenų saugumo pažeidimą, apklausti asmenį, dėl kurio veiksnių galimai kilo asmens duomenų saugumo pažeidimas, jei su šiuo asmeniu yra galimybė susisiekti, patikrinti fizinę vietą ar skaitmeninę erdvę, kurioje pastebėtas asmens duomenų saugumo pažeidimas arba apie jį sužinota.

12. Tyrimo pabaigoje Atsakingas asmuo surašo tyrimo išvadą, ataskaitą (priedas 1, 4), kurioje

pažymima, ar buvo nustatytas asmens duomenų saugumo pažeidimas. Jei asmens duomenų saugumo pažeidimas nebuvo nustatytas, tyrimas nutraukiamas. Jei asmens duomenų saugumo pažeidimas nustatomas, tyrimą atlikęs asmuo privalo papildomai įvertinti asmens duomenų saugumo pažeidimo sukeltos rizikos duomenų subjektų teisėms ir laisvėms lygį.

13. Rizikos lygiai skirstomi į žemą, vidutinę ir didelę riziką. Vertinant, kokio lygio rizika kyla duomenų subjekto teisėms ir laisvėms, reikia vadovautis protingumo principu ir atsižvelgti į tai, kokie padariniai atsiranda dėl asmens duomenų saugumo pažeidimo.

14. Tyrimas privalo būti atliktas ir išvada pateikta per 24 val. nuo informacijos apie galimą asmens duomenų saugumo pažeidimą gavimo momento.

VI SKYRIUS

NUSTATYTO ASMENS DUOMENŲ SAUGUMO PAŽEIDIMO VALDYMAS IR ŠALINIMAS

15. Tarnyba asmens duomenų saugumo pažeidimą valdo ir pažeidimo sukeltus neigiamus padarinius šalina įgyvendindama tinkamas organizacines ir technines apsaugos priemonės, nustatomas Tarnybos Asmens duomenų tvarkymo taisyklėse, bei įgyvendindama papildomas organizacines ir technines apsaugos priemonės, pasiūlytas galimo asmens duomenų saugumo pažeidimo tyrimo išvadoje.

16. Jei asmens duomenų saugumo pažeidimo sukeltų padarinių pašalinti neįmanoma, Tarnybos taikomos organizacinės ir techninės apsaugos priemonės turi kiek įmanoma labiau sumažinti šiuos padarinius.

VII SKYRIUS

PRANEŠIMAS VDAI APIE NUSTATYTĄ ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ

17. Jei tyrimo išvadoje buvo nustatyta, kad atitinkamas asmens duomenų saugumo pažeidimas kelia bet kurio lygio riziką duomenų subjektų teisėms ir laisvėms, Tarnyba pateikia VDAI pranešimą apie Tarnyboje nustatytą asmens duomenų saugumo pažeidimą, užpildant VDAI patvirtintą Pranešimo apie asmens duomenų saugumo pažeidimą rekomenduojamą formą ir ją pateikiant internetu ar kitais VDAI nustatytais būdais.

18. Apie asmens duomenų saugumo pažeidimą VDAI informuojama ne vėliau kaip per 72 val. nuo sužinojimo apie galimą asmens duomenų saugumo pažeidimą momento. Jei, atsižvelgiant į asmens duomenų saugumo pažeidimo sudėtingumą, šio pažeidimo tyrimo bei įgyvendinamų organizacinių ir techninių apsaugos priemonių apimtis ir kitas objektyvias aplinkybes, VDAI informuoti per 72 val. nėra galimybės, Tarnyba gali informuoti VDAI vėliau pranešime pateikdama vėlavimo priežastis.

VIII SKYRIUS

PRANEŠIMAS DUOMENŲ SUBJEKTUI APIE NUSTATYTĄ ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ

19. Jei tyrimo išvadoje buvo nustatyta, kad atitinkamas asmens duomenų saugumo pažeidimas kelia didelę riziką duomenų subjektų teisėms ir laisvėms, Tarnyba privalo pateikti duomenų subjektams, kurių teisėms ir laisvėms kyla didelė rizika, pranešimą apie Tarnyboje nustatytą asmens duomenų saugumo pažeidimą. Pranešime turi būti nurodoma ši informacija (priedas 3):

19.1. nustatyto asmens duomenų saugumo pažeidimo aprašymas;

19.2. Tarnybos darbuotojo, atsakingo už duomenų apsaugą ir atsakingo asmens, atlikusio tyrimą, vardas pavardė ir kontaktiniai duomenys;

19.3. asmens duomenų saugumo pažeidimo neigiami padariniai, keliantys didelę riziką

duomenų subjekto teisėms ir laisvėms;

19.4. organizacinių ir techninių apsaugos priemonių, kurios padėtų pašalinti arba kiek įmanoma sumažinti neigiamus padarinius duomenų subjekto teisėms ir laisvėms, aprašymas;

19.5. kita Tarnybos manymu su asmens duomenų saugumo pažeidimu susijusi informacija, kuri turėtų būti pateikiama duomenų subjektui.

20. Pranešimas duomenų subjektui siunčiamas duomenų subjekto turimais kontaktiniais duomenimis.

21. Apie asmens duomenų saugumo pažeidimą duomenų subjektas informuojamas ne vėliau kaip per 72 val. nuo sužinojimo apie galimą asmens duomenų saugumo pažeidimą momento. Jei, atsižvelgiant į asmens duomenų saugumo pažeidimo sudėtingumą, šio pažeidimo tyrimo bei įgyvendinamų organizacinių ir techninių apsaugos priemonių apimtis ir kitas objektyvias aplinkybes, duomenų subjekto informuoti per 72 val. nėra galimybės, Tarnyba gali informuoti duomenų subjektą vėliau pranešime pateikdama vėlavimo priežastis.

22. Pranešimo duomenų subjektui teikti Tarnyba neprivalo, jei egzistuoja bent viena iš žemiau nurodytų sąlygų:

22.1. Tarnyba įgyvendino tinkamas organizacines ir technines apsaugos priemones, kurios pašalino nustatyto asmens duomenų saugumo pažeidimo keliamus neigiamus padarinius duomenų subjekto teisėms ir laisvėms arba sumažino nustatyto asmens duomenų saugumo pažeidimo keliamą didelę riziką iki vidutinės ar žemos rizikos;

22.2. pranešimo teikimas duomenų subjektui iš Tarnybos pareikalautų neproporcingų pastangų dėl asmens duomenų saugumo pažeidimo sudėtingumo, pažeidimo tyrimo bei įgyvendinamų organizacinių ir techninių apsaugos priemonių apimties, duomenų subjektų, kurių teisėms ir laisvėms kilo didelė rizika, didelio skaičiaus ir kitų objektyvių aplinkybių. Tokiu atveju duomenų subjektui pranešimas yra teikiamas ne asmeniškai, o viešai, pasitelkiant žiniasklaidos ir kitas informacijos sklaidos priemones.

IX SKYRIUS

DUOMENŲ TVARKYTOJO PAREIGOS, ĮVYKUS ASMENS DUOMENŲ SAUGUMO PAŽEIDIMUI

23. Bet kuris Tarnybos darbuotojas, pastebėjęs ar kitaip sužinojęs apie galimą duomenų tvarkytojo tvarkomų asmens duomenų saugumo pažeidimą, privalo nedelsiant apie tai informuoti duomenų tvarkytojo įgaliotus asmenis, atsakingus už asmens duomenų saugumo pažeidimų tyrimą, valdymą ir šalinimą. Duomenų tvarkytojo įgalioti asmenys apie galimą asmens duomenų saugumo pažeidimą atitinkamai turi informuoti Tarnybos administraciją.

24. Duomenų tvarkytojas, nustatęs asmens duomenų saugumo pažeidimą, taip pat privalo imtis visų reikalingų organizacinių ir techninių apsaugos priemonių, kad pašalintų, o jei pašalinti neįmanoma, kad sumažintų riziką, kylančią duomenų subjektų teisėms ir laisvėms.

X SKYRIUS

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ REGISTRAVIMAS

25. Tarnyba registruoja visus asmens duomenų saugumo pažeidimus: tiek nustatytus, tiek nenustatytus. Asmens duomenų saugumo pažeidimai registruojami Asmens duomenų saugumo pažeidimų registracijos žurnale (priedas 2).

26. Tarnybos Asmens duomenų saugumo pažeidimų registracijos žurnalas yra tvarkomas elektronine forma.

XI SKYRIUS
BAIGIAMOSIOS NUOSTATOS

27. Visi Tarnybos darbuotojai: duomenų tvarkytojai ir darbuotojai, paskirti tvarkyti asmens duomenis, privalo laikytis šiame Apraše nustatytų reikalavimų.

28. Tarnybos darbuotojai su Aprašu supažindinami pasirašytinai.

29. Apie šį Aprašą yra informuotas darbuotojų atstovas ir su juo dėl Aprašo priėmimo yra pasikonsultuota.

KELMĖS ŠVIETIMO PAGALBOS TARNYBOS GALIMO ASMENS DUOMENŲ SAUGUMO PAŽEIDIMO TYRIMO IŠVADA

20 m.d. Nr.
Kelmė

Atlikto tyrimo metu asmens duomenų saugumo pažeidimas buvo (*nustatytas/nenustatytas*).

Nr.	Sąlyga	Išvados
1.	Asmens duomenų saugumo pažeidimo tipas	
2.	Asmens duomenų saugumo pažeidimo aprašymas	
3.	Asmens duomenų saugumo pažeidimo paaiškėjimo data	
4.	Apytikslis asmens duomenų saugumo pažeidimo paaiškėjimo laikas	
5.	Fizinė vieta arba skaitmeninė erdvė, kurioje užfiksuotas asmens duomenų saugumo pažeidimas	
6.	Duomenų subjektų, kurių teisėms ir laisvėms asmens duomenų saugumo pažeidimas sukėlė ar galėjo sukelti neigiamų padarinių, kategorijos ir sąrašas	
7.	Asmens duomenų, kurie buvo paveikti asmens duomenų saugumo pažeidimo, kategorijos ir sąrašas	
8.	Asmens duomenų saugumo pažeidimo sukeltos rizikos duomenų subjektų teisėms ir laisvėms lygis (nenustatytas, žemas, vidutinis, didelis)	
9.	Nustatyti asmens duomenų saugumo pažeidimo sukelti arba tikėtini padariniai duomenų subjektų teisėms ir laisvėms	
10.	Priežastys, kodėl asmens duomenų saugumo pažeidimas nekelia rizikos duomenų subjektų teisėms ir laisvėms (praleisti, jei pateikta išvada dėl sąlygos Nr. 9)	
11.	Pasiūlymai dėl organizacinių ir techninių apsaugos priemonių, kurios padėtų pašalinti arba kiek įmanoma sumažinti neigiamus padarinius duomenų subjektų teisėms ir laisvėms	
12.	Pasiūlymai dėl prevencijos priemonių, padėsiančių ateityje išvengti tokių pačių ar panašių asmens duomenų saugumo pažeidimų	

13.	Kitos tyrimo metu nustatytos aplinkybės	
14.		
15.		
16.		

Tyrimą atlikusio asmens pareigos, vardas, pavardė

Parašas

KELMĖS ŠVIETIMO PAGALBOS TARNYBA

 (struktūrinio padalinio pavadinimas)

 (pareigų pavadinimas)

 (vardas, pavardė)
**PRANEŠIMAS
APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ**

Nr. _____

Kelmė

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	

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 skirtose vietose palikti dokumentai su asmens duomenimis ir pan.)	

(pareigos)

(vardas, pavardė)

KELMĖS ŠVIETIMO PAGALBOS TARNYBOS ASMENS DUOMENŲ SAUGUMO PAŽEIDIMO ATASKAITA

_____ Nr. _____
 (data) (rašto numeris)

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, įstaigos, kurioje 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 (be leidimo ar neteisėtai atskleidžiami asmens duomenys arba gaunama prieiga prie jų)	
1.5.2. asmens duomenų vientisumo praradimas (kai asmens duomenys pakeičiami be leidimo ar netyčia)	
1.5.3. asmens duomenų prieinamumo praradimas (kai netyčia arba neteisėtai prarandama prieiga prie jų arba sunaikinami asmens duomenys)	
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 Susisiekimo ministerijai (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 neįgaliesiems 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 pasekmės	
3. Pranešimų pateikimas	

3.1. Ar pranešta duomenų subjektui apie asmens duomenų saugumo pažeidimą:	
3.1.1. Taip	(Pranešimo turinys ir data)
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	(rašto data ir numeris)
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	(rašto data ir numeris, adresatas)
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	(rašto data ir numeris, adresatas)
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 Inspekcijai apie asmens duomenų saugumo pažeidimą priežastys	

Direktoriaus įgaliotas asmuo

(vardas, pavardė, parašas)

Susipažino duomenų apsaugos pareigūnas

(vardas, pavardė, parašas)