PATVIRTINTA
KĮ Lietuvos nacionalinės filharmonijos
generalinio direktoriaus
2022 m. rugpjūčio 10 d.
įsakymu Nr. V- 41

LIETUVOS
NACIONALINĖ
FILHARMONIJA

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ KONCERINĖJE ĮSTAIGOJE LIETUVOS NACIONALINĖJE FILHARMONIJOJE VALDYMO TVARKOS APRAŠAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Asmens duomenų saugumo pažeidimų Koncertinėje įstaigoje Lietuvos nacionalinėje filharmonijoje valdymo tvarkos aprašas (toliau – Aprašas) reglamentuoja asmens duomenų saugumo pažeidimų nustatymo, tyrimo, pašalinimo ir pranešimo apie juos Koncertinėje įstaigoje Lietuvos nacionalinėje filharmonijoje (toliau – Filharmonija) valdymo tvarką.

2. 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) (toliau – Reglamentas (ES) 2016/679).

3. Apraše vartojamos sąvokos:

3.1. **asmens duomenų saugumo pažeidimas** (toliau – 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;

3.2. **darbuotojas** – Filharmonijos darbuotojas, dirbantis pagal darbo sutartį;

3.3. **atsakingas asmuo** – Filharmonijos generalinio direktoriaus paskirtas duomenų apsaugos pareigūnas ar kitas darbuotojas, atliekantis konkretaus pažeidimo tyrimą, pranešantis apie pažeidimą Valstybinei duomenų apsaugos inspekcijai (toliau – VDAI) ir asmens duomenų subjektams.

4. Kitos Apraše vartojamos sąvokos atitinka Reglamente (ES) 2016/679 apibrėžtas sąvokas.

5. Aprašas taikomas duomenų valdytojui – Filharmonijai, tvarkančiai asmens duomenis, ir Filharmonijos pasitelktiems juridiniams ir fiziniams asmenims, tvarkantiems asmens duomenis Filharmonijos vardu ir pagal jos nurodymus (toliau – duomenų tvarkytojai), kuriems pagal Reglamento (ES) 2016/679 33 straipsnio 2 dalį yra nustatyta prievolė pranešti Filharmonijai apie pažeidimą.

II SKYRIUS
PAŽEIDIMŲ, JŲ PRIEŽASČIŲ, KELIAMŲ RIZIKŲ KLASIFIKAVIMAS

6. Asmens duomenų saugumo pažeidimai pagal pobūdį (tipą) yra:

6.1. konfidencialumo pažeidimas – kai yra be leidimo ar neteisėtai atskleidžiami asmens duomenys arba gaunama prieiga prie jų;

6.2. vientisumo pažeidimas – asmens duomenų pakeitimas be leidimo ar netyčia;

6.3. prieinamumo pažeidimas – netyčinis arba neteisėtas prieigos prie asmens duomenų praradimas arba asmens duomenų sunaikinimas;

6.4. mišraus pobūdžio pažeidimas – asmens duomenų konfidencialumo, prieinamumo ir vientisumo pažeidimas ar bet kurių Aprašo 6.1–6.3 papunkčiuose nurodytų pažeidimų derinys.

7. Pažeidimai gali būti nulemti šių priežasčių:

7.1. netyčiniai veiksmai, kai asmens duomenų saugumas pažeidžiamas neturint tikslo tai padaryti (dėl duomenų tvarkymo klaidos, informacijos laikmenų, duomenų įrašų ištrynimo,

sunaikinimo ar sistemų sutrikimų dėl elektros tiekimo nutrūkimo, įvykusio dėl asmens veiklos, kompiuterinio viruso, paskleisto dėl asmens veiklos, vidaus taisyklių pažeidimo, sistemos priežiūros trūkumo, programinės įrangos testų atlikimo, netinkamos duomenų laikmenų priežiūros, netinkamo ryšio linijų pajėgumo ir apsaugos nustatymo, kompiuterių integravimo į tinklą, netinkamos kompiuterinių programų apsaugos parinkimo, asmens duomenų persiuntimo ne tam adresatui, ne saugojimui skirtoje vietoje paliktų dokumentų, pamestų nešiojamų įrenginių (telefono, nešiojamo kompiuterio, išorinės duomenų laikmenos) ir kt.);

7.2. tyčiniai veiksmai, kai asmens duomenų saugumas pažeidžiamas sąmoningai turint tikslą tai padaryti (kibernetinė ataka, vagystė, neteisėtas įsibrovimas į asmens duomenų tvarkytojo patalpas, asmens duomenų laikmenų saugyklas, informacines sistemas, kompiuterių tinklą, tyčinis nustatytų taisyklių tvarkant asmens duomenis pažeidimas, sąmoningas kompiuterinio viruso platinimas, neteisėtas naudojimasis kito darbuotojo teisėmis ir kt.);

7.3. force majeure ir kiti netikėti įvykiai, kurių negalima kontroliuoti, numatyti ir užkirsti kelio jų atsiradimui (žaibas, gaisras, potvynis, užliejimas, audros, elektros instaliacijos degimas, temperatūros ir (ar) drėgmės pakitimų poveikis, purvo, dulkių ir magnetinių laukų įtaka, techninės avarijos, išskyrus nurodytas Aprašo 7.1 papunktyje, ir kt.).

8. Pažeidimas, galintis kelti pavojų duomenų subjektų teisėms ir laisvėms, yra toks, dėl kurio, laiku nesiėmus tinkamų priemonių, kyla grėsmė duomenų subjektų sveikatai ir (ar) gyvybei ar grėsmė patirti materialinę ar nematerialinę žalą, pvz., prarasti savo asmens duomenų kontrolę, patirti teisių apribojimą, diskriminaciją, gali būti pavogta ar suklastota jo asmens tapatybė, jam padaryta finansinių nuostolių, neleistinai panaikinti pseudonimai, gali būti pakenkta jo reputacijai, prarastas asmens duomenų, kurie saugomi profesine paslaptimi, konfidencialumas arba padaryta kita ekonominė ar socialinė žala. Preziumuojama, kad pažeidimas kelia riziką, kai pažeidimas yra susijęs su specialių kategorijų asmens duomenimis.

9. Pažeidimo sukeltos rizikos duomenų subjektų teisėms ir laisvėms lygis skirstomas:

9.1. žema rizikos tikimybė (dėl pažeidimo nėra pavojaus fizinių asmenų teisėms ir laisvėms): fizinis asmuo gali susidurti su tam tikrais nepatogumais (pvz., sugaištas laikas iš naujo suvedant informaciją, susierzinimas, nepasitenkinimas ir pan.);

9.2. vidutinė rizikos tikimybė (dėl pažeidimo yra/gali kilti nedidelis pavojus fizinių asmenų teisėms ir laisvėms): fizinis asmuo gali patirti nepatogumų, kuriuos jis galės įveikti nepaisant tam tikrų sunkumų (pvz., papildomos išlaidos, prieigos prie reikalingų išteklių praradimas, stresas, nedideli fiziniai negalavimai ir kt.);

9.3. didelė rizikos tikimybė (dėl pažeidimo yra/gali kilti didelis pavojus fizinių asmenų teisėms ir laisvėms): fizinis asmuo gali patirti reikšmingas pasekmes ir norint jas ištaisyti, pašalinti reikės susidurti su rimtais sunkumais (pvz., lėšų praradimas, asmens įtraukimas į finansinių institucijų juodąjį sąrašą, turto nuostoliai (žala), darbo vietos praradimas, teisminiai procesai, sveikatos būklės pablogėjimas ir pan.) arba dideles ar negrįžtamas pasekmes, kurių negalės ištaisyti, pašalinti (pvz., negalėjimas dirbti, ilgalaikiai psichiniai ar fiziniai negalavimai, mirtis ir pan.).

III SKYRIUS
PRANEŠIMO APIE PAŽEIDIMĄ PATEIKIMAS

10. Darbuotojas, nustatęs arba kitaip sužinojęs apie galimą pažeidimą arba kai informacija apie galimą pažeidimą gaunama iš duomenų tvarkytojo, žiniasklaidos ar kito šaltinio:

10.1. nedelsdamas, bet ne vėliau kaip per 2 darbo valandas nuo galimo pažeidimo paaiškėjimo momento, žodžiu (tiesiogiai ar telefonu) arba elektroniniu paštu informuoja Filharmonijos generalinį direktorių, savo tiesioginį vadovą ir darbuotoją atliekantį duomenų apsaugos pareigūno funkcijas Filharmonijoje (toliau – duomenų apsaugos pareigūnas);

10.2. užpildo Aprašo 1 priede nurodytos formos Pranešimą apie asmens duomenų saugumo pažeidimą, kuris registruojamas elektroninėje dokumentų valdymo sistemoje (toliau – EDVS) ir nedelsiant, bet ne vėliau kaip per 2 darbo valandas nuo asmens duomenų saugumo pažeidimo

paaiškėjimo momento perduodamas per EDVS ir elektroniniu paštu Filharmonijos generaliniam direktoriui, darbuotojo tiesioginiam vadovui ir duomenų apsaugos pareigūnui;

10.3. tuo atveju, jei terminas nuo momento, kai darbuotojui tapo žinoma apie pažeidimą iki pranešimo Filharmonijos generaliniam direktoriui, tiesioginiam vadovui ir duomenų apsaugos pareigūnui, yra ilgesnis nei 2 darbo valandos, Filharmonijos darbuotojas kartu su Pranešimu apie asmens duomenų saugumo pažeidimą pateikia paaiškinimą dėl uždelsto informacijos pateikimo priežasčių;

10.4. jei įmanoma, pagal kompetenciją imasi priemonių pašalinti pažeidimą ir (ar) priemonių sumažinti jo sukeltas neigiamas pasekmes.

11. Duomenų tvarkytojas, nustatęs galimą pažeidimą, nedelsdamas, bet ne vėliau kaip per 24 valandas nuo pažeidimo paaiškėjimo momento, apie tai praneša Filharmonijos el. pašto adresu dap@filharmonija.lt , pateikdamas užpildytą Aprašo 1 priede nurodytos formos Pranešimą apie asmens duomenų saugumo pažeidimą.

12. Tuo atveju, jei terminas nuo momento, kai duomenų tvarkytojui tapo žinoma apie pažeidimą iki pranešimo Filharmonijai yra ilgesnis nei 24 valandos, duomenų tvarkytojas kartu su pranešimu pateikia Filharmonijai paaiškinimą dėl uždelsto informacijos pateikimo priežasčių.

13. Duomenų tvarkytojas pateikia visą Filharmonijos prašomą informaciją, susijusią su pažeidimu ir jo tyrimu, per Filharmonijos nurodytą laiką.

IV SKYRIUS
PAŽEIDIMO TYRIMAS IR PAŠALINIMAS

14. Filharmonijos generalinis direktorius, sužinojęs apie pažeidimą, žodžiu, rašytine rezoliucija arba įsakymu paskiria atsakingą asmenį, kuris pradeda pažeidimo tyrimą ir imasi šių veiksmų:

14.1. nagrinėja Pranešime apie asmens duomenų saugumo pažeidimą nurodytas aplinkybes ir įvertina, ar įvyko pažeidimas;

14.2. kiek įmanoma tiksliau surenka duomenis ir įrodymus apie įvykusį pažeidimą (pvz., kas, kada ir iš kokio įrenginio jungėsi prie duomenų bazės ar informacinės sistemos, kam per klaidą išsiųsti asmens duomenys, kokiomis aplinkybėmis buvo prarastas įrenginys su asmens duomenimis ir kt.);

14.3. dokumentuoja pažeidimo tyrimą (apžiūros aktai, specialistų išvados, liudytojų parodymai, fotofiksacija ir kt.);

14.4. konsultuojasi su duomenų apsaugos pareigūnu (jeigu atsakingas asmuo kartu nėra ir duomenų apsaugos pareigūnas); esant būtinybei, pagal kompetenciją konsultuojasi su kitais Filharmonijos specialistais;

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

15. Darbuotojai ir duomenų tvarkytojai privalo išsaugoti esamos situacijos, susijusios su galimu pažeidimu, įrodymus, kad vėliau naudojant technines ir organizacines priemones (pvz., duomenų srauto ir prisijungimų analizės įrankius ar kt.) galima būtų tirti pažeidimą.

16. Tyrimo metu objektyviai įvertinamos pažeidimo aplinkybės ir atsižvelgiama į:

16.1. pažeidimo pobūdį (tipą);

16.2. asmens duomenų pobūdį, kategoriją (pvz., specialių kategorijų asmens duomenys), asmens duomenų, kurių saugumas pažeistas pažeidimu, apimtį;

16.3. duomenų subjekto identifikavimo galimybę tiesiogiai ar netiesiogiai pasinaudojant pažeidimo objektu esančiais duomenimis;

16.4. pažeidimo sukeltos rizikos duomenų subjektų teisėms ir laisvėms lygį;

16.5. duomenų subjekto savybes (pvz., vaikas ar kitas pažeidžiamas asmuo, kt.);

16.6. duomenų subjektų, kurių asmens duomenų saugumas buvo pažeistas, skaičių;

16.7. kitas reikšmingas aplinkybes.

17. Atsakingas asmuo atlikto pažeidimo tyrimo rezultatus įformina Asmens duomenų saugumo pažeidimo tyrimo ataskaitoje (Aprašo 2 priedas), kuri registruojama EDVS.

18. Asmens duomenų saugumo pažeidimo tyrimo ataskaita yra perduodama Filharmonijos generaliniam direktoriui rezoliucijai įrašyti ir duomenų apsaugos pareigūnui, kuris šias ataskaitas kaupia ir saugo. Atsakingas asmuo perduoda Asmens duomenų saugumo pažeidimo tyrimo ataskaitą susipažinti duomenų tvarkytojo vadovui, jei tai susiję su duomenų tvarkytojo atliekamais asmens duomenų tvarkymo veiksmais.

19. Atsižvelgiant į Asmens duomenų saugumo pažeidimo tyrimo ataskaitą, Filharmonijos generalinis direktorius, konsultuodamasis su duomenų apsaugos pareigūnu:

19.1. priima sprendimą apie pažeidimą pranešti VDAI, kai dėl pažeidimo yra arba gali kilti pavojus fizinių asmenų teisėms ir laisvėms;

19.2. priima sprendimą apie pažeidimą nepranešti VDAI, kai pažeidimas nekelia pavojaus fizinių asmenų teisėms ir laisvėms;

19.3. priima sprendimą apie pažeidimą pranešti duomenų subjektams, kai dėl pažeidimo yra arba gali kilti didelis pavojus fizinių asmenų teisėms ir laisvėms;

19.4. priima sprendimą apie pažeidimą nepranešti duomenų subjektams, kai dėl pažeidimo nekyla arba negali kilti didelis pavojus fizinių asmenų teisėms ir laisvėms;

19.5. priima sprendimą dėl tolesnių veiksmų, susijusių su pažeidimu, jei reikia, tvirtina priemonių planą, kuriame numatomas būtinų techninių, organizacinių, administracinių ir kitų priemonių poreikis dėl pažeidimo pašalinimo, paskiria atsakingus vykdytojus ir nustato priemonių įgyvendinimo terminus.

20. Sprendžiant pažeidimo pašalinimo klausimą bei tvirtinant priemonių planą, pirmiausia būtina atlikti veiksmus, siekiant apriboti ar sustabdyti pažeidimą. Priklausomai nuo konkrečių pažeidimo aplinkybių, turėtų būti atlikti tokie veiksmai, kaip: ištrinti asmens duomenis nuotoliniu būdu iš pamesto ar pavogto nešiojamo / mobilaus įrenginio (telefono, nešiojamo kompiuterio ir kt.); jei asmens duomenys per klaidą išsiunčiami ne tam adresatui, kuriam jie buvo skirti, kuo skubiau kreiptis į jį su prašymu ištrinti atsiųstus asmens duomenis be galimybės juos atkurti ir patvirtinti ištrynimo faktą; pakeisti prisijungimo prie duomenų bazės ar informacinės sistemos vardus ir slaptažodžius; naudoti atsargines kopijas, siekiant atkurti prarastus, sugadintus ar pakeistus duomenis ir kt.).

21. Priemonių plane turi būti numatyti veiksmai, nukreipti ne vien į esamo pažeidimo priežasties pašalinimą, pavojaus fizinių asmenų teisėms ir laisvėms sumažinimą ar pašalinimą, bet taip pat skirti neleisti pasikartoti pažeidimui. Būtina atsižvelgti į trūkumus ir duomenų tvarkymo silpnąsias vietas, kurios buvo išnaudotos įvykdant pažeidimą bei imtis priemonių tuos trūkumus pašalinti.

V SKYRIUS
PRANEŠIMAS APIE PAŽEIDIMĄ PRIEŽIŪROS INSTITUCIJAI

22. Tyrimo metu nustačius, kad pažeidimas įvyko, atsakingas asmuo Filharmonijos generalinio direktoriaus pavedimu nedelsdamas nustato, ar yra Reglamento (ES) 2016/679 34 straipsnyje nustatyti pagrindai, dėl kurių būtina nedelsiant pranešti duomenų subjektui apie asmens duomenų saugumo pažeidimą, ir, esant šiems pagrindams, parengia pranešimo projektą, kuriame nurodoma Reglamento (ES) 2016/679 34 straipsnio 2 dalyje nurodoma informacija. Pranešimas duomenų subjektui neteikiamas esant bent vienai Reglamento (ES) 2016/679 34 straipsnio 3 dalyje nustatytai sąlygai, išskyrus Aprašo 19.2 punkte nustatytą atvejį.

23. Tyrimo metu nustačius, kad pažeidimas įvyko, atsakingas asmuo Filharmonijos generalinio direktoriaus pavedimu nustato, ar yra Reglamento (ES) 2016/679 33 straipsnyje nustatyti pagrindai pranešti Valstybinei duomenų apsaugos inspekcijai apie asmens duomenų saugumo pažeidimą, ir, esant šiems pagrindams, jei įmanoma, nepraėjus 72 valandoms nuo to laiko, kai buvo sužinota apie asmens duomenų saugumo pažeidimą, informuoja Valstybinę duomenų apsaugos inspekciją, pateikdamas užpildytą Pranešimo apie asmens duomenų saugumo pažeidimą

rekomenduojamą formą, patvirtintą VDAI direktoriaus 2018 m. gegužės 24 d. įsakymu Nr. 1T-53 (1.12) „Dėl pranešimo apie asmens duomenų saugumo pažeidimą rekomenduojamos formos patvirtinimo“. Kai atsižvelgiant į pažeidimo pobūdį būtina atlikti išsamų tyrimą ir nustatyti papildomas svarbias aplinkybes, susijusias su pažeidimu, ir per 72 valandas nuo sužinojimo apie pažeidimą momento dėl objektyvių priežasčių to padaryti neįmanoma, pranešime Valstybinei duomenų apsaugos inspekcijai pateikiama tuo metu prieinama informacija, nurodant kada bus pateikta detalesnė informacija. Pranešimas Valstybinei duomenų apsaugos inspekcijai neteikiamas, jeigu asmens duomenų saugumo pažeidimas neturėtų kelti pavojaus fizinių asmenų teisėms ir laisvėms.

24. Jeigu, įvertinus riziką, abejojama, ar pažeidimas kelia pavojų fizinių asmenų teisėms ir laisvėms, apie pažeidimą pranešama VDAI.

25. Jeigu įvertinus riziką, nustatoma, kad apie pažeidimą VDAI pranešti nereikia, pasikeitus situacijai, pažeidimas bei jo keliamas pavojus fizinių asmenų teisėms ir laisvėms turėtų būti vertinamas iš naujo (pvz., pamesta USB atmintinė, kurioje saugomi asmens duomenys, užšifruoti taikant pažangų algoritmą, yra atsarginės duomenų kopijos ir nėra pavojaus šifro saugumui, tačiau vėliau paaiškėjus, kad gali kilti pavojus šifro saugumui, pažeidimo keliamas pavojus bus vertinamas iš naujo ir sprendžiama dėl pranešimo VDAI).

26. Tuo atveju kai, priklausomai nuo pažeidimo pobūdžio, būtina atlikti išsamesnį tyrimą, nustatyti visus svarbius faktus, susijusius su pažeidimu, ir per 72 valandas dėl objektyvių priežasčių nėra įmanoma ištirti pažeidimą, informacija VDAI teikiama etapais, nurodant vėlavimo priežastis. Apie informacijos teikimą etapais VDAI informuojama teikiant pirminį pranešimą.

27. Jeigu po pranešimo VDAI pateikimo, atlikus tolesnį tyrimą, yra nustatoma, kad pažeidimo nebuvo, apie tai nedelsiant informuojama VDAI.

28. Tuo atveju, kai yra įtariama, kad pažeidimas turi nusikalstamos veikos požymių, informacija apie galimą nusikalstamą veiką pateikiama atitinkamoms valstybinėms institucijoms, įgaliotoms atlikti ikiteisminį tyrimą.

VI SKYRIUS
PRANEŠIMAS APIE PAŽEIDIMĄ DUOMENŲ SUBJEKTUI

29. Tyrimo metu nustačius, kad dėl pažeidimo gali kilti didelis pavojus fizinių asmenų teisėms ir laisvėms, atsakingas asmuo Filharmonijos generalinio direktoriaus pavedimu nedelsdamas ir, jei įmanoma, praėjus ne daugiau kaip 72 valandoms nuo to laiko, kai buvo sužinota apie pažeidimą, praneša apie tai duomenų subjektui, kurio teisėms ir laisvėms gali kilti didelis pavojus.

30. Duomenų subjektas informuojamas tiesiogiai, t. y. siunčiant jam pranešimą paštu, elektroniniu paštu, trumpąja žinute (SMS) ar kitu būdu. Pranešimas duomenų subjektui siunčiamas atskirai nuo kitos siunčiamos informacijos, kaip naujienlaiškiai ar standartiniai pranešimai, o iš el. pašto dap@filharmonija.lt.

31. Pagrindinis pranešimo duomenų subjektui tikslas – pateikti konkrečią informaciją apie tai, kokių veiksmų jis turėtų imtis, kad apsisaugotų nuo neigiamų pažeidimo pasekmių. Pranešime duomenų subjektui aiškia ir paprasta kalba pateikiama ši informacija:

31.1. pažeidimo pobūdžio (tipo) ir tikėtinų pažeidimo pasekmių aprašymas;

31.2. priemonių, kurių ėmėsi Filharmonija, kad būtų pašalintas pažeidimas, įskaitant priemonių galimoms neigiamoms jo pasekmėms sumažinti, aprašymas;

31.3. duomenų apsaugos pareigūno, atsakingo asmens arba kito kontaktinio asmens, galinčio suteikti daugiau informacijos, vardas, pavardė ir kontaktiniai duomenys;

31.4. kita reikšminga informacija, susijusi su pažeidimu, kuri, atsakingo asmens manymu, turėtų būti pateikta duomenų subjektui, pvz., patarimai, kaip apsisaugoti nuo galimų neigiamų pažeidimo pasekmių.

32. Pranešimo apie pažeidimą duomenų subjektams teikti nereikia jeigu:

32.1. Filharmonija įgyvendino tinkamas technines ir organizacines apsaugos priemones ir tos priemonės taikytos asmens duomenims, kuriems pažeidimas turėjo poveikio, visų pirma tas

priemones, kuriomis užtikrinama, kad asmeniui, neturinčiam leidimo susipažinti su duomenimis, jie būtų nesuprantami (pvz., asmens duomenų šifravimo priemonės);

32.2. iš karto po pažeidimo Filharmonija ėmėsi priemonių, kuriomis užtikrinama, kad nekiltų didelis pavojus duomenų subjektų teisėms ir laisvėms;

32.3. tiesioginio pranešimo duomenų subjektui pateikimas pareikalautų neproporcingai didelių pastangų, pvz., jei jų kontaktiniai duomenys buvo prarasti dėl pažeidimo arba iš pradžių nebuvo žinomi. Tokiu atveju apie pažeidimą viešai paskelbiama Filharmonijos interneto svetainėje, spaudoje, pasitelkiami ne vienas, o keli informavimo būdai arba taikomos panašios priemonės, kuriomis duomenų subjektai būtų efektyviai informuojami (pvz., vien tik pranešimas interneto svetainėje tam tikrais atvejais gali būti nepakankama priemonė).

33. Jeigu įvertinus riziką, nustatoma, kad tuo metu apie pažeidimą duomenų subjektams pranešti nereikia, po kurio laiko situacija gali pasikeisti, todėl pažeidimas bei jo keliamas pavojus fizinių asmenų teisėms ir laisvėms turėtų būti vertinamas iš naujo (pvz., įvykdoma kibernetinė ataka, naudojant išpirkos reikalaujančią programą ir duomenų bazėje esantys asmens duomenys užšifruojami, tačiau atlikus tyrimą, paaiškėja, kad vienintelė išpirkos reikalaujančios programos užduotis buvo užšifruoti asmens duomenis ir jokio kito kenksmingo poveikio duomenų bazei ir asmens duomenims nėra; tačiau, jei vėliau paaiškėja, kad prarastas ne tik duomenų prieinamumas, bet ir konfidencialumas, pažeidimo keliamas pavojus bus vertinamas iš naujo bei sprendžiama, ar atsižvelgiant į tikėtinas pažeidimo pasekmes apie jį reikia pranešti duomenų subjektams).

34. Tam tikromis aplinkybėmis, kai tai yra pagrįsta, Filharmonija pasitarusi su teisėsaugos institucijomis ir atsižvelgdamas į teisėtus teisėsaugos interesus, gali atidėti asmenų, kuriems pažeidimas turi poveikio, informavimą apie pažeidimą iki to laiko, kai tai netrukdys pažeidimo tyrimui.

VII SKYRIUS
PAŽEIDIMŲ DOKUMENTAVIMAS

35. Tyrimas dėl asmens duomenų saugumo pažeidimo yra pradedamas gavus Pranešimą arba bet kokios pagrįstos informacijos, sudarančios pagrindo manyti, kad buvo pažeistas asmens duomenų saugumas. Darbuotojas ar atsakingas asmuo pildo Pranešimą apie asmens duomenų saugumo pažeidimą, kurį registruoja EDVS (Aprašo 1 priedas). Pranešimu yra informuojamas apie pažeidimo faktą Filharmonijos generalinis direktorius ir duomenų apsaugos pareigūnas. Duomenų apsaugos pareigūnas šio pranešimo pagrindu užpildo Asmens duomenų saugumo pažeidimo ataskaitą (Aprašo 2 priedas), registruoja EDVS, kaupia ir saugo.

36. Visi pažeidimai, nepriklausomai nuo to, ar apie juos buvo pranešta VDAI, asmens duomenų apsaugos pareigūnas registruojami Pranešimų apie asmens duomenų saugumo pažeidimų registravimo žurnale elektroninėje formoje (Aprašo 3 priedas) ir Pranešimų apie galimą asmens duomenų saugumo pažeidimo žurnalo elektroninėje formoje (Aprašo 4 priedas), kurias pildo Duomenų apsaugos pareigūnas.

37. Informacija apie pažeidimą į Asmens duomenų saugumo pažeidimų registravimo žurnalą įvedama nedelsiant, kai tik paaiškėja galimas pažeidimas, bet ne vėliau kaip per 5 darbo dienas nuo galimo pažeidimo paaiškėjimo momento. Kai pasikeičia Asmens duomenų saugumo pažeidimų registravimo žurnale nurodyta informacija arba paaiškėja nauja informacija, Asmens duomenų saugumo pažeidimų registravimo žurnale esanti informacija turi būti papildoma ir (ar) koreguojama.

38. Asmens duomenų saugumo pažeidimų registravimo žurnale nurodoma:

38.1. pažeidimo nustatymo aplinkybės (pažeidimo nustatymo data, laikas, vieta, subjektas, pranešęs apie pažeidimą);

38.2. pažeidimo aplinkybės (pažeidimo data, vieta, pažeidimo pobūdis, priežastys, asmens duomenų, kurių saugumas pažeistas, kategorijos ir apytikslis skaičius, duomenų subjektų, kurių asmens duomenų saugumas pažeistas, kategorijos ir apytikslis skaičius);

38.3. tikėtinos pažeidimo pasekmės ir pavojus duomenų subjekto teisėms ir laisvėms;

38.4. priemonės, kurių buvo imtasi, kad būtų pašalintas pažeidimas, įskaitant priemones galimoms neigiamoms pažeidimo pasekmėms sumažinti;

38.5. informacija apie pranešimo apie pažeidimą pateikimą VDAI:

38.5.1. jei apie pažeidimą nebuvo pranešta VDAI, nurodomi tokio sprendimo motyvai; jei apie pažeidimą buvo pranešta VDAI, nurodoma pranešimo data ir numeris, taip pat, ar pranešimas teikiamas etapais;

38.5.2. jeigu apie pažeidimą buvo vėluojama pranešti VDAI, nurodomos tokio vėlavimo priežastys;

38.6. informacija apie pranešimą duomenų subjektui (subjektams) apie pažeidimą:

38.6.1. jei apie pažeidimą nebuvo pranešta duomenų subjektui (subjektams), nurodomi tokio sprendimo motyvai; jei apie pažeidimą buvo pranešta duomenų subjektui (subjektams), nurodoma pranešimo (pranešimų) data (datos) ir būdas (būdai);

38.6.2. jeigu apie pažeidimą buvo vėluojama pranešti duomenų subjektui (subjektams), nurodomos tokio vėlavimo priežastys;

38.6.3. kita reikšminga informacija, susijusi su pažeidimu.

39. Asmens duomenų saugumo pažeidimų registravimo žurnalas yra tvarkomas elektronine forma ir saugomas pagal patvirtintą Filharmonijos dokumentacijos planą.

40. Asmens duomenų saugumo pažeidimų registravimo žurnalą pildo ir tvarko duomenų apsaugos pareigūnas.

41. Kai padarytas pažeidimas yra susijęs su kibernetiniu incidentu, informacija apie kibernetinį incidentą, susijusį su pažeidimu, pateikiama Lietuvos Respublikos kibernetinio saugumo įstatyme nurodytoms valstybės institucijoms šio įstatymo nustatyta tvarka ir atvejais.

VIII SKYRIUS
BAIGIAMOSIOS NUOSTATOS

42. Darbuotojai su Aprašu bei jo pakeitimais supažindinami elektroninio pašto ir kitomis informavimo priemonėmis.

43. Aprašas duomenų apsaugos pareigūno peržiūrimas periodiškai, ne rečiau kaip kartą per tris metus arba įvykus organizaciniams, sisteminiams ar kitiems pokyčiams, arba pasikeitus teisės aktų reikalavimams.

44. Darbuotojai, pažeidę Aprašo reikalavimus, atsako Lietuvos Respublikos teisės aktų nustatyta tvarka.

Asmens duomenų saugumo pažeidimų
Koncertinėje įstaigoje
Lietuvos nacionalinėje filharmonijoje
Valdymo tvarkos aprašo 1 priedas

LIETUVOS
NACIONALINĖ
FILHARMONIJA

KONCERINĖS ĮSTAIGOS LIETUVOS NACIONALINĖS FILHARMONIJOS PRANEŠIMO APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ FORMA

_____

_____

(duomenų valdytojo atstovo pavadinimas, duomenų valdytojo (fizinio asmens) vardas, pavardė)

_____

_____

_____

(juridinio asmens kodas ir buveinės adresas arba fizinio asmens kodas, gimimo data (jeigu asmuo neturi asmens kodo) ir asmens duomenų tvarkymo vieta

_____

_____

_____

(telefono ryšio numeris ir (ar) elektroninio pašto adresas)

Koncertinės įstaigos Lietuvos nacionalinės filharmonijos generaliniam direktoriui

PRANEŠIMAS
APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ

_____ Nr. _____
(data) (rašto numeris)

1.Asmens duomenų saugumo pažeidimo apibūdinimas

1.1. Asmens duomenų saugumo pažeidimo data ir laikas:

Asmens duomenų saugumo pažeidimo:

Data _____ Laikas _____

Asmens duomenų saugumo pažeidimo nustatymo:

Data _____ Laikas _____

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

☐ Informacinė sistema
☐ Duomenų bazė
☐ Internetinė svetainė
☐ Debesų/ EDVS kompiuterijos paslaugos
☐ Nešiojami / mobilūs įrenginiai

☐ Neautomatiniu būdu susistemintos bylos (archyvas)

☐ Kita _____

1.3. 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)

1.4. Apytikslis duomenų subjektų, kurių asmens duomenų saugumas pažeistas, skaičius:

_____

1.5. Duomenų subjektų, kurių asmens duomenų saugumas pažeistas, kategorijos (atskiriamos pagal jai būdingą požymį):

_____

_____

_____

1.6. Asmens duomenų, kurių saugumas pažeistas, kategorijos (pažymėti tinkamą (-as):

☐ Asmens tapatybę patvirtinantys 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, mokėtojo kodas, slaptažodžiai):

_____

_____

_____

☐ Kiti:

_____

_____

_____

☐ Nežinomi (pranešimo teikimo metu)

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

_____

1.8. Kita duomenų valdytojo nuomone reikšminga informacija apie asmens duomenų saugumo pažeidimą:

_____
_____
_____
_____
_____
_____
_____
_____
_____

2. Galimos asmens duomenų saugumo pažeidimo pasekmės

2.1. Konfidencialumo praradimo atveju:

☐ Asmens duomenų išplitimas labiau nei yra būtina ir duomenų subjekto kontrolės praradimas savo asmens duomenų atžvilgiu (pavyzdžiui, asmens duomenys išplito internete)

☐ Skirtingos informacijos susiejimas (pavyzdžiui, gyvenamosios vietos adreso susiejimas su asmens buvimo vieta realiu laiku)

☐ Galimas panaudojimas kitais, nei nustatytais ar neteisėtais tikslais (pavyzdžiui, komerciniais tikslais, asmens tapatybės pasisavinimo tikslu, informacijos panaudojimo prieš asmenį tikslu)

☐ Kita

_____
_____
_____

2.2. Vientisumo praradimo atveju:

☐ Pakeitimas į neteisingus duomenis dėl ko asmuo gali netekti galimybės naudotis programomis.

☐ Pakeitimas į galiojančius duomenis, kad asmens duomenų tvarkymas būtų nukreiptas (pavyzdžiui, pavogta asmens tapatybė susiejant vieno asmens identifikuojančius duomenis su kito asmens biometriniais duomenimis)

☐ Kita

_____
_____
_____

2.3. Duomenų prieinamumo praradimo atveju:

☐ Dėl asmens duomenų trūkumo negalima teikti paslaugų (pavyzdžiui, administracinių procesų sutrikdymas, dėl ko negalima įgyvendinti duomenų subjekto teises)

☐ Dėl klaidų asmens duomenų tvarkymo procesuose negalima teikti tinkamos paslaugos (pavyzdžiui, asmens darbo bylos istorijoje neliko informacijos apie asmens pateiktus asmens duomenis, tam tikra informacija iš mokesčių deklaracijos išnyko, dėl ko negalima tinkamai apskaičiuoti mokesčių ir pan.)

☐ Kita

_____
_____
_____

2.4. Kita:

_____

3. Priemonės, kurių imtasi siekiant pašalinti pažeidimą ar sumažinti jo pasekmes

3.1. Taikytos priemonės siekiant sumažinti poveikį duomenų subjektams:

3.2. Taikytos priemonės siekiant pašalinti asmens duomenų saugumo pažeidimą:

3.3. Taikytos priemonės siekiant, kad pažeidimas nepasikartotų:

3.4. Kita:

4. Siūlomos priemonės sumažinti asmens duomenų saugumo pažeidimo pasekmėms

5. Duomenų subjektų informavimas apie asmens duomenų saugumo pažeidimą

5.1. Duomenys apie informavimo faktą:

☐ Taip, duomenų subjektai informuoti (nurodoma data) _____

☐ Ne, bet jie bus informuoti (nurodoma data) _____

☐ Ne

5.2. Duomenų subjektų, kurių asmens duomenų saugumas pažeistas, neinformavimo priežastys:

☐ Ne, nes nekyla didelis pavojus duomenų subjektų teisėms ir laisvėms (nurodoma kodėl)

_____

_____

_____

☐ Ne, nes įgyvendintos tinkamos techninės ir organizacinės priemonės, užtikrinančios, kad asmeniui, neturinčiam leidimo susipažinti su asmens duomenimis, jie būtų nesuprantami (nurodomos kokios)

_____

_____

_____

☐ Ne, nes įgyvendintos tinkamos techninės ir organizacinės priemonės, užtikrinančios, kad nekiltų didelis pavojus duomenų subjektų teisėms ir laisvėms (nurodomos kokios)

_____

_____

_____

☐ 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)

_____

_____

_____

☐ Ne, nes dar neidentifikuoti duomenų subjektai, kurių asmens duomenų saugumas pažeistas

_____

_____

_____

5.3. Informacija, kuri buvo pateikta duomenų subjektams (gali būti pridėtas pranešimo duomenų subjektui kopija):

_____

_____

_____

5.4. Būdas, kokiu duomenų subjektai buvo informuoti:

☐ Paštu

☐ Elektroniniu paštu

☐ Kitu būdu _____

5.5. Informuotų duomenų subjektų skaičius _____

6. Asmuo galintis suteikti daugiau informacijos apie asmens duomenų saugumo pažeidimą (duomenų apsaugos pareigūnas ar kitas kontaktinis asmuo)

6.1. Vardas ir pavardė _____

6.2. Telefono ryšio numeris _____

6.3. Elektroninio pašto adresas _____

6.4. Pareigos _____

6.5. Darbovietės pavadinimas ir adresas _____

7. Pranešimo pateikimo Valstybinei duomenų apsaugos inspekcijai pateikimo vėlavimo priežastys

_____
_____
_____
_____
_____

8. Kita reikšminga informacija

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

_____	_____	_____
(pareigos)	(parašas)	(vardas, pavardė)

Asmens duomenų saugumo pažeidimų
Koncertinėje įstaigoje
Lietuvos nacionalinėje filharmonijoje
Valdymo tvarkos aprašo 2 priedas

LIETUVOS
NACIONALINĖ
FILHARMONIJA

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMO ATASKAITA

_____ Nr. _____
(data) (rašto numeris)

1. Asmens duomenų saugumo pažeidimo aprašymo kriterijai	Konkretaus 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 muitinės įstaigai (tapatybės vagystė, grėsmė fiziniam saugumui ir emocinei gerovei, žala reputacijai, teisinė atsakomybė, konfidencialumo, saugumo nuostatų pažeidimas ir pan.)?	
2.11. Dėl asmens duomenų saugumo pažeidimo nėra pavojaus fizinių asmenų teisėms ir laisvėms (žema rizikos tikimybė)	
2.12. Dėl asmens duomenų saugumo pažeidimo yra / gali kilti pavojus fizinių asmenų teisėms ir laisvėms (būtina pranešti Valstybinei duomenų apsaugos inspekcijai) (vidutinė rizikos tikimybė)	
2.13. Dėl asmens duomenų saugumo pažeidimo yra / gali kilti didelis pavojus fizinių asmenų teisėms ir laisvėms (būtina pranešti Valstybinei duomenų apsaugos inspekcijai ir duomenų subjektams) (aukšta rizikos tikimybė)	
2.14. Kokių veiksmų/priemonių buvo imtasi sužinojus apie padarytą asmens duomenų saugumo pažeidimą?	
2.15. Kokios techninės priemonės buvo taikomos asmens duomenų saugumo pažeidimo paveiktiems asmens duomenims, užtikrinant, kad asmens duomenys nebūtų prieinami neįgaliotiems asmenims?	

2.16. 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 Informuotų duomenų subjektų skaičius	
3.4. Ar pranešta Valstybinei duomenų apsaugos inspekcijai apie asmens duomenų saugumo pažeidimą:	
3.4.1. Taip	(rašto data ir numeris)
3.4.2. 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 Valstybinei duomenų apsaugos inspekcijai priežastys	
3.9. Vėlavimo pranešti Valstybinei duomenų apsaugos inspekcijai apie asmens duomenų saugumo pažeidimą priežastys	
Duomenų apsaugos pareigūnas	(vardas, pavardė, parašas)
Saugos administravimo pakomitetis (pildoma, jei asmens duomenų saugumo pažeidimas įvyko teritorinėje muitinėje ar specialiojoje muitinės įstaigoje)	(nario vardas, pavardė, parašas)

Asmens duomenų saugumo pažeidimų
Koncertinėje įstaigoje
Lietuvos nacionalinėje filharmonijoje
Valdymo tvarkos aprašo 3 priedas

LIETUVOS
NACIONALINĖ
FILHARMONIJA

(Žurnalo forma)

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ REGISTRAVIMO ŽURNALAS

Eil. Nr.	**Duomenų saugumo pažeidimo ataskaitos data ir numeris**	**Pradžia** *(metai, mėnuo, diena, valanda)*	**Asmens duomenų saugumo pažeidimo aprašymas, su duomenų saugumo pažeidimu susiję faktai** *(priežastys, poveikis, pasekmės)*	**Duomenų saugumo pažeidimo tipas** *(konfidencialumo, pasiekiamumo, vientisumo)*	**Ar buvo pranešta Valstybinei duomenų apsaugos inspekcijai, duomenų subjektams** *(jei ne, nurodyti priežastis)*. **Vėlavimo pranešti Valstybinei duomenų apsaugos inspekcijai, duomenų subjektams priežastys** *(jei taikoma)*	**Taisomieji veiksmai, kurių buvo imtasi, įskaitant organizacines-technines priemones**	**Pabaiga** *(metai, mėnuo, diena, valanda)*	**Pašalino** *(vardas, pavardė, parašas)*	**Duomenų apsaugos pareigūnas** *(vardas, pavardė, parašas)*	**Kita reikšminga informacija, susijusi su pažeidimu**

Asmens duomenų saugumo pažeidimų
Koncertinėje įstaigoje
Lietuvos nacionalinėje filharmonijoje
Valdymo tvarkos aprašo 4 priedas

LIETUVOS
NACIONALINĖ
FILHARMONIJA

(Žurnalo forma)

PRANEŠIMŲ APIE GALIMĄ ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ REGISTRAVIMO ŽURNALAS

Eil. Nr.	Pranešimą apie galimą asmens duomenų saugumo pažeidimą pateikęs subjektas (jeigu žinomas)	Pranešimo gavimo Filharmonijoje data	Trumpas asmens duomenų saugumo pažeidimo aprašymas	Duomenų apsaugos pareigūnas arba kitas asmuo, įgaliotas atlikti asmens duomenų saugumo pažeidimo tyrimą *(vardas, pavardė, parašas)*	Kita reikšminga informacija, susijusi su pažeidimu