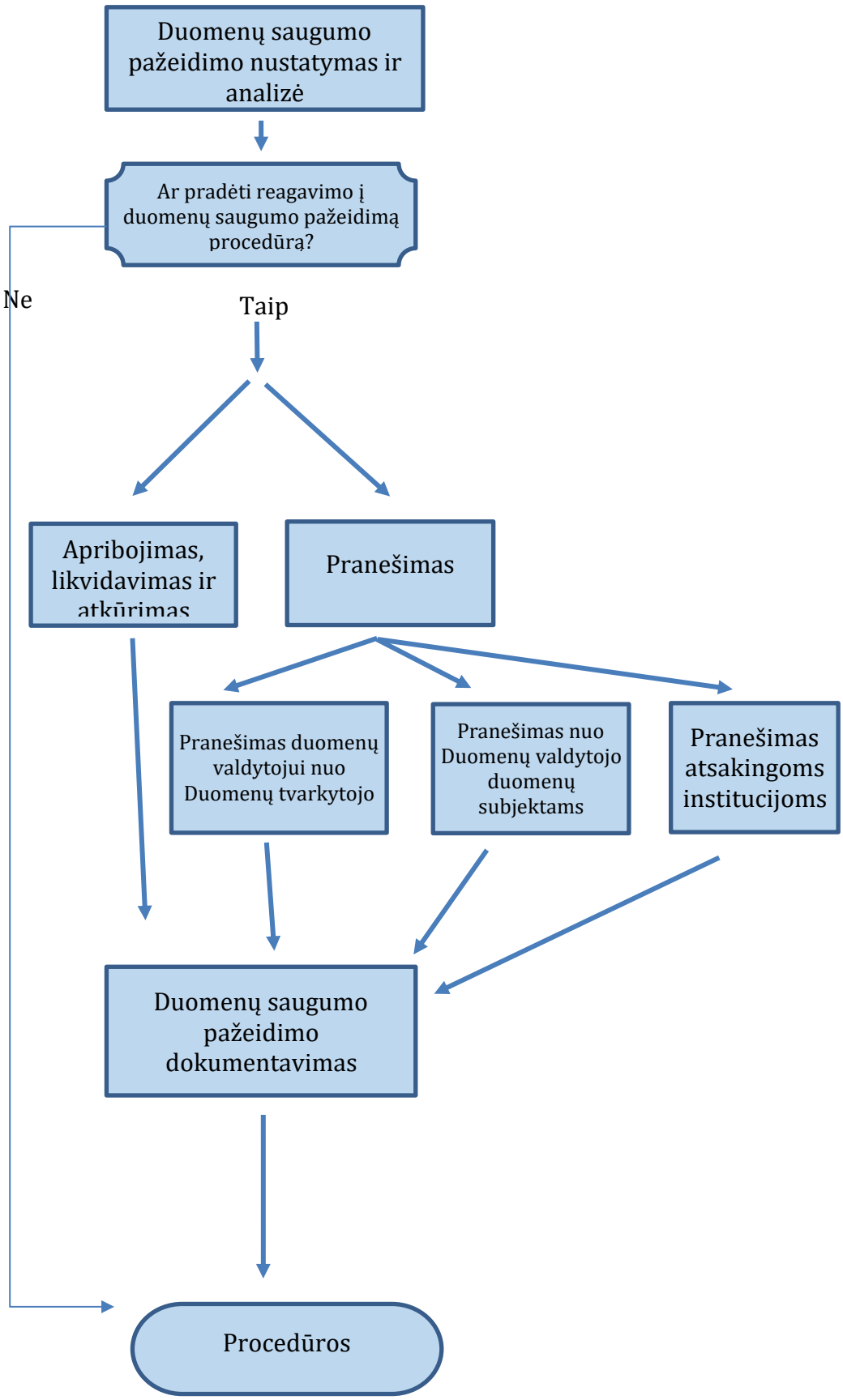
Asmens duomenų tvarkymo taisyklių, patvirtintų
Lietuvos muzikos ir teatro akademijos rektoriaus
2023 m. kovo 27 d. įsakymu Nr. 37-VĮ 5 priedas

LIETUVOS MUZIKOS IR TEATRO AKADEMIJOS ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ IDENTIFIKAVIMO IR VALDYMO TVARKOS APRAŠAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Lietuvos muzikos ir teatro akademijos (toliau – Akademija) asmens duomenų saugumo pažeidimų identifikavimo ir valdymo tvarkos aprašas (toliau – tvarkos aprašas) reglamentuoja asmens duomenų saugumo pažeidimų identifikavimo, tyrimo ir kontrolės tvarką Akademijoje ir yra taikomas visiems Akademijos darbuotojams, dirbantiems su asmens duomenimis.
2. **Duomenų saugumo pažeidimas** reiškia pažeidimą, 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. **Duomenų valdytojas –** Lietuvos muzikos ir teatro akademija, adresas Gedimino pr. 42, Vilnius, juridinio asmens kodas 111950624.
4. **Už duomenų saugą atsakingas asmuo** – Duomenų valdytojo rektoriaus paskirtas darbuotojas, turintis kompetenciją imtis reagavimo į Duomenų saugumo pažeidimą procedūros vykdymo.
5. **Priežiūros institucija** reiškia valstybės narės pagal BDAR 51 straipsnį įsteigtą nepriklausomą valdžios instituciją. Lietuvos Respublikos atveju tokia institucija yra Valstybinė duomenų apsaugos inspekcija.
6. **Procedūra** reiškia reagavimo į asmens duomenų saugumo pažeidimus procedūrą.
7. Ši Procedūra taikoma įvykus asmens Duomenų saugumo pažeidimui pagal BDAR 33 straipsnį ir 34 straipsnį.
8. Šiame dokumente išdėstyta Procedūra turėtų būti vadovaujamasi reaguojant į Duomenų saugumo pažeidimą, atsižvelgiant į konkrečios situacijos faktines aplinkybes.
9. Visi asmenys, turintys prieigą prie Duomenų valdytojo tvarkomų asmens duomenų, privalo žinoti ir vadovautis šia Procedūra duomenų saugumo pažeidimo atveju.

II SKYRIUS
REAGAVIMO Į ASMENS SAUGUMO PAŽEIDIMĄ SCHEMA



Iliustracija 1 – Reagavimo į Duomenų saugumo pažeidimus schema

III SKYRIUS
PROCEDŪRA – DUOMENŲ SAUGUMO PAŽEIDIMO NUSTATYMAS IR ANALIZĖ

9. Saugumo pažeidimu laikomas toks saugumo incidentas, dėl kurio įvyksta konkretus pažeidimas (gali patekti daugiau nei viena kategorija):

9.1. Konfidencialumo pažeidimas – netyčia ar neteisėtai atskleidžiami asmens duomenys arba prie asmens duomenų suteikiama prieiga tam teisės neturintiems asmenims. Tokio pobūdžio pažeidimo pavyzdžiais galėtų būti įrenginio, kuriame išsaugota visos ar dalies duomenų bazės kopija, pametimas arba vagystė, darbuotojų asmens duomenų kopijos išsiuntimas trečiajam asmeniui, neturinčiam teisinio pagrindo juos gauti, prisijungimo prie asmens duomenų bazės slaptažodžio paviešinimas ir pan.;

9.2. Pasiekiamumo pažeidimas – netyčia ar neteisėtai prarandama prieiga prie asmens duomenų arba asmens duomenys yra sunaikinami. Tokio pobūdžio pažeidimu galėtų būti visos ar dalies asmens duomenų bazės ištrynimas nesant atsarginės kopijos, iš kurios būtų galima atkurti prarastus asmens duomenis. Pasiekiamumo pažeidimu, kuris turėtų būti aprašytas, būtų ir laikinas įprastinę Duomenų valdytojo veiklą sutrikdęs prieigos prie duomenų praradimas;

9.3. Vientisumo pažeidimas – netyčia ar neteisėtai atliekami asmens duomenų pakeitimai. Tai, pavyzdžiui, galėtų būti trečiojo asmens, įgijusio neteisėtą prisijungimą prie asmens duomenų bazės, įvykdyti joje esančių įrašų pakeitimai.

10. Kai yra nustatomas duomenų saugumo pažeidimas, jį nustatęs darbuotojas turi kuo skubiau informuoti už duomenų apsaugą atsakingą asmenį asmeniškai, el. paštu, telefonu, ir/arba kitomis komunikacijos priemonėmis.

11. Už duomenų apsaugą atsakingas asmuo atlieka pradinį vertinimą tam, kad nuspręstų dėl tinkamo veiksmų plano. Šis vertinimas turėtų apimti šiuos pagrindinius veiksnius:

11.1. Poveikio IT infrastruktūrai apimtis;

11.2. Informacinius išteklius, kuriems gali būti arba yra kilęs pavojus (kokios asmens duomenų bazės yra arba gali būti paveiktos);

11.3. Tikėtina duomenų saugumo pažeidimo trukmė (kada prasidėjo ir kada buvo sustabdytas pažeidimas arba kaip skubiai tikėtina galima būtų tai padaryti);

11.4. Paveikti Duomenų subjektai ir poveikio jiems apimtis (ar paveikti tik konkrečios Duomenų subjektų grupės asmens duomenys, kokia konkrečios grupės dalis yra paveikta ir pan.);

11.5. Pradiniai duomenų saugumo pažeidimo pasekmių požymiai (tai galėtų būti prieigos prie asmens duomenų praradimas, nustatyti neteisėti asmens duomenų pakeitimai, rasti paviešinti asmens duomenys ir pan.).

12. Aukščiau nurodyta informacija turėtų būti fiksuojama tokiu būdu, kad atliekant vėlesnę peržiūrą būtų galima susidaryti aiškią chronologinę seką apie situacijos eigą ir priemones, kurių buvo imtasi.

13. Atsižvelgdamas į aukščiau aprašytą pradinę analizę, už duomenų apsaugą atsakingas asmuo pagal 11 punkte nurodytus kriterijus įvertina, ar duomenų saugumo pažeidimo apimtis ir faktinis ar galimas poveikis lemia Procedūros pradėjimą.

IV SKYRIUS
PROCEDŪRA – REAGAVIMO Į DUOMENŲ SAUGUMO PAŽEIDIMUS PROCEDŪROS PRADĖJIMAS

14. Formalus reagavimas į duomenų saugumo pažeidimą visais atvejais turėtų būti pradėtas tada, jei

nustatytos bet kurios iš toliau nurodytų aplinkybių:

14.1. Prarastas arba gali būti prarastas reikšmingas kiekis asmens duomenų;

14.2. Duomenų saugumo pažeidimas tikėtinai gali kelti didelį pavojų fizinių asmenų teisėms ir laisvėms;

14.3. Daromas poveikis dideliam Duomenų subjektų skaičiui;

14.4. Bet kokia kita situacija, kuri gali sukelti reikšmingą poveikį Duomenų valdytojui ir/arba Duomenų subjektams.

15. Jei nusprendžiama nepradėti Procedūros, tada 11 punkte aprašytas vertinimas turi būti tinkamai dokumentuotas už duomenų apsaugą atsakingo asmens raštu išdėstant sprendimo priežastis, motyvus ir kitas svarbias aplinkybes, o ši Procedūra laikoma užbaigta.

V SKYRIUS
PROCEDŪRA – DUOMENŲ SAUGUMO PAŽEIDIMO APRIBOJIMAS, LIKVIDAVIMAS IR ATKŪRIMAS

16. Pirmasis žingsnis sprendžiant duomenų saugumo pažeidimą yra jo apribojimas. Konkretūs veiksmai, atliktini norint tai pasiekti priklauso nuo konkretaus pažeidimo aplinkybių, bet tai galėtų būti tokie veiksmai kaip:

16.1. Asmens duomenų ištrynimas nuotoliniu būdu iš pamesto ar pavogto įrenginio;

16.2. Kuo skubesnis kreipimasis į asmenį, kuriam per klaidą buvo išsiųsti asmens duomenys, su prašymu neatidarinėti atsiųstų duomenų ir juos ištrinti be galimybės atkurti;

16.3. Atskleisto tretiesiems asmenims prisijungimo prie asmens duomenų bazės slaptažodžio pakeitimas;

16.4. Prarastų asmens duomenų atkūrimas iš turimos atsarginės kopijos;

16.5. Kiti veiksmai, kurie gali užtikrinti duomenų saugumo pažeidimo apribojimą, likvidavimą ar asmens duomenų atkūrimą.

17. Vykdant šią Procedūrą reikia imtis atsargumo priemonių tam, kad būtų užtikrinta, jog būtų surinkti kiek įmanoma tikslesni duomenys bei įrodymai apie įvykusį Duomenų saugumo pažeidimą (pavyzdžiui, užfiksuojama, kas, kada ir iš kokio įrenginio jungėsi prie asmens duomenų bazės, kam konkrečiai buvo per klaidą išsiųsti asmens duomenys, kokiomis aplinkybėmis buvo prarastas įrenginys su duomenimis).

18. Veiksmai, skirti atitaisyti žalą, sukeltą duomenų saugumo pažeidimo, turėtų būti nukreipti ne vien į esamo pažeidimo priežasties pašalinimą, bet ir skirti neleisti duomenų saugumo pažeidimui pasikartoti. Turėtų būti nustatytas bet koks pažeidžiamumas, kuris gali būti išnaudotas kaip pažeidimo elementas.

19. Prireikus gali būti pasitelkiama IT specialistų ar teisininkų pagalba.

20. Atkūrimo stadijoje sistemos turėtų būti pagal galimybes atstatytos į ankstesnę būklę, tačiau turėtų būti imamasi būtinų veiksmų tam, kad būtų atsižvelgta į trūkumus ir asmens duomenų tvarkymo silpnąsias vietas, kurios buvo išnaudotos įvykdant duomenų saugumo pažeidimą.

VI SKYRIUS
PROCEDŪRA – DUOMENŲ VALDYTOJO PRANEŠIMAS PRIEŽIŪROS INSTITUCIJAI APIE DUOMENŲ SAUGUMO PAŽEIDIMĄ

21. Duomenų valdytojas nepagrįstai nedelsdamas privalo informuoti Priežiūros instituciją apie duomenų saugumo pažeidimą tada, jei už duomenų apsaugą atsakingas asmuo nustato, kad duomenų saugumo pažeidimas tikėtinai gali kelti pavojų Duomenų subjektų, paveiktų duomenų

saugumo pažeidimo, teisėms ir laisvėms. Pavojų keliančiu laikytinas toks pažeidimas, dėl kurio Duomenų subjektas galėtų patirti kūno sužalojimą, materialinę ar nematerialinę žalą, teisių apribojimą, diskriminaciją, galėtų būti pavogta ar suklastota asmens tapatybė, jam padaryta finansinių nuostolių, neleistinai panaikinti pseudonimai, pakenkta jo reputacijai, prarastas asmens duomenų, kurie saugomi profesine paslaptimi, konfidencialumas arba padaryta kita ekonominė ar socialinė žala.

22. Jei Duomenų saugumo pažeidimas kelia pavojų Duomenų subjektų teisėms ir laisvėms, už duomenų apsaugą atsakingas asmuo ne vėliau kaip per 72 valandas nuo Duomenų valdytojo sužinojimo apie pažeidimą Priežiūros institucijai pateikia tokią informaciją:

22.1. Duomenų saugumo pažeidimo pobūdį, įskaitant, jeigu įmanoma, atitinkamai paveiktų Duomenų subjektų kategorijas ir apytikslį skaičių, taip pat atitinkamų asmens duomenų įrašų kategorijas ir apytikslį skaičių;

22.2. Kontaktinio asmens, galinčio suteikti daugiau informacijos, vardą, pavardę ir kontaktinius duomenis;

22.3. Tikėtinų duomenų saugumo pažeidimo pasekmių aprašymą;

22.4. Priemones, kurių ėmėsi arba planuoja imtis Duomenų valdytojas tam, kad būtų pašalintas duomenų saugumo pažeidimas, įskaitant, kai tinkama, priemones galimoms neigiamoms jo pasekmėms sumažinti.

23. Jeigu visos informacijos neįmanoma pateikti tuo pačiu metu, tolesnė informacija nepagrįstai nedelsiant gali būti teikiama etapais.

VII SKYRIUS
PROCEDŪRA – DUOMENŲ VALDYTOJO PRANEŠIMAS DUOMENŲ SUBJEKTUI APIE DUOMENŲ SAUGUMO PAŽEIDIMĄ

24. Kai dėl duomenų saugumo pažeidimo gali kilti didelis pavojus fizinių asmenų teisėms ir laisvėms, Duomenų valdytojas nepagrįstai nedelsdamas praneša apie asmens duomenų saugumo pažeidimą Duomenų subjektams. Didelį pavojų keliančiu gali būti laikytinas bet kuris 22 punkte nurodytų pasekmių riziką keliantis pažeidimas tada, jei tokios pažeidimo pasekmės yra labai tikėtinos, tvarkomi jautrūs asmens duomenys (pavyzdžiui, asmens duomenys apie sveikatą), pažeidimas turi neigiamą poveikį dideliam Duomenų subjektų skaičiui ir pan.

25. Už duomenų apsaugą atsakingas asmuo Duomenų subjektui aiškia ir paprasta kalba aprašo duomenų saugumo pažeidimo pobūdį ir pateikia bent jau žemiau nurodytą informaciją:

25.1. Kontaktinio asmens, galinčio suteikti daugiau informacijos, vardą, pavardę ir kontaktinius duomenis;

25.2. Tikėtinų duomenų saugumo pažeidimo pasekmių aprašymą;

25.3. Priemones, kurių ėmėsi arba planuoja imtis Duomenų valdytojas tam, kad būtų pašalintas duomenų saugumo pažeidimas, įskaitant, kai tinkama, priemones galimoms neigiamoms jo pasekmėms sumažinti.

26. Šios Procedūros 25 punkte nurodytas komunikavimas su Duomenų subjektu nebus reikalingas tada, jei egzistuoja bet kuri iš šių aplinkybių:

26.1. Duomenų valdytojas įgyvendino tinkamas technines ir organizacines apsaugos priemones ir tos priemonės taikytos asmens duomenims, kuriems duomenų saugumo pažeidimas turėjo poveikio, visų pirma tas priemones, kuriomis užtikrinama, kad asmeniui, neturinčiam leidimo susipažinti su asmens duomenimis, jie būtų nesuprantami, pavyzdžiui, šifravimo priemones;

26.2. Duomenų valdytojas vėliau ėmėsi priemonių, kuriomis užtikrinama, kad ateityje negalėtų kilti

didelis pavojus Duomenų subjektų teisėms ir laisvėms;

26.3. Tai pareikalautų neproporcingai daug pastangų. Tokiu atveju apie įvykusį duomenų saugumo pažeidimą paskelbiama viešai arba taikoma panaši priemonė, kuria Duomenų subjektai būtų informuojami taip pat efektyviai.

27. Priežiūros institucija, apsvarsčiusi, kokia yra tikimybė, kad dėl duomenų saugumo pažeidimo kils didelis pavojus, gali pareikalauti, kad Duomenų valdytojas informuotų Duomenų subjektus apie duomenų saugumo pažeidimą. Už duomenų apsaugą atsakingas asmuo gavęs tokį nurodymą turi nedelsdamas jį vykdyti.

VIII SKYRIUS
PROCEDŪRA – DUOMENŲ SAUGUMO PAŽEIDIMO DOKUMENTAVIMAS IR PROCEDŪROS UŽBAIGIMAS

28. Visi Asmens duomenų saugumo pažeidimai turi būti dokumentuoti, užpildant informaciją apie juos Asmens duomenų saugumo pažeidimo registre. Asmens duomenų saugumo pažeidimai registruojami nepriklausomai nuo to, ar apie tokį pažeidimą bus pranešama Priežiūros institucijai ir duomenų subjektams. Už Asmens duomenų saugumo pažeidimo registro pildymą atsako už duomenų apsaugą atsakingas asmuo.

29. Visi veiksmai, kurių imamasi Procedūros metu turi būti aprašomi ir visi susiję įrašai apie duomenų saugumo pažeidimą peržiūrimi tam, kad būtų užtikrintas jų išbaigtumas, tikslumas ir atitiktis teisiniam reguliavimui.

30. Už duomenų apsaugą atsakingas asmuo, gavęs supažindinto su duomenų saugumo pažeidimo ir jo pašalinimo aplinkybėmis Duomenų valdytojo vadovo pritarimą, priima sprendimą užbaigti Procedūrą tada, kai duomenų saugumo pažeidimas laikytinas pašalintu, o visoms reikalingoms šalims apie pažeidimą yra pranešta.

_____