PATVIRTINTA
Viešosios įstaigos
Vilniaus miesto krepšinio mokykla
Direktoriaus Vytenio Tupčiausko
2022 m. kovo 21 d.
įsakymu Nr. V-1.6 –64

Viešosios įstaigos Vilniaus miesto krepšinio mokyklos

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ REAGAVIMO TVARKOS APRAŠAS

1. BENDROSIOS NUOSTATOS

1.1. Šio Asmens duomenų saugumo pažeidimų reagavimo tvarkos aprašo (toliau – **Tvarka**) tikslas nustatyti Viešosios įstaigos Vilniaus miesto krepšinio mokykla, juridinio asmens kodas 305935833, buveinė adresu Birželio 23-iosios g. 10, Vilnius 03205, Lietuvos Respublika (toliau – **Mokykla**), procedūras, atliekamas siekiant tinkamai valdyti bet kokius asmens duomenų saugumo pažeidimus.

1.2. Tvarka yra privaloma visiems Mokyklos darbuotojams ir praktikantams.

2. ASMENS DUOMENŲ SAUGUMO PAŽEIDIMAS

2.1. Asmens duomenų saugumo pažeidimas yra tuomet, kai atsitiktinai ar neteisėtai atliekamas bet kuris iš šių veiksmų:

2.1.1. atskleidžiama ar suteikiama prieiga prie Mokyklos tvarkomų asmens duomenų (toliau – **Asmens duomenys**) (konfidencialumo pažeidimas);

2.1.2. prarandama prieiga prie Asmens duomenų arba jie sunaikinami (prieinamumo pažeidimas);

2.1.3. pakeičiami Asmens duomenys (vientisumo pažeidimas).

(toliau – bet kuris iš 2.1 p. nurodytų veiksmų – **ADSP**)

2.2. ADSP be kita ko apima šiuos atvejus:

2.2.1. konfidencialios informacijos atskleidimas asmenims, neturintiems teisės juos gauti;

2.2.2. duomenų arba įrangos, kuriuose saugomi duomenys, praradimas ar vagystė;

2.2.3. popierinių įrašų praradimas ar vagystė;

2.2.4. netinkamos prieigos kontrolės priemonės, leidžiančios neteisėtai naudoti informaciją;

2.2.5. įtariamas Mokyklos Informacinių ir komunikacinių technologijų naudojimo bei darbuotojų stebėsenos ir kontrolės darbo vietoje tvarkos aprašo pažeidimas;

2.2.6. mėginimas gauti neteisėtą prieigą prie kompiuterių sistemų, pvz., įsilaužimas;

2.2.7. įrašai pakeičiami arba ištrinami be leidimo;

2.2.8. virusai ar kita saugumo ataka prieš IT sistemas ar tinklus;

2.2.9. fizinio saugumo pažeidimai, pvz., fizinis ar elektroninis durų ar langų pažeidimas patalpose, kuriose laikoma konfidenciali informacija;

2.2.10. konfidencialios informacijos palikimas laisvai prieinamose vietose;

2.2.11. IT įrangos palikimas be priežiūros, kai prisijungiama prie vartotojo abonemento, neužblokuojamas ekranas;

2.2.12. sustabdoma neįgaliotų asmenų prieiga prie informacijos;

2.2.13. el. laiškai, kuriuose yra asmens duomenys, klaidingai išsiunčiami neteisingam gavėjui ir kt.

3. ADSP PRIELAIDOS

3.1. Pagrindiniai šaltiniai, kuriais naudojantis gali būti sukeltas ADSP ir sutrikdyta Mokyklos infrastruktūra, yra:

3.1.1. išorinės kompiuterinės laikmenos;

3.1.2. internetas;

3.1.3. interneto svetainių pagrindu veikianti programinė įranga;

3.1.4. paprasta įranga;

3.1.5. kiti ADSP šaltiniai.

3.2. Informacija apie galimą ADSP gali būti gaunama iš įvairių informacijos šaltinių:

3.2.1. IT paslaugų teikėjo, kuris atlieka asmens duomenų saugumo pažeidimų stebėseną;

3.2.2. Asmens duomenų tvarkytojų;

3.2.3. kompetentingų valstybės institucijų;

3.2.4. tarptautinių organizacijų arba institucijų, atliekančių asmens duomenų saugumo užtikrinimo funkcijas;

3.2.5. kitų juridinių ar fizinių asmenų.

3.3. Bet kuris darbuotojas ar praktikantas, gavęs informacijos apie galimą ADSP, nedelsiant praneša savo skyriaus vadovui ir duomenų apsaugos pareigūnui arba asmeniui, atsakingam už duomenų apsaugą Mokykloje, jei duomenų apsaugos pareigūnas nepaskirtas (toliau – **Saugumo pareigūnas**).

3.4. Reaguojant į galimą ADSP, atliekami tokie veiksmai (žr. lentelę apačioje):

3.4.1. ADSP nustatymas;

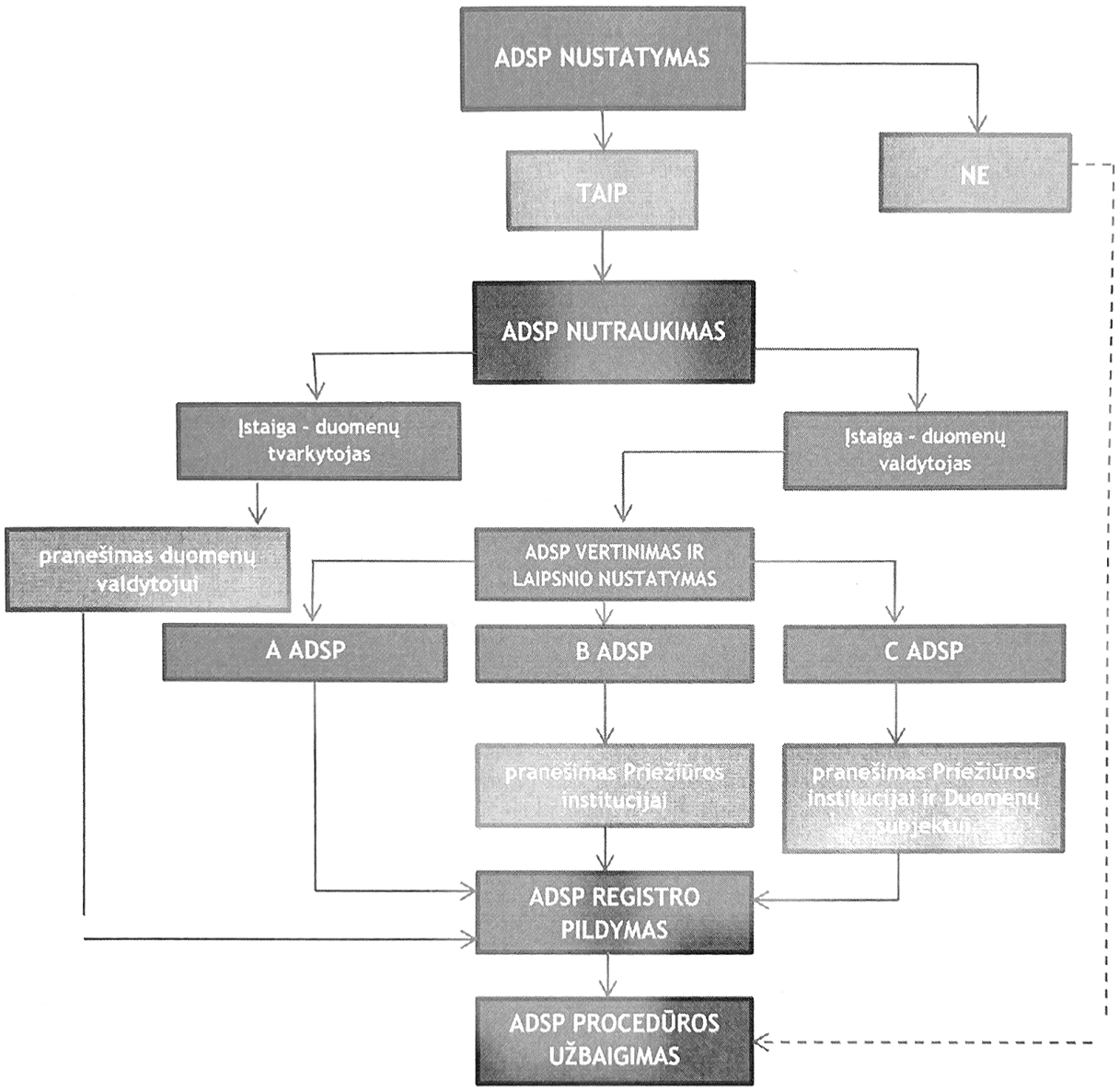
3.4.2. ADSP nutraukimas ir Asmens duomenų atkūrimas;

3.4.3. ADSP laipsnio vertinimas ir nustatymas;

3.4.4. pranešimas apie ADSP;

3.4.5. ADSP registro pildymas;

3.4.6. ADSP procedūros užbaigimas.



4. ADSP NUSTATYMAS

4.1. Saugumo pareigūnas įvertina gautą informaciją apie galimą ADSP pagal Tvarkos 2.1, 2.2 p. nurodytus kriterijus ir patvirtina arba paneigia ADSP nustatymo faktą.

4.2. Saugumo pareigūnas, patvirtinęs ADSP nustatymo faktą, per kuo trumpesnį laiką praneša Mokyklos vadovui apie ADSP. Jei reikia, sudaroma ADSP valdymo komanda (toliau – **Valdymo komanda**), į kurios sudėtį įeina Saugumo pareigūnas, taip pat gali įeiti atitinkamų skyrių vadovai, IT specialistas.

4.3. Saugumo pareigūnas nustato, ar pažeidimas susijęs su Asmens duomenimis, kuriuos tvarkydama Mokykla veikia kaip duomenų valdytojas, ar kaip tvarkytojas.

5. PAŽEIDIMO NUTRAUKIMAS IR PADĖTIES ATKŪRIMAS

5.1. Saugumo pareigūnas nedelsiant imasi visų įmanomų priemonių ADSP nutraukti ir padėčiai atstatyti. Jei būtina, pasitelkiami kiti Įstaigos darbuotojai, IT paslaugų teikėjai, Valdymo komanda.

5.2. Saugumo pareigūnas, veikdamas kartu su IT specialistu ir/arba Valdymo komanda, pagal kompetenciją, priklausomai nuo situacijos įvertina Mokyklos informacinės infrastruktūros būklę, nustato pažeistas jos dalis ir per kuo trumpesnį laiką imasi veiksmų pažeistoms dalims atkurti arba pakeisti ir (arba) teikia Mokyklos IT infrastuktūros paslaugos teikėjams siūlymus dėl pažeistų dalių atkūrimo arba pakeitimo, jeigu to negalima padaryti savo jėgomis.

5.3. Prieš atkurdamas Mokyklos informacinės infrastruktūros veiklą, Saugumo pareigūnas, veikdamas kartu su IT specialistu, privalo įsitikinti, ar pašalintas pažeidžiamumas, dėl kurio įvyko ADSP.

5.4. Pagrindiniai kriterijai, kuriais vadovaujantis priimamas sprendimas dėl ADSP valdymo priemonių:

5.4.1. numatytas galimas poveikis ir žala;

5.4.2. ADSP įrašų išsaugojimo, jų patikimumo, vientisumo ir pasiekiamumo užtikrinimas;

5.4.3. informacinės infrastruktūros neveikimo terminas;

5.4.4. ADSP valdymo sprendimui įgyvendinti reikalingas laikas ir ištekliai;

5.4.5. numatoma kita žala, kurią gali padaryti ADSP, priėmus jo valdymo sprendimą.

5.5. Konkretūs veiksmai, siekiant nutraukti ADSP ir atstatyti padėtį, galėtų būti tokie:

5.5.1. duomenų ištrynimas nuotoliniu būdu iš pamesto ar pavogto įrenginio;

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

5.5.3. tretiesiems asmenims atskleisto prisijungimo prie duomenų bazės slaptažodžio pakeitimas;

5.5.4. prarastų Asmens duomenų atkūrimas iš turimos atsarginės kopijos.

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

5.7. Suvaldant ADSP, taip pat vadovaujamasi Mokyklos duomenų tvarkymo informacinės sistemos veiklos tęstinumo valdymo planu.

6. PAŽEIDIMO LAIPSNIO VERTINIMAS

6.1. Saugumo pareigūnas nedelsiant, bet ne vėliau, kaip per 4 val. nuo ADSP, kuris susijęs su Asmens duomenimis, kuriuos Mokykla tvarko kaip duomenų valdytojas, nustatymo, išsiaiškina ADSP aplinkybes ir įvertina ADSP sunkumą, suteikiant ADSP vieną iš šių laipsnių: A – tikėtina, kad rizikos asmenims dėl ADSP nėra (toliau - **A ADSP**); B – dėl ADSP kyla rizika asmenims (toliau - **B ADSP**); C – dėl ADSP yra didelė rizika asmenims (toliau - **C ADSP**). Konkretus ADSP sunkumo laipsnis nustatomas pagal žemiau nurodytus kriterijus. Konkretų ADSP laipsnį patvirtina Įstaigos vadovas pagal Saugumo pareigūno rekomendaciją.

6.2. A ADSP laipsnis nustatomas tada, kai patiriamas ADSP, dėl kurio neturėtų kilti pavojaus fizinių asmenų, kurių Asmens duomenys tvarkomi (toliau – **Duomenų subjektai**), teisėms ir laisvėms. A ADSP gali būti, pavyzdžiui, kai nustatoma, kad paliktas kompiuteris neužrakintu ekranu, tačiau jokie asmenys, neturintys prieigos prie duomenų, nepateko į patalpą.

6.3. B ADSP laipsnis nustatomas tada, kai patiriamas ADSP, kuris kelia pavojų Duomenų subjektams (pavojų keliančiu laikytinas toks pažeidimas, dėl kurio asmuo galėtų patirti materialinę ar nematerialinę žalą, teisių apribojimą, diskriminaciją, galėtų būti pavogta ar suklastota asmens tapatybė, asmeniui padaryta finansinių nuostolių, neleistinai panaikinti pseudonimai, pakenkta asmens reputacijai, prarasti Asmens duomenys, kurie laikomi profesine paslaptimi, konfidencialumas arba padaryta kita ekonominė ar socialinė žala). Tokie atvejai galėtų būti, pavyzdžiui, laikmenos praradimas su kelių fizinių asmenų kontaktais.

6.4. C ADSP nustatomas tada, kai dėl ADSP gali kilti didelis pavojus fizinių Duomenų subjektų teisėms ir laisvėms (didelį pavojų keliančiu ADSP laikytinas bet kuris 6.3. punkte nurodytų pasekmių riziką keliantis ADSP, tada, kai tokios pažeidimo pasekmės yra labai tikėtinos, tvarkomi jautrūs Asmens duomenys (pavyzdžiui, duomenys apie sveikatą), pažeidimas turi neigiamą poveikį dideliam Duomenų subjektų skaičiui ir pan.). Pavyzdžiui, pametamas nešiojamasis kompiuteris, kuriame yra sutartys su fiziniais asmenimis.

7. PRANEŠIMAS APIE ADSP

7.1. Patvirtinus A ADSP, pranešimas nei Valstybinei duomenų apsaugos inspekcijai (toliau – **Priežiūros institucija**), nei Duomenų subjektams nėra teikiamas. ADSP dokumentuojama, kaip nurodyta Priede Nr. 1, ir užbaigiama ADSP procedūra.

7.2. Nustačius B ADSP, Saugumo pareigūnas ne vėliau kaip per 72 valandas nuo ADSP patvirtinimo momento Priežiūros institucijai pateikia reikiamą informaciją, užpildydamas Pranešimo formą, pateiktą Priede Nr. 2. Pranešimas Duomenų subjektams nėra teikiamas.

7.3. Pranešimas Priežiūros institucijai teikiamas per interneto svetainę www.vdai.lrv.lt, naudojantis elektronine paslaugų sistema; nesant tokios galimybės, pranešimas teikiamas elektroninio pašto adresu ada@ada.lt; nesant

tokioms galimybėms, Valstybinė duomenų apsaugos inspekcija informuojama telefono ryšio numeriu, kuris skelbiamas www.vdai.lrv.lt, ir nedelsiant informacija išsiunčiama registruotu laišku.

7.4. Jei Priežiūros institucijai apie ADSP nepranešama per 72 valandas, prie pranešimo Mokykla privalo pateikti vėlavimo priežastis.

7.4.1. Kai ir jeigu informacijos apie ADSP neįmanoma pateikti visa apimtimi tuo pačiu metu, informacija toliau nepagrįstai nedelsiant gali būti teikiama etapais.

7.4.2. Jei Priežiūros institucija paprašo patikslinti arba papildyti informaciją apie ADSP, Saugumo pareigūnas organizuoja papildomos informacijos surinkimą ir pateikimą Priežiūros institucijai jos nustatytu laiku.

7.5. Patvirtinus C ADSP, Mokykla praneša Priežiūros institucijai (tokia pačia tvarka, kaip pranešama apie B ADSP) ir nepagrįstai nedelsdama praneša apie ADSP Duomenų subjektams. Duomenų pareigūnas arba kitas atsakingas asmuo Duomenų subjektams turi pateikti aiškią ir suprantamą informaciją, kurioje turi būti bent ši informacija:

7.5.1. ADSP apibūdinimas;

7.5.2. tikėtinų padarinių, kurie jau atsirado arba gali atsirasti ateityje, sąrašas;

7.5.3. priemonių, kurių buvo imtasi ir/ar bus imtasi, norint sustabdyti ADSP bei pašalinti atsiradusius arba atsirasiančius padarinius, priemonių galimoms neigiamoms pasekmėms sumažinti sąrašas;

7.5.4. Saugumo pareigūno kontaktai.

7.6. 7.5. punkte nurodytas pranešimas Duomenų subjektui gali būti neteikiamas, jei egzistuoja bet kuri iš šių aplinkybių:

7.6.1. Mokykla įgyvendino tinkamas technines ir organizacines apsaugos priemones ir tos priemonės taikytos Asmens duomenims, kuriems ADSP turėjo poveikį;

7.6.2. Mokykla vėliau ėmėsi priemonių, kuriomis užtikrinama, kad ateityje negalėtų kilti didelis pavojus Duomenų subjektų teisėms ir laisvėms;

7.6.3. tiesioginis komunikavimas pareikalautų neproporcingai daug pastangų; tokiu atveju apie įvykusį ADSP, Mokyklos vadovui patvirtinus, paskelbiama viešai arba taikoma panaši priemonė, kuria Duomenų subjektai būtų informuojami taip pat efektyviai.

7.7. Saugumo pareigūnas, įvertinęs gautą informaciją apie ADSP, esant Mokyklos vadovo sutikimui, nedelsdamas informuoja apie ADSP nustatymo faktą ne tik Priežiūros instituciją ar Duomenų subjektą (kai reikia), bet ir policiją – nustačius, kad ADSP gali turėti nusikalstamos veikos požymių.

7.8. Jei nustatoma, kad ADSP susijęs su Asmens duomenimis, kuriuos Mokykla tvarko kaip duomenų tvarkytojas, informuojamas minėtų asmens duomenų valdytojas (pvz., bankas, draudimo įstaiga).

8. ADSP REGISTRO PILDYMAS

8.1. Visi veiksmai, kurių imamasi ADSP valdymo procedūros metu, turi būti aprašomi ir visi susiję įrašai apie ADSP peržiūrimi tam, kad būtų užtikrintas jų išbaigtumas, tikslumas ir atitiktis atitinkamam teisiniam reguliavimui. Šiam tikslui pasiekti turi būti vedamas ADSP žurnalas, kuriame tiksliai aprašomi veiksmai, kurių buvo imtasi įgyvendinant ADSP valdymo procedūrą.

8.2. ADSP žurnalo elektroninė forma yra pateikta Priede Nr. 1. Elektroninį ADSP registrą pildo Saugumo pareigūnas. ADSP žurnale saugomi ne senesni, nei 10 metų, įrašai.

8.3. ADSP žurnale esantys įrašai peržiūrimi Saugumo pareigūno ne rečiau, kaip kartą per kalendorinį ketvirtį. ADSP išanalizuojami ne vėliau, kaip per vieną kalendorinį mėnesį nuo jų nustatymo. Saugumo pareigūnas išanalizuoja ADSP ir pateikia ataskaitą su išvadomis bei rekomenduojamomis įgyvendinti prevencijos priemonėmis Mokyklos vadovui. Prevencijos priemonės įgyvendinamos Saugumo pareigūno ataskaitoje pasiūlytais ir vadovo patvirtintais terminais. Saugumo pareigūnas kontroliuoja, kaip įgyvendinamos ADSP prevencijos priemonės.

9. ADSP PROCEDŪROS UŽBAIGIMAS

9.1. Suvaldžius ADSP, Saugumo pareigūnas apie ADSP suvaldymo rezultatus informuoja Mokykla vadovą.

9.2. Saugumo pareigūnas, gavęs supažindinto su ADSP ir jo pašalinimo aplinkybėmis Mokyklos vadovo pritarimą, priima sprendimą užbaigti ADSP valdymo procedūrą tada, kai ADSP laikytinas likviduotu, o visoms reikalingoms šalims apie ADSP yra pranešta.

10. DARBUOTOJŲ SUPAŽINDINIMAS SU TVARKA

10.1. Darbuotojai supažindinami su šia Tvarka tokiu būdu:

10.1.1. nedelsiant po Tvarkos patvirtinimo Tvarka išsiunčiama esamiems Mokykla darbuotojams, kurie turi darbinį elektroninį paštą, elektroniniu paštu;

10.1.2. nedelsiant po Tvarkos patvirtinimo Tvarka patalpinama Mokyklos serveryje (ar kitoje vietoje, kur saugomi visi Mokyklos vidaus dokumentai, tvarkos ir taisyklės) ir ten yra pasiekiama darbuotojams bet kuriuo metu;

10.1.3. kiekvienas naujas darbuotojas supažindinamas su Tvarka pirmąją jo darbo dieną Mokykloje, pateikiant jam Tvarką elektroniniu paštu ar sudarant galimybę pasiekti Tvarką Mokyklos serveryje;

10.1.4. tie darbuotojai, kurie neturi darbinio elektroninio pašto, su Tvarka supažindinami raštu;

10.1.5. praktikantai su Tvarka supažindinami raštu.

10.2. Elektroniniu paštu išsiųsta Tvarka yra laikoma įteikta:

(i) tą pačią darbo dieną, jei buvo išsiųsta ne vėliau kaip likus 1 (vienai) valandai iki Mokyklos darbo laiko pabaigos;

(ii) kitą darbo dieną, jei buvo išsiųsta vėliau, kaip likus 1 (vienai) valandai iki Mokyklos darbo laiko pabaigos arba po Mokyklos darbo laiko pabaigos;

(iii) artimiausią darbo dieną, jei buvo išsiųsta poilsio ar švenčių dieną;

(iv) artimiausią Mokyklos darbo dieną, jei buvo išsiųsta darbuotojui jo kasmetinių atostogų ar nedarbingumo metu;

(v) artimiausią darbuotojo darbo dieną po komandiruotės, jei buvo išsiųsta darbuotojui jo komandiruotės metu, o komandiruotėje nebuvo užtikrintas interneto ryšys.

Forma patvirtinta Valstybinės duomenų apsaugos inspekcijos direktoriaus 2018 m. rugpjūčio 29 d. įsakymu Nr. 1T-82(1.12.E).

Priedas Nr. 2 prie
ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ REAGAVIMO
TVARKOS APRAŠO

_____

(duomenų valdytojo (juridinio asmens) pavadinimas, duomenų valdytojo atstovo pavadinimas, duomenų valdytojo (fizinio asmens) vardas, pavardė)[1]

_____

(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, ir (ar) elektroninės siuntos pristatymo dėžutės adresas)

Valstybinei duomenų apsaugos inspekcijai

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 _____

[1] Kai pranešimas apie asmens duomenų saugumo pažeidimą teikiamas pagal Lietuvos Respublikos asmens duomenų, tvarkomų nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas, bausmių vykdymo arba nacionalinio saugumo ar gynybos tikslais, teisinės apsaugos įstatymo (toliau – Įstatymas) 29 straipsnį, nurodomi tik duomenų valdytojo (juridinio asmens) duomenys.

Asmens duomenų saugumo pažeidimo nustatymo:

Data _____ Laikas _____

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

- ☐ Informacinė sistema
- ☐ Duomenų bazė
- ☐ Tarnybinė stotis
- ☐ Internetinė svetainė
- ☐ Debesų kompiuterijos paslaugos
- ☐ Nešiojami / mobilus 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 paslaugomis
- ☐ 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 prieiti, pavyzdžiui, prie asmens sveikatos istorijų ir teikti pacientams sveikatos paslaugų, arba įgyvendinti duomenų subjekto teises)
- ☐ Dėl klaidų asmens duomenų tvarkymo procesuose negalima teikti tinkamos paslaugos (pavyzdžiui, asmens sveikatos istorijoje neliko informacijos apie asmens alergijas, 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)[2]

6.1. Vardas ir pavardė _____

[2] Kai pranešimas apie asmens duomenų saugumo pažeidimą teikiamas pagal Įstatymo 29 straipsnį, nenurodomi šios formos 6.4 ir 6.5 papunkčiuose nurodyti duomenys.

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)