PATVIRTINTA
Higienos instituto direktoriaus
2020 m. rugsėjo 8 d. įsakymu Nr. V-47
(Higienos instituto direktoriaus
2021 m. liepos 26 d. įsakymo Nr. V-29
redakcija)

HIGIENOS INSTITUTO TVARKOMŲ ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ VALDYMO TVARKOS APRAŠAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Higienos instituto tvarkomų asmens duomenų saugumo pažeidimų valdymo tvarkos aprašas (toliau – Aprašas) nustato asmens duomenų saugumo pažeidimų (toliau – pažeidimas) ir jų priežasčių klasifikavimą, pranešimo apie pažeidimus Valstybinei duomenų apsaugos inspekcijai (toliau – Inspekcija) ir duomenų subjektams, pažeidimų tyrimo, jų ir jų pasekmių pašalinimo ir mažinimo, pažeidimų prevencijos ir dokumentavimo tvarką.

2. Aprašas taikomas Higienos instituto darbuotojams ir Higienos instituto tvarkytojams.

3. Aprašas parengtas atsižvelgiant į 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentą (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) (toliau – Reglamentas (ES) 2016/679).

4. Apraše vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos Reglamente (ES) 2016/679 ir Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme.

II SKYRIUS
PAŽEIDIMŲ IR JŲ PRIEŽASČIŲ KLASIFIKAVIMAS

5. Pažeidimai pagal pobūdį (tipą) yra:

5.1. konfidencialumo pažeidimas – netyčinis arba neteisėtas asmens duomenų laikinas ar nuolatinis atskleidimas ar prieigos prie asmens duomenų suteikimas asmenims, kurie neturi teisės susipažinti su asmens duomenimis;

5.2. prieinamumo pažeidimas – neteisėtas, laikinas ar nuolatinis prieigos prie asmens duomenų praradimas arba asmens duomenų sunaikinimas;

5.3. vientisumo pažeidimas – neteisėtas asmens duomenų laikinas ar nuolatinis pakeitimas;

5.4. mišraus pobūdžio (tipo) pažeidimas – asmens duomenų konfidencialumo, prieinamumo ir vientisumo pažeidimas ar bet kurių Aprašo 5.1–5.3 papunkčiuose nurodytų pažeidimų derinys.

6. Pažeidimai gali būti nulemti šių priežasčių:

6.1. 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 ir kt.);

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

6.3. *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 6.1 papunktyje, ir kt.).

III SKYRIUS
PRANEŠIMAS APIE GALIMĄ PAŽEIDIMĄ IR JO NAGRINĖJIMAS

7. Higienos instituto darbuotojas ar Higienos instituto tvarkytojo darbuotojas, sužinojęs ar pats nustatęs galimą pažeidimą arba kai informacija apie galimą pažeidimą gaunama iš žiniasklaidos ar kito šaltinio (toliau – galimo pažeidimo paaiškėjimas), privalo:

7.1. nedelsiant, bet ne vėliau kaip per 2 darbo valandas nuo galimo pažeidimo paaiškėjimo momento informuoti žodžiu, raštu ar elektroninėmis priemonėmis savo tiesioginį vadovą ir Higienos instituto duomenų apsaugos pareigūną;

7.2. nedelsiant, bet ne vėliau kaip per 4 darbo valandas nuo galimo pažeidimo paaiškėjimo momento užpildyti Aprašo 1 priede nustatytos formos pranešimą apie galimą pažeidimą (toliau – pranešimas) ir perduoti jį tiesioginiam vadovui ir Higienos instituto duomenų apsaugos pareigūnui;

7.3. jei įmanoma, imtis priemonių pašalinti galimą pažeidimą ir priemonių galimoms neigiamoms jo pasekmėms sumažinti.

8. Higienos instituto duomenų apsaugos pareigūnas, gavęs pranešimą privalo:

8.1. informaciją apie galimą pažeidimą fiksuoti Asmens duomenų saugumo pažeidimų registracijos žurnale (Aprašo 2 priedas) (toliau – Žurnalas);

8.2. nedelsiant perduoti pranešimą Higienos instituto direktoriaus įgaliotam asmeniui;

8.3. Higienos instituto direktoriui patarti dėl pažeidimo tyrimo ir teikti išvadas dėl pranešimų Inspekcijai ir (ar) duomenų subjektui;

8.4. bendradarbiauti su Inspekcija dėl pažeidimų;

8.5. stebėti, kaip vykdomos Reglamente (ES) 2016/679 ir Apraše nustatytos Higienos instituto pareigos, susijusios su pažeidimų valdymu.

9. Higienos instituto direktoriaus įgaliotas asmuo, gavęs iš Higienos instituto duomenų apsaugos pareigūno pranešimą, privalo:

9.1. atlikti pažeidimo tyrimą Aprašo IV skyriaus nustatyta tvarka;

9.2. pasitelkti Higienos instituto darbuotojus pagal kompetenciją, jei pažeidimas yra susijęs su elektroninės informacijos saugos ir (ar) kibernetiniu incidentu;

9.3. asmens duomenų saugumo galimo pažeidimo atveju, kai galimas pažeidimas yra susijęs su kibernetiniu incidentu, informaciją apie galimą pažeidimą kartu su informacija apie kibernetinį incidentą pateikti asmeniui, atsakingam už kibernetinio saugumo organizavimą ir užtikrinimą Higienos institute;

9.4. teikti rekomendacijas Higienos instituto darbuotojams, atsakingiems už pažeidimo ir (ar) jo pasekmių pašalinimą ir (ar) sumažinimą, dėl tinkamų techninių ir organizacinių priemonių, kad pažeidimas būtų išsamiai ištirtas ir jis ir (ar) jo pasekmės būtų pašalintos ir (ar) sumažintos ir pažeidimas ateityje nepasikartotų, taikymo ir (arba) pats imtis šių veiksmų.

10. Kai yra įtariama, kad pažeidimas turi nusikalstamos veikos požymių, informacija apie galimą nusikalstamą veiką pateikiama valstybės institucijoms, įgaliotoms atlikti ikiteisminį

tyrimą, teisės aktų, reguliuojančių tokios informacijos teikimą, nustatyta tvarka. Asmens duomenų, tvarkomų Higienos institute, saugumo pažeidimo atveju tokį pranešimą pateikia Higienos instituto direktoriaus įgaliotas asmuo.

IV SKYRIUS
PAŽEIDIMO TYRIMAS

11. Higienos instituto direktoriaus įgaliotas asmuo nedelsiant, bet ne vėliau kaip per 24 valandas nuo pranešimo gavimo momento, išnagrinėja pranešime nurodytas aplinkybes, įvertina, ar padarytas pažeidimas, jei pažeidimas padarytas, nustato, kokio pobūdžio (tipo) pažeidimas padarytas, asmens duomenų, kurių saugumas pažeistas, kategorijas, įskaitant specialių kategorijų asmens duomenis, pažeidimo priežastis, pažeidimo apimtis (duomenų subjektų kategorijos ir jų skaičius), esamas ir (ar) galimas pasekmes ir žalą, padarytą duomenų subjektui (-ams), įvertina pavojų duomenų subjekto teisėms ir laisvėms (toliau – rizika), kuris gali atsirasti dėl galimo pažeidimo, Aprašo 13-14 punktuose nustatyta tvarka ir pateikia Higienos instituto duomenų apsaugos pareigūnui ir Higienos instituto direktoriui išvadą dėl pažeidimo buvimo ir rizikos.

12. Pažeidimo tyrimo metu Higienos instituto darbuotojai privalo operatyviai teikti Higienos instituto direktoriaus įgaliotam asmeniui visą jo paprašytą su pažeidimu susijusią informaciją ir dokumentus.

13. Rizika vertinama objektyviai įvertinus pažeidimo aplinkybes ir atsižvelgiant į:

13.1. pažeidimo pobūdį (tipą);

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

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

13.4. padarinių duomenų subjektui sunkumą. Vertinant riziką turi būti laikoma, kad 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;

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

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

13.7. duomenų valdytojo savybes (pvz., veiklos pobūdį).

14. Įvertinus riziką nustatoma, kad yra:

14.1. maža rizika, kai nustatoma, kad pavojaus duomenų subjekto teisėms ir laisvėms nėra;

14.2. vidutinė rizika, kai nustatoma, kad dėl asmens duomenų saugumo pažeidimo yra / gali kilti nedidelis pavojus duomenų subjektų teisėms ir laisvėms;

14.3. didelė rizika, kai nustatoma, kad dėl asmens duomenų saugumo pažeidimo yra / gali kilti didelis pavojus duomenų subjektų teisėms ir laisvėms.

15. Jeigu per 24 val. nuo pranešimo gavimo momento dėl objektyvių priežasčių nebuvo nustatytos visos aplinkybės, nurodytos Aprašo 13, 14 punktuose, Higienos instituto direktoriaus įgaliotas asmuo atlieka tolesnį pažeidimo tyrimą. Šiame punkte nurodytas tyrimas turi būti atliktas ir parengta Aprašo 3 priede nustatytos formos Asmens duomenų saugumo pažeidimo ataskaita (toliau – Ataskaita), kuri turi būti pateikta Higienos instituto direktoriui, Higienos instituto

duomenų apsaugos pareigūnui ne vėliau kaip per 20 darbo dienų nuo pažeidimo paaiškėjimo dienos.

16. Jeigu išvadoje dėl pažeidimo buvimo ir rizikos nurodyta, kad rizikos nėra, tačiau Aprašo 15 punkte nurodyto pažeidimo tyrimo metu nustatoma, kad rizika gali kilti, arba jo metu pasikeitė rizikos laipsnis, Higienos instituto direktoriaus įgaliotas asmuo turi riziką vertinti iš naujo Aprašo 13–14 punktuose nustatyta tvarka.

V SKYRIUS
PRANEŠIMAS INSPEKCIJAI

17. Aprašo 14.2 ir 14.3 papunkčiuose nurodytais atvejais Higienos institutas ne vėliau kaip per 72 valandas nuo galimo pažeidimo paaiškėjimo momento, Inspekcijos nustatyta tvarka ir sąlygomis praneša apie pažeidimą Inspekcijai (toliau – pranešimas Inspekcijai). Kai sužinojus apie galimai įvykusį pažeidimą nėra objektyvių galimybių per 72 valandas nustatyti, ar pažeidimas tikrai įvyko, Inspekcijai per 72 valandas nuo sužinojimo apie galimai įvykusį pažeidimą pateikti pranešimą apie pažeidimą, nurodant tiek informacijos, kiek tuo metu yra žinoma. Jeigu, įvertinus riziką, abejojama, ar ji yra ir ar reikia pranešti apie Pažeidimą Inspekcijai, būtina pranešti.

18. Higienos instituto duomenų apsaugos pareigūnas per 24 val. nuo Higienos instituto direktoriaus įgalioto asmens išvados dėl pažeidimo buvimo ir rizikos gavimo momento, pateikia išvadą Higienos instituto direktoriui dėl pranešimo apie pažeidimą Inspekcijai bei Aprašo 14.2 ir 14.3 papunkčiuose nurodytais atvejais parengia pranešimo dėl asmens duomenų, tvarkomų Higienos institute, saugumo pažeidimo projektą.

19. Higienos instituto direktorius per 24 val. nuo Aprašo 18 punkte nurodytos Higienos instituto direktoriaus duomenų apsaugos pareigūno išvados gavimo momento priima sprendimą dėl pranešimo teikimo Inspekcijai ir informuoja apie priimtą sprendimą Higienos instituto direktoriaus įgaliotą asmenį ir Higienos instituto duomenų apsaugos pareigūną. Jeigu abejojama dėl rizikos priskyrimo Aprašo 14.2 ar 14.3 papunkčiuose nurodytam rizikos lygiui, apie pažeidimą Inspekcijai pranešama.

20. Jeigu atliekamas Aprašo 15 punkte nurodytas tyrimas, Inspekcijai informacija gali būti teikiama etapais. Apie informacijos teikimą etapais Higienos institutas Inspekciją informuoja pranešime Inspekcijai.

21. Jeigu po pranešimo Inspekcijai pateikimo, atlikus Aprašo 15 punkte nurodytą tolesnį tyrimą, yra nustatoma, kad saugumo incidentas buvo sustabdytas ir nebuvo pažeidimo, apie tai ne vėliau kaip per 3 darbo dienas nuo šios informacijos paaiškėjimo momento Higienos institutas informuoja Inspekciją ir apie tai pažymima Žurnale.

VI SKYRIUS
PRANEŠIMAS DUOMENŲ SUBJEKTUI

22. Aprašo 14.3 papunktyje nurodytu atveju Higienos institutas privalo nedelsdamas, jei yra galimybė, per 72 val. nuo galimo pažeidimo paaiškėjimo momento, apie tai raštu pranešti duomenų subjektui, kurio teisėms ir laisvėms dėl šio pažeidimo kyla didelė rizika. Pranešimas rengiamas ir teikiamas šio skyriaus ir Aprašo 17–19 punktuose *mutatis mutandis* nustatyta tvarka.

23. Pranešime duomenų subjektui aiškia ir paprasta kalba pateikiama:

23.1. pažeidimo pobūdžio aprašymas;

23.2. Higienos instituto duomenų apsaugos pareigūno arba kito kontaktinio asmens vardas, pavardė (pavadinimas) ir kontaktiniai duomenys;

23.3. galimų pažeidimo pasekmių aprašymas;

23.4. priemonių, kurių ėmėsi Higienos institutas arba siūlo imtis duomenų subjektui, kad būtų pašalintas pažeidimas ir (ar) pašalintos ar sumažintos galimos neigiamos jo pasekmės, aprašymas (pvz., kad apie pažeidimą yra informuota Inspekcija ir kad yra gautas patarimas dėl

pažeidimo pasekmių pašalinimo ar sumažinimo; siūlymas duomenų subjektui pasikeisti slaptažodžius ir kt.);

23.5. kita reikšminga informacija, susijusi su pažeidimu, kuri, Higienos instituto manymu, turėtų būti pateikta duomenų subjektui.

24. Pranešimo pateikimo būdas pasirenkamas atsižvelgiant į tai, kokius duomenų subjekto kontaktinius duomenis tvarko Higienos institutas, ir į tai, kuris būdas geriausiai užtikrintų, kad pranešimas pasiektų adresatą. Šis pranešimas turi būti atskirtas nuo kitos siunčiamos informacijos, tokios kaip nuolatiniai atnaujinimai, naujienlaiškiai ar standartiniai pranešimai. Gali būti taikomi keli pranešimo duomenų subjektui apie pažeidimą būdai.

25. Pranešimas duomenų subjektui apie pažeidimą neteikiamas, išskyrus, jei teikti pranešimą reikalauja Inspekcija, šiais atvejais:

25.1. Higienos institutas įgyvendino tinkamas technines ir organizacines asmens duomenų apsaugos priemones, kurios užtikrino, kad įvykus pažeidimui nekils rizika, ir tos priemonės taikytos asmens duomenims, kuriems pažeidimas turėjo poveikio (pvz., asmens duomenys buvo šifruoti);

25.2. iš karto po pažeidimo Higienos institutas ėmėsi priemonių, kuriomis užtikrinama, kad nebegalėtų kilti rizika;

25.3. reikėtų neproporcingai daug pastangų susisiekti su duomenų subjektais (pvz., kai jų kontaktiniai duomenys buvo prarasti dėl pažeidimo arba nežinomi). Tokiu atveju Aprašo 23 punkte nurodyta informacija apie pažeidimą paskelbiama viešai arba taikoma panaši priemonė, kuria duomenų subjektai būtų informuojami taip pat efektyviai, pvz., pranešimas interneto svetainėje, spaudoje ar pan.

26. Jeigu Higienos institutas pranešimo duomenų subjektui apie pažeidimą neteikė, Higienos institutas turi pagrįsti Inspekcijai, kad įvykdė vieną iš Aprašo 25 punkte nurodytų sąlygų.

VII SKYRIUS
ŽURNALO DUOMENŲ TVARKYMAS

27. Higienos institute tvarkomas Žurnalas, kuriame nurodoma:

28.1. Visi su pažeidimu susiję faktai – pažeidimo priežastis, kas įvyko ir kokie asmens duomenys pažeisti;

28.2. pažeidimo poveikis ir pasekmės;

28.3. taisomieji veiksmai (techninės priemonės), kurių buvo imtasi;

28.4. su pažeidimu susijusių sprendimų priėmimo priežastys (pvz., kodėl duomenų valdytojas nusprendė nepranešti apie pažeidimą Inspekcijai ir (ar) duomenų subjektui, t. y. kodėl nusprendė, kad rizika žema, arba kokią Aprašo 25 punkte nurodytą sąlygą įvykdė);

28.5. pranešimo Inspekcijai pateikimo vėlavimo priežastys (jeigu pranešimą vėluojama pateikti ar pranešimas teikiamas etapais);

28.6. informacija, susijusi su pranešimu duomenų subjektui (pvz., ar buvo pranešta, kodėl nepranešta ir pan.);

28.7. kita reikšminga informacija, susijusi su pažeidimu (pvz., kad tyrimo metu nustatyta, jog Pažeidimo nebuvo, o buvo tik saugumo incidentas).

29. Už Žurnalo pildymą ir saugojimą atsakingas Higienos instituto duomenų apsaugos pareigūnas. Žurnale registruojami visi pažeidimai, nepaisant to, ar apie juos pranešta Inspekcijai ir (ar) duomenų subjektui, ar tokie pažeidimai kelia riziką. Žurnalas turi būti popierinės formos. Užpildytas Žurnalas saugomas 5 metus nuo paskutinio įrašo Žurnale padarymo.

31. Informacija apie pažeidimą į Žurnalą turi būti įvedama nedelsiant, kai tik paaiškėja galimas pažeidimas, bet ne ilgiau kaip per 5 darbo dienas nuo galimo pažeidimo paaiškėjimo momento. Kai pasikeičia Žurnale nurodyta informacija arba paaiškėja nauja informacija, Žurnale esanti informacija turi būti papildoma ir (ar) koreguojama.

32. Žurnalas yra pateikiamas Inspekcijai jai pareikalavus.

33. Higienos instituto duomenų apsaugos pareigūnas kartą per ketvirtį peržiūri Žurnale esančius įrašus ir pasiūlo Higienos instituto direktoriui, kokios prevencijos priemonės turėtų būti įgyvendintos bei kaip turėtų būti kontroliuojamas šių prevencijos priemonių įdiegimas, kad ateityje tokie patys pažeidimai nesikartotų.

VIII SKYRIUS
BAIGIAMOSIOS NUOSTATOS

34. Higienos instituto darbuotojai 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.

35. Prireikus Higienos institute gali būti sudaryta darbo grupė tirti pažeidimus (įskaitant jų priežastis, pasekmes) bei teikti pasiūlymus Higienos instituto direktoriui dėl pažeidimų išvengimo ateityje. Higienos institutas nuolat tobulina vidinius procesus, atsižvelgdamas į nustatytas pažeidimų priežastis.

36. Atsižvelgęs į Ataskaitą Higienos instituto direktorius prireikus tvirtina priemonių planą, kuriame numatomos būtinos techninės, organizacinės, administracinės ir kitos priemonės, reikalingos užkirsti kelią pažeidimams, jų pasekmėms pašalinti ar sumažinti, atsakingi priemonių vykdytojai ir įgyvendinimo terminai.

_____