UŽDAROSIOS AKCINĖS BENDROVĖS
„KRETINGOS VANDENYS"
DIREKTORIUS

ĮSAKYMAS
DĖL ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ VALDYMO TVARKOS APRAŠO PATVIRTINIMO

2025 m. birželio 9 d. Nr. V-30
Kretinga

Vadovaudamasi 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) ir Lietuvos Respublikos vietos savivaldos įstatymo 29 straipsnio 8 dalies 2 punktu:

1. T v i r t i n u Asmens duomenų saugumo pažeidimų valdymo tvarkos aprašą (pridedama).
2. P a v e d u UAB „Kretingos vandenys" administratorei Aušrai Danylienei dokumentų valdymo sistemoje „Kontora" su šiuo įsakymu supažindinti bendrovės darbuotojus.
3. Į p a r e i g o j u IT, GIS, telemetrijos procesų inžinierių Tomą Dorelį paskelbti šį įsakymą ir pridedamus dokumentus viešai Bendrovės interneto svetainėje.

Direktorė Eglė Alonderienė

Šarūnas Jonas Tamulis, 115
Išplatinama: 112, 115, 116, 117, 1200P, 1201E, 1202T, 1204V, 1205N, 1206D, 1207SE, 1208SA

PATVIRTINTA
UAB „Kretingos vandenys“ direktoriaus
2025 m. birželio 9 d. įsakymu Nr. V-30

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ VALDYMO TVARKOS APRAŠAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Asmens duomenų saugumo pažeidimų valdymo tvarkos aprašas (toliau – Aprašas) nustato UAB „Kretingos vandenys“ (toliau – Bendrovė) bei darbuotojų, dirbančių pagal darbo sutartis (toliau – Darbuotojai), veiksmus įvykus duomenų saugumo pažeidimui, jų išaiškinimo, tyrimo, pašalinimo ir pranešimo priežiūros institucijai, duomenų subjektams tvarką bei kitus atvejus įgyvendinant 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamento (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 – BDAR) 5, 33 ir 34 straipsnių reikalavimus.

2. Aprašu privalo vadovautis visi Bendrovės darbuotojai, kurie tvarko asmens duomenis arba eidami savo pareigas juos sužino.

3. Darbuotojai privalo užtikrinti, kad Bendrovės pasitelkiami duomenų tvarkytojai, be kitų reikalavimų, numatytų BDAR 28 straipsnyje, būtų įpareigoti laikytis atitinkamų Apraše numatytų reikalavimų, užtikrinančių pareigą pasitelkiamam duomenų tvarkytojui tinkamai informuoti Bendrovę apie jos nustatytu tikslu ir priemonėmis tvarkomų duomenų saugumo pažeidimą, bendradarbiauti aiškinantis duomenų saugumo pažeidimo priežastis, teikti visą reikiamą informaciją, kad Bendrovė galėtų tinkamai įgyvendinti duomenų valdytojui tenkančias pareigas, numatytas BDAR.

4. Aprašas parengtas vadovaujantis BDAR, Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu (toliau – Įstatymas) ir kitais galiojančiais teisės aktais.

5. Apraše vartojamos sąvokos:

5.1. **duomenų saugumo pažeidimas** – bet koks įvykis, dėl kurio netyčia arba neteisėtai sunaikinami, prarandami, pakeičiami, be leidimo atskleidžiami tvarkomi asmens duomenys arba prie jų be leidimo gaunama prieiga;

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

5.3. **priežiūros institucija** – valstybės narės pagal BDAR 51 straipsnį įsteigta nepriklausoma valdžios institucija. Administracijos atžvilgiu tai Valstybinė duomenų apsaugos inspekcija (įmonės kodas 188607912, L. Sapiegos g. 17, 10312 Vilnius, el. paštas ada@ada.lt);

5.4. kitos Apraše vartojamos sąvokos atitinka BDAR ir Įstatyme įtvirtintas sąvokas.

II SKYRIUS
ASMENS DUOMENŲ SAUGUMO PAŽEIDIMO NUSTATYMAS

6. Duomenų saugumo pažeidimu (toliau – Pažeidimas) laikomas bet koks saugumo incidentas, dėl kurio įvyksta vienas arba keli toliau numatyti pažeidimai:

6.1. konfidencialumo pažeidimas – netyčia ar neteisėtai atskleidžiami asmens duomenys (pvz., duomenų kopijos išsiuntimas trečiajam asmeniui, neturinčiam teisinio pagrindo juos gauti); prisijungimo prie duomenų bazės slaptažodžio paviešinimas, praradimas, atskleidimas kitam Darbuotojui, neturinčiam teisės dirbti su šiais duomenimis; ne saugojimui skirtoje vietoje palikti dokumentai, kuriuose yra asmens duomenų; pamesti

nešiojami / mobilūs įrenginiai (telefonas, nešiojamas kompiuteris, išorinės duomenų laikmenos), kuriuose saugomi asmens duomenys ir kt.; vagystė (pvz., pavogti nešiojami / mobilūs įrenginiai, kuriuose saugomi asmens duomenys; pavogtos ar kitokiu būdu prarastos neautomatiniu būdu susistemintos bylos, kuriose yra asmens duomenų ir kt.); neleistina (neautorizuota) prieiga prie asmens duomenų (pvz., įgaliojimų neturintys asmenys patenka į patalpas, kuriose saugomos bylos su asmens duomenimis, įgaliojimų neturintys asmenys prisijungia prie duomenų bazių ar informacinių sistemų ir kt.);

6.2. prieinamumo pažeidimas – netyčia ar neteisėtai prarandama prieiga prie asmens duomenų arba duomenys yra sunaikinami. Tokio pobūdžio pažeidimu galėtų būti laikomas duomenų bazės ištrynimas nesant atsarginės kopijos, iš kurios būtų galima atkurti prarastus duomenis. Prieinamumo pažeidimu laikytinas ir įprastinę Bendrovės veiklą sutrikdęs prieigos prie duomenų praradimas bei nenumatytos (force majeure) aplinkybės ir kitos priežastys (gaisras, vandens užliejimas, dėl kurių sugadinami arba prarandami asmens duomenys ir kt.) ar įrenginių programinės įrangos gedimas, saugos sistemos spragos (pvz., energijos tiekimo nutrūkimas, dėl kurio negalima prieiga prie asmens duomenų; programos kodo, kuriuo kontroliuojamas prieigos teisių suteikimas informacinių sistemų naudotojams, klaida ir kt.);

6.3. vientisumo pažeidimas – netyčia ar neteisėtai atlikti asmens duomenų pakeitimai. Tai galėtų būti trečiojo asmens, įgijusio neteisėtą prisijungimą prie duomenų bazės, įvykdyti joje esančių įrašų pakeitimai ar kibernetinė ataka (pvz., duomenų bazėje ar informacinėje sistemoje esantys asmens duomenys užšifruojami naudojant išpirkos reikalaujančią programą; internete paskelbiami informacinių sistemų naudotojų vardai ir slaptažodžiai ir kt.);

6.4. mišraus pobūdžio pažeidimas – asmens duomenų konfidencialumo, prieinamumo ir vientisumo pažeidimas ar bet kurių aukščiau nurodytų pažeidimų derinys.

7. Pažeidimas, galintis kelti pavojų asmens teisėms ir laisvėms, yra toks, dėl kurio, laiku nesiėmus tinkamų priemonių, fiziniai asmenys gali patirti kūno sužalojimą, materialinę ar nematerialinę žalą (pvz., asmuo gali patirti teisių apribojimą, diskriminaciją, gali būti pavogta ar suklastota jo asmens tapatybė, jam padaryta finansinių nuostolių, pakenkta jo reputacijai, prarastas duomenų, kurie laikomi profesine paslaptimi, konfidencialumas ir kt.).

8. Aprašu siekiama užtikrinti, kad Darbuotojai sugebėtų laiku nustatyti galimus asmens duomenų saugumo pažeidimus ir suprastų, kokie veiksmai privalo būti atlikti valdant juos (reagavimo į duomenų saugumo pažeidimus procedūros schema pateikiama Aprašo 1 priede).

9. Nustačius arba įtariant, kad įvyko Pažeidimas, atitinkantis bet kurį iš Aprašo 6 punkto reikalavimų, Pažeidimą nustatęs asmuo esant galimybei pirmiausia imasi priemonių, kad Pažeidimas būtų kuo skubiau apribotas (sustabdytas, nutrauktas, pašalintas). Jeigu Pažeidimo sustabdyti Darbuotojas pats nėra pajėgus, Darbuotojas nedelsiant informuoja duomenis tvarkančio padalinio vadovą. Konkretūs veiksmai Pažeidimui apriboti atliekami įvertinus konkretaus Pažeidimo aplinkybes, mastą, specifiką ir pan. Siekiant Pažeidimą apriboti gali būti imamasi šių pavyzdinių priemonių:

9.1. duomenų ištrynimas nuotoliniu būdu iš pamesto, pavogto ar kitaip prarasto įrenginio;

9.2. duomenų užšifravimas nuotoliniu būdu pamestame, pavogtame ar kitaip prarastame įrenginyje;

9.3. skubus kreipimasis į asmenį, kuriam per klaidą buvo išsiųsti ar kitaip atskleisti duomenys, su prašymu neatidaryti atsiųstų duomenų ir juos ištrinti be galimybės atkurti;

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

9.5. prarastų duomenų atkūrimas iš turimos atsarginės kopijos.

10. Šiame etape būtina imtis atsargumo priemonių siekiant užtikrinti, kad būtų surinkti kiek įmanoma tikslesni duomenys bei įrodymai apie įvykusį Pažeidimą (pavyzdžiui,

užfiksuojama, kas, kada ir iš kokio įrenginio jungėsi prie duomenų bazės ar informacinės sistemos, kam konkrečiai buvo per klaidą išsiųsti asmens duomenys, kokiomis aplinkybėmis buvo prarastas įrenginys su duomenimis ir kt.).

11. Veiksmai, skirti ištaisyti arba sumažinti žalą duomenų subjektui, sukeltą Pažeidimo, turėtų būti nukreipti ne vien į esamo Pažeidimo priežasties pašalinimą, bet ir siekiant neleisti Pažeidimui pasikartoti ateityje. Turėtų būti nustatytos bent vykdomų procesų, naudojamų sistemų pažeidimo priežastys, dėl kurių ir toliau gali įvykti Pažeidimų arba kurios savaime sudaro prielaidas Pažeidimui įvykti.

III SKYRIUS
PRANEŠIMAS APIE GALIMĄ ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ

12. Darbuotojas, nustatęs arba kitaip sužinojęs apie galimą Pažeidimą, atitinkantį Aprašo 6 punkte nurodytus atvejus, nedelsdamas, bet ne vėliau kaip per 2 darbo valandas nuo Pažeidimo paaiškėjimo momento, informuoja žodžiu (tiesiogiai ar telefonu) savo tiesioginį vadovą ir (arba) Bendrovės duomenų apsaugos pareigūną (toliau – pareigūnas).

13. Darbuotojas arba jo tiesioginis vadovas užpildo pranešimą apie asmens duomenų saugumo pažeidimą (forma – Aprašo 2 priedas) ir nedelsdamas perduoda jį pareigūnui.

14. Bendrovės duomenų tvarkytojas, nustatęs galimą Pažeidimą, nedelsdamas, bet ne vėliau kaip per 24 valandas nuo Pažeidimo paaiškėjimo momento, apie tai praneša Bendrovei, pateikdamas užpildytą pranešimą apie asmens duomenų saugumo pažeidimą (Aprašo 2 priedas). Duomenų tvarkytojas pateikia visą Bendrovės prašomą informaciją, susijusią su saugumo pažeidimu ir jo tyrimu

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

IV SKYRIUS
ASMENS DUOMENŲ SAUGUMO PAŽEIDIMO TYRIMAS IR PAŠALINIMAS

16. Pareigūnas, gavęs Darbuotojo ar duomenų tvarkytojo pateiktą pranešimą apie Pažeidimą:

16.1. nedelsdamas nagrinėja pranešime nurodytas aplinkybes;

16.2. jei saugumo pažeidimas yra susijęs su elektroninės informacijos saugos incidentu, pasitelkia Bendrovės ar duomenų tvarkytojo informacinių technologijų specialistus, informacinių sistemų saugos įgaliotinį;

16.3. įvertina, ar padarytas asmens duomenų saugumo pažeidimas;

16.4. jei Pažeidimas padarytas, nustato pažeidimo pobūdį, priežastis, asmens duomenų kategorijas, jų pobūdį ir kiekį, duomenų subjektų kategorijas ir jų kiekį, įvertina padarytą žalą fiziniams asmenims bei tikėtinas pažeidimo pasekmes;

16.5. įvertina, kokių skubių ir tinkamų priemonių būtina imtis, kad būtų pašalintas saugumo pažeidimas;

16.6. nustato, ar apie Pažeidimą būtina pranešti priežiūros institucijai;

16.7. nustato, ar apie Pažeidimą būtina pranešti duomenų subjektams.

17. Pareigūnas papildomai įvertina Pažeidimo keliamos rizikos duomenų subjektų teisėms ir laisvėms lygį. Vertinant rizikos lygį atsižvelgiama į konkrečias Pažeidimo aplinkybes, pavojaus duomenų subjektų teisėms ir laisvėms atsiradimo tikimybę ir rimtumą. Rizikos lygis vertinamas atsižvelgiant į šiuos kriterijus:

17.1. saugumo pažeidimo pobūdis (konfidencialumo, vientisumo ar prieinamumo pažeidimas) – nustatomas saugumo pažeidimo pobūdis: nuo padaryto pažeidimo pobūdžio gali priklausyti pavojaus duomenų subjektams dydis;

17.2. asmens duomenų, pobūdis, jautrumas ir kiekis – nustatomas asmens duomenų, kurių saugumas buvo pažeistas, pobūdis, jautrumas ir jų kiekis: kuo jautresni asmens duomenys ir kuo didesnis jų kiekis, tuo didesnis žalos pavojus;

17.3. galimybė identifikuoti fizinį asmenį – įvertinama, ar neįgaliotiems asmenims, kuriems tapo prieinami asmens duomenys, bus lengva nustatyti konkrečių asmenų tapatybę arba susieti tuos duomenis su kita informacija (pvz., tinkamai užšifruoti asmens duomenys nebus suprantami neįgaliotiems asmenims, todėl pažeidimas padarys mažesnį poveikį duomenų subjektams);

17.4. fizinio asmens specifiniai ypatumai – nustatomi fizinių asmenų, kurių asmens duomenims kilo pavojus, specifiniai ypatumai: kuo asmenys yra labiau pažeidžiami (pvz., vaikai, negalią turintys asmenys), tuo didesnį poveikį pažeidimas gali jiems padaryti;

17.5. nukentėjusių duomenų subjektų skaičius – nustatomas nukentėjusių asmenų skaičius: kuo daugiau yra asmenų, kuriems pažeidimas turi poveikio, tuo didesnis žalos pavojus;

17.6. pasekmės, sukeltos fiziniams asmenims – įvertinamos visos galimos pažeidimo pasekmės bei jų rimtumas; taip pat atsižvelgiama į pasekmių ilgalaikiškumą: jei pažeidimo pasekmės yra ilgalaikės, tai poveikis fiziniams asmenims bus didesnis.

18. Įvertinus riziką nustatomas vienas iš trijų rizikos tikimybių lygių – maža, vidutinė ar didelė rizikos tikimybė.

19. Pareigūnas, atlikęs Pažeidimo tyrimą, užpildo šio Aprašo 3 priede nurodytos formos Asmens duomenų saugumo pažeidimo tyrimo ataskaitą (toliau – Ataskaita).

20. Ataskaita yra pateikiama Bendrovės direktoriui ir duomenų tvarkytojo vadovui, jei tai susiję su duomenų tvarkytojo atliekamais asmens duomenų tvarkymo veiksmais.

21. Atsižvelgdamas į Ataskaitą, Bendrovės direktorius, jei reikia, tvirtina priemonių planą, kuriame numatomas būtinų techninių, organizacinių, administracinių ir kitų priemonių poreikis dėl saugumo pažeidimo pašalinimo, paskiria atsakingus vykdytojus ir nustato priemonių įgyvendinimo terminus.

22. Priemonių plane turi būti numatyti veiksmai, skirti ne vien esamo Pažeidimo priežasčiai pašalinti, pavojui fizinių asmenų teisėms ir laisvėms sumažinti ar pašalinti, bet taip pat skirti neleisti pasikartoti Pažeidimui. Būtina atsižvelgti į trūkumus ir duomenų tvarkymo silpnąsias vietas, kurios buvo išnaudotos įvykdant Pažeidimą, ir imtis priemonių tiems trūkumams pašalinti.

23. Visa gauta, renkama informacija fiksuojama tokiu būdu, kad atliekant vėlesnę peržiūrą būtų galima nustatyti aiškią chronologinę veiksmų seką ir situacijos eigą bei priemones, kurių buvo imtasi.

24. Bendrovė registruoja visus asmens duomenų saugumo pažeidimus: tiek nustatytus, tiek nenustatytus. Asmens duomenų saugumo pažeidimai registruojami Asmens duomenų saugumo pažeidimų registracijos žurnale (4 priedas).

25. Bendrovėje Asmens duomenų saugumo pažeidimų registracijos žurnalas yra tvarkomas elektroniniu būdu.

26. Už Asmens duomenų saugumo pažeidimų registravimo žurnalo tvarkymą ir saugojimą atsakingas duomenų apsaugos pareigūnas.

V SKYRIUS
PRANEŠIMAS APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ PRIEŽIŪROS INSTITUCIJAI

27. Pažeidimo tyrimo metu nustačius, kad asmens duomenų saugumo pažeidimas įvyko, pareigūnas, jeigu įmanoma, ne vėliau kaip per 72 valandas nuo tada, kai tapo žinoma apie pažeidimą, apie tai informuoja priežiūros instituciją, išskyrus atvejus, kai saugumo pažeidimas nekelia pavojaus fizinių asmenų teisėms ir laisvėms.

28. Priežiūros institucija informuojama Pranešimo apie asmens duomenų saugumo pažeidimą pateikimo Valstybinei duomenų apsaugos inspekcijai tvarkos aprašo, patvirtinto VDAI direktoriaus 2018 m. liepos 27 d. įsakymu Nr. 1T-72(1.12.E) „Dėl Pranešimo apie asmens duomenų saugumo pažeidimą pateikimo Valstybinei duomenų apsaugos inspekcijai tvarkos aprašo patvirtinimo“ (su visais aktualiais pakeitimais), nustatyta tvarka ir sąlygomis, užpildant Pranešimo apie asmens duomenų saugumo pažeidimo formą, patvirtintą Valstybinės duomenų apsaugos inspekcijos direktoriaus 2018 m. rugpjūčio 29 d. įsakymu Nr. 1T-82(1.12.E) „Dėl Pranešimo apie asmens duomenų saugumo pažeidimą rekomenduojamos formos patvirtinimo“.

29. Jeigu priežiūros institucijai apie Pažeidimą nepranešama per 72 valandas nuo tada, kai tapo žinoma apie Pažeidimą, prie pranešimo turi būti pridedamos vėlavimo priežastys.

30. Jeigu įvertinus riziką abejojama, ar Pažeidimas kelia pavojų fizinių asmenų teisėms ir laisvėms, pareigūnas kartu su Bendrovės direktoriumi sprendžia, ar apie pažeidimą turėtų būti pranešta priežiūros institucijai.

31. Jeigu įvertinus riziką nustatoma, kad tuo metu apie saugumo pažeidimą priežiūros institucijai pranešti nereikia, bet po kurio laiko situacija gali pasikeisti, tada saugumo 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. Jeigu yra atsarginės duomenų kopijos ir nėra pavojaus šifro saugumui, apie tokį saugumo pažeidimą pranešti priežiūros institucijai nereikia, tačiau jei vėliau paaiškėja, kad gali kilti pavojus šifro saugumui, pažeidimo keliamas pavojus bus vertinamas iš naujo ir apie tokį pažeidimą reikės pranešti priežiūros institucijai).

32. Jeigu visos informacijos priežiūros institucijai neįmanoma pateikti vienu metu arba toliau aiškinamasi Pažeidimo priežastis, informacija, nepažeidžiant Aprašo 27 punkte nustatyto termino, gali būti teikiama etapais. Apie tai, kad informacija bus teikiama etapais, priežiūros institucija informuojama pirminiame pranešime.

33. Jeigu po pranešimo priežiūros institucijai pateikimo, atlikus tolesnį tyrimą, yra nustatoma, kad saugumo incidentas buvo sustabdytas ir faktiškai asmens duomenų saugumo pažeidimo nebuvo, apie tai nedelsiant informuojama priežiūros institucija.

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

VI SKYRIUS
PRANEŠIMAS APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ DUOMENŲ SUBJEKTUI

35. Tyrimo metu nustačius, kad dėl asmens duomenų saugumo pažeidimo gali kilti didelis pavojus fizinių asmenų teisėms ir laisvėms, Bendrovė, jeigu įmanoma, nepraėjus daugiau kaip 72 valandoms nuo to laiko, kai buvo sužinota apie Pažeidimą, praneša apie tai ir duomenų subjektams, kurių teisėms ir laisvėms gali kilti didelis pavojus.

36. Didelį pavojų keliančiu gali būti laikomas bet kuris 7 punkte nurodytų pasekmių riziką keliantis Pažeidimas tada, jei tokios Pažeidimo pasekmės yra labai tikėtinos, tvarkomi jautrūs asmens duomenys (pavyzdžiui, duomenys apie sveikatą), Pažeidimas turi neigiamą poveikį dideliam duomenų subjektų skaičiui ir pan.

37. Pagrindinis pranešimo duomenų subjektui tikslas – pateikti konkrečią informaciją apie tai, kokių veiksmų jis turėtų imtis, kad apsisaugotų nuo neigiamų Pažeidimo pasekmių. Duomenų subjektas informuojamas siunčiant jam pranešimą paštu, elektroniniu paštu, telefonu, trumpąja žinute (SMS) ar kitu būdu. Pranešimas duomenų subjektui siunčiamas atskirai nuo kitos siunčiamos informacijos kaip naujienlaiškiai ar standartiniai pranešimai ir jame turi būti aiškiai, suprantama, paprasta kalba pateikia bent ši informacija:

37.1. Pažeidimo aprašymas;

37.2. tikėtinų Pažeidimo pasekmių duomenų subjektui aprašymas;

37.3. priemonės, kurių ėmėsi arba planuoja imtis Bendrovė tam, kad būtų pašalintas Pažeidimas, įskaitant, kai tinkama, priemonės galimoms neigiamoms jo pasekmėms sumažinti;

37.4. kontaktinio asmens, galinčio suteikti daugiau informacijos, vardas, pavardė ir kontaktiniai duomenys arba pareigūno kontaktai;

37.5. kita reikšminga informacija, susijusi su Pažeidimu, kuri gali būti reikšminga duomenų subjektui.

38. Pranešimo pateikti duomenų subjektui neprivaloma, jei egzistuoja bet kuri iš šių aplinkybių:

38.1. Bendrovė įgyvendino tinkamas technines ir organizacines apsaugos priemones ir tos priemonės taikytos asmens duomenims, kuriems Pažeidimas turėjo poveikį, visų pirma, tas priemones, kuriomis užtikrinama, kad asmeniui, neturinčiam leidimo susipažinti su asmens duomenimis, jie būtų nesuprantami, pavyzdžiui, šifravimo priemonės;

38.2. Bendrovė įvykus Pažeidimui ėmėsi priemonių, kuriomis užtikrinama, kad nekiltų didelis pavojus duomenų subjektų teisėms ir laisvėms;

38.3. 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 Bendrovės 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 nėra efektyvi informavimo priemonė);

38.4. tam tikromis aplinkybėmis, kai tai yra pagrįsta, Bendrovė pasitarusi su teisėsaugos institucijomis ir atsižvelgdama į teisėtus teisėsaugos interesus, gali atidėti asmenų, kuriems Pažeidimas turi poveikio, informavimą apie Pažeidimą iki to laiko, kai tai netrukdys teisėsaugos institucijų tyrimams atlikti.

39. Jeigu įvertinus riziką nustatoma, kad tuo metu apie saugumo pažeidimą duomenų subjektų 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 – jei atlikus tyrimą, paaiškėja, kad vienintelė išpirkos reikalaujančios programos užduotis buvo užšifruoti asmens duomenis ir jokio kito kenksmingo poveikio duomenų bazei nėra, apie saugumo pažeidimą reikės pranešti tik priežiūros institucijai, tačiau jei vėliau paaiškėja, kad prarastas ne tik duomenų prieinamumas, bet ir konfidencialumas, saugumo pažeidimo keliamas pavojus bus vertinamas iš naujo bei sprendžiama, ar atsižvelgiant į tikėtinas saugumo pažeidimo pasekmes reikia apie jį pranešti duomenų subjektams).

40. Gavusi priežiūros institucijos reikalavimą informuoti duomenų subjektus apie Pažeidimą, Bendrovė nedelsdama jį vykdo.

VII SKYRIUS
BAIGIAMOSIOS NUOSTATOS

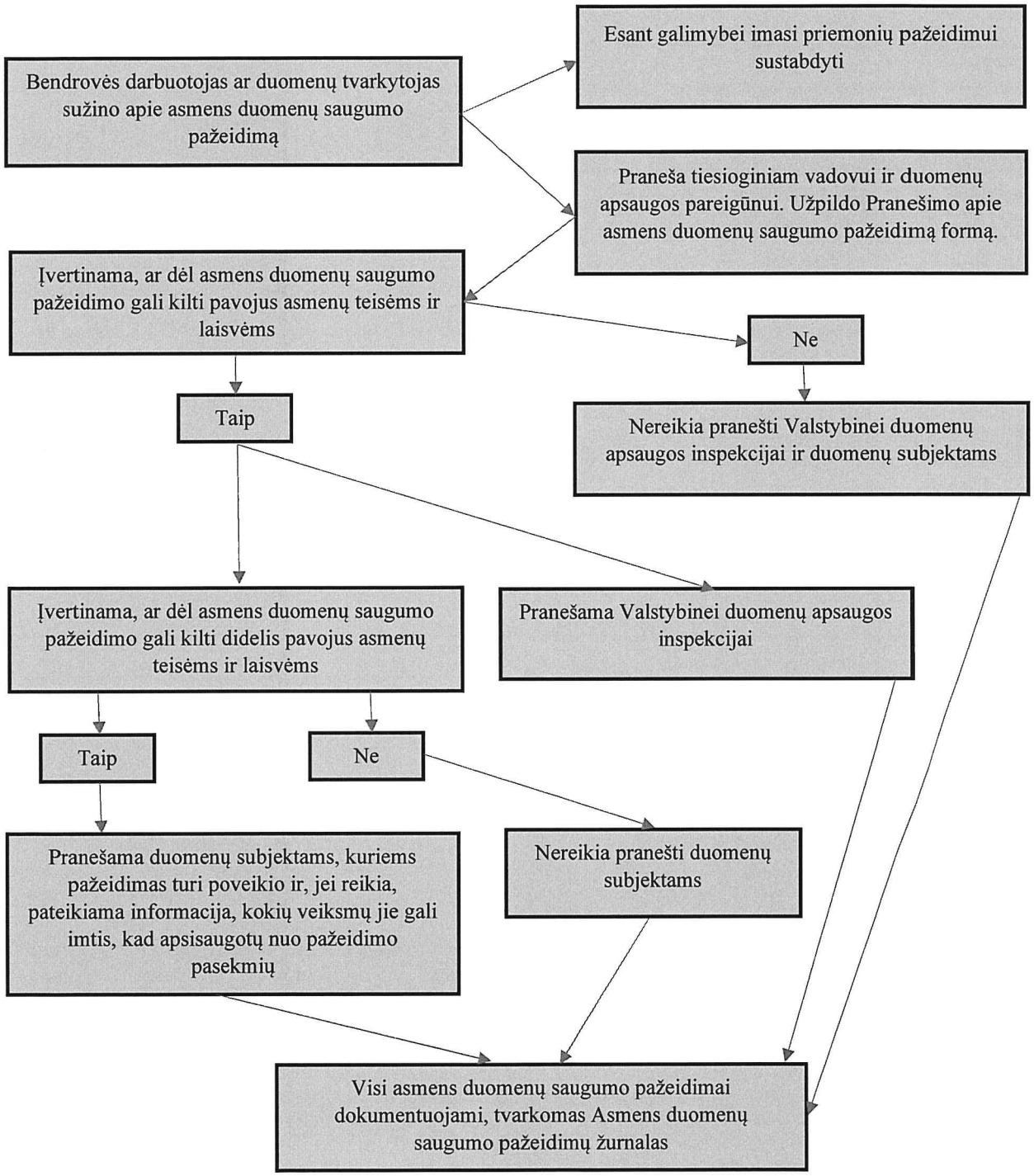
41. Visi Darbuotojai privalo būti supažindinti ir vadovautis Aprašu Pažeidimo atveju.

42. Asmenys, nesilaikantys arba pažeidę Aprašo reikalavimus, dėl kurių Bendrovė neįgyvendino arba netinkamai įgyvendino BDAR reikalavimus, atsako teisės aktų nustatyta tvarka.

_____

Asmens duomenų saugumo pažeidimų
valdymo tvarkos aprašo
1 priedas

REAGAVIMO Į DUOMENŲ SAUGUMO PAŽEIDIMUS PROCEDŪROS SCHEMA



Asmens duomenų saugumo pažeidimų
valdymo tvarkos aprašo
2 priedas

(Pranešimo apie asmens duomenų saugumo pažeidimą forma)

_____
(juridinio asmens pavadinimas)

_____
(struktūrinio padalinio pavadinimas)

_____
(pareigų pavadinimas)

_____
(vardas, pavardė)

PRANEŠIMAS APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ

_____ Nr. _____
(data)

Klaipėda

Informuoju apie asmens duomenų saugumo pažeidimą, pateikdamas turimą informaciją:

1. Asmens duomenų saugumo pažeidimo nustatymo data, laikas ir vieta:

_____
_____
_____

2. Asmens duomenų saugumo pažeidimo padarymo data, laikas ir vieta:

_____
_____
_____

3. Asmens duomenų saugumo pažeidimo esmė ir aplinkybės:

_____
_____
_____
_____
_____
_____
_____
_____

4. Duomenų subjektų, kurių asmens duomenų saugumas pažeistas, kategorijos (pvz., Bendrovės darbuotojai, asmenys, pateikę prašymus, skundus, asmenys, kuriems teikiamos viešosios ar administracinės paslaugos ir kt.) ir apytikslis jų skaičius:

_____
_____
_____
_____
_____

5. Asmens duomenų, kurių saugumas pažeistas, kategorijos (pažymėti tinkamą (-us) atsakymą (-us):

☐ Asmens tapatybę patvirtinantys duomenys (vardas, pavardė, gimimo data, lytis ir kt.)

☐ Asmens identifikaciniai ar prisijungimo duomenys (asmens kodas, mokėtojo kodas, slaptažodžiai ir kt.)

☐ Asmens kontaktiniai duomenys (gyvenamosios vietos adresas, telefono numeris, elektroninio pašto adresas ir kt.)

☐ Specialių kategorijų asmens duomenys (duomenys, susiję su asmens sveikata, genetiniai duomenys, biometriniai duomenys, duomenys, susiję su asmens rasine ar etnine kilme, duomenys, susiję su asmens politinėmis pažiūromis, religiniais, filosofiniais įsitikinimais ar naryste profesinėse sąjungose, duomenys, susiję su asmens lytiniu gyvenimu ir lytine orientacija ir kt.)

☐ Duomenys apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas

☐ Kiti asmens duomenys (įrašyti):

_____

_____

_____

_____

_____

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

_____

_____

7. Veiksmai (priemonės), kurių buvo imtasi sužinojus apie padarytą asmens duomenų saugumo pažeidimą (pvz., pakeisti prisijungimo prie informacinės sistemos slaptažodžiai, panaudotos atsarginės kopijos, siekiant atkurti prarastus ar sugadintus duomenis, atnaujinta programinė įranga, surinkti ne saugojimo vietoje palikti dokumentai su asmens duomenimis ir kt.):

_____

_____

_____

_____

_____

_____	_____	_____
(pareigos)	(parašas)	(vardas ir pavardė)

Asmens duomenų saugumo pažeidimų
valdymo tvarkos aprašo
3 priedas

(Asmens duomenų saugumo pažeidimo tyrimo ataskaitos forma)

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMO TYRIMO ATASKAITA

_____ Nr. _____
(data)

1. Asmens duomenų saugumo pažeidimo aprašymas

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) atsakymą (-us):

☐ Informacinė sistema

☐ Duomenų bazė

☐ Tarnybinė stotis

☐ Interneto svetainė

☐ Debesų kompiuterijos paslaugos

☐ Nešiojamieji ar mobilieji įrenginiai

☐ Neautomatiniu būdu susistemintos bylos (archyvas)

☐ Kita (įrašyti):

_____

_____

_____

1.3. Asmens duomenų saugumo pažeidimo pobūdis (pažymėti tinkamą (-us) atsakymą (-us):

☐ Konfidencialumo pažeidimas (neautorizuota prieiga ar atskleidimas)

☐ Vientisumo pažeidimas (neautorizuotas asmens duomenų pakeitimas)

☐ Prieinamumo pažeidimas (asmens duomenų praradimas, sunaikinimas)

1.4. Asmens duomenų, kurių saugumas pažeistas, kategorijos (pažymėti tinkamą (-us) atsakymą (-us) ir aprašyti):

☐ Asmens tapatybę patvirtinantys duomenys (vardas, pavardė, gimimo data, lytis ir kt.):

_____

_____

_____

☐ Asmens identifikaciniai ar prisijungimo duomenys (asmens kodas, mokėtojo kodas, slaptažodžiai ir kt.):

_____

_____

_____

☐ Asmens kontaktiniai duomenys (gyvenamosios vietos adresas, telefono numeris, elektroninio pašto adresas ir kt.):

☐ Specialių kategorijų asmens duomenys (duomenys, susiję su asmens sveikata, genetiniai duomenys, biometriniai duomenys, duomenys, susiję su asmens rasine ar etnine kilme, duomenys, susiję su asmens politinėmis pažiūromis, religiniais, filosofiniais įsitikinimais ar naryste profesinėse sąjungose, duomenys, susiję su asmens lytiniu gyvenimu ir lytine orientacija ir kt.):

☐ Duomenys apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas:

☐ Kiti asmens duomenys:

1.5. Apytikslis asmens duomenų, kurių saugumas pažeistas, skaičius: ☐

1.6. Duomenų subjektų, kurių asmens duomenų saugumas pažeistas, kategorijos (Bendrovės darbuotojai, asmenys, pateikę prašymus, skundus, asmenys, kuriems teikiamos viešosios ar administracinės paslaugos ir kt.):

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

1.8. Darbuotojas, pranešęs apie asmens duomenų saugumo pažeidimą (vardas, pavardė, Bendrovės struktūrinio padalinio, kuriame dirba darbuotojas, pavadinimas, telefono numeris, elektroninio pašto adresas):

1.9. Duomenų tvarkytojas, pranešęs apie asmens duomenų saugumo pažeidimą (pavadinimas, kontaktinio asmens duomenys (vardas, pavardė, telefono numeris, elektroninio pašto adresas):

2. Asmens duomenų saugumo pažeidimo keliamos rizikos duomenų subjektų teisėms ir laisvėms įvertinimas

2.1. Specifiniai fizinių asmenų, kurių asmens duomenų saugumas buvo pažeistas, ypatumai (vaikai, asmenys su negalia ir kt.):

2.2. Galimybė identifikuoti fizinį asmenį (pvz., iki asmens duomenų saugumo pažeidimo asmens duomenys buvo tinkamai užšifruoti, anonimizuoti arba iki saugumo pažeidimo asmens duomenims šifravimas nebuvo taikomas ir kt.):

2.3. Kas gavo prieigą prie asmens duomenų, kurių saugumas pažeistas?

2.4. Ar buvo kokių kitų įvykių ar aplinkybių, turėjusių poveikį asmens duomenų saugumo pažeidimui padaryti?

2.5. Kokia galima žala padaryta fiziniams asmenims (duomenų subjektams)?

2.6. Galimos asmens duomenų saugumo pažeidimo pasekmės:

2.6.1. Konfidencialumo pažeidimo atveju (pažymėti tinkamą (-us) atsakymą (-us):

☐ Asmens duomenų išplitimas ir duomenų subjekto kontrolės praradimas savo asmens duomenų atžvilgiu (pvz., asmens duomenys išplito internete)

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

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

☐ Kita:

2.6.2. Vientisumo pažeidimo atveju (pažymėti tinkamą (-us) atsakymą (-us):

☐ Pakeitimas į neteisingus duomenis, dėl ko asmuo gali netekti galimybės naudotis paslaugomis

☐ Pakeitimas į kitus duomenis, kad asmens duomenų tvarkymas būtų nukreiptas tam tikra linkme (pvz., pavogta asmens tapatybė susiejant vieno asmens identifikuojančius duomenis su kito asmens biometriniais duomenimis)

☐ Kita:

2.6.3. Prieinamumo pažeidimo atveju (pažymėti tinkamą (-us) atsakymą (-us):

☐ Dėl asmens duomenų trūkumo negalima teikti paslaugų (pvz., administracinių procesų sutrikdymas, dėl ko negalima prieiti prie tvarkomų asmens duomenų ir įgyvendinti duomenų subjekto teisę susipažinti su jo tvarkomais asmens duomenimis)

☐ Dėl klaidų asmens duomenų tvarkymo procesuose negalima teikti tinkamos paslaugos (pvz., tam tikra informacija iš informacinės sistemos išnyko, dėl ko negalima tinkamai suteikti administracinės paslaugos)

☐ Kita:

2.7. Asmens duomenų saugumo pažeidimo sukeltos rizikos duomenų subjektų teisėms ir laisvėms lygis:

☐ Žema rizikos tikimybė (dėl asmens duomenų saugumo pažeidimo nėra pavojaus fizinių asmenų teisėms ir laisvėms)

☐ Vidutinė rizikos tikimybė (dėl asmens duomenų saugumo pažeidimo yra ar gali kilti pavojus fizinių asmenų teisėms ir laisvėms)

☐ Didelė rizikos tikimybė (dėl asmens duomenų saugumo pažeidimo yra ar gali kilti didelis pavojus fizinių asmenų teisėms ir laisvėms)

2.8. Kokių veiksmų ar priemonių buvo imtasi sužinojus apie padarytą asmens duomenų saugumo pažeidimą?

2.9. Kokios taikytos priemonės, siekiant sumažinti neigiamą poveikį duomenų subjektams?

2.10. Kokios techninės priemonės buvo taikomos asmens duomenų saugumo pažeidimo paveiktiems asmens duomenims, užtikrinant, kad asmens duomenys nebūtų prieinami neįgaliotiems asmenims?

2.11. Techninės ir (ar) organizacinės saugumo priemonės, kurios įgyvendintos dėl asmens duomenų saugumo pažeidimo, taip pat siekiant, kad pažeidimas nepasikartotų:

2.12. Techninės ir (ar) organizacinės saugumo priemonės, kurios ketinamos įgyvendinti dėl asmens duomenų saugumo pažeidimo, įskaitant ir priemones sumažinti asmens duomenų saugumo pažeidimo pasekmes:

3. Pranešimų apie asmens duomenų saugumo pažeidimą pateikimas

3.1. Ar pranešta Valstybinei duomenų apsaugos inspekcijai (toliau – VDAI) apie asmens duomenų saugumo pažeidimą?

☐ Taip

☐ Ne (nurodomos nepranešimo VDAI priežastys):

_____

_____

_____

☐ Apie duomenų saugumo pažeidimą pranešta VDAI vėliau nei per 72 valandas (nurodomos vėlavimo pranešti VDAI priežastys):

_____

_____

_____

3.2. Ar pranešta duomenų subjektui apie asmens duomenų saugumo pažeidimą?

☐ Taip

Informuotų duomenų subjektų skaičius ☐

Pranešimo duomenų subjektui būdas (pažymėti tinkamą (-us): ☐ paštu ☐ elektroniniu paštu ☐ trumpąja žinute (SMS) ☐ kitais būdais

Pranešimo duomenų subjektui turinys:

_____

_____

_____

_____

☐ Ne (nurodomos nepranešimo duomenų subjektui priežastys):

_____

_____

_____

☐ Apie saugumo pažeidimą pranešta viešai (nurodoma kada ir kur paskelbta informacija viešai arba jei taikyta kita priemonė, nurodoma kokia ir kada taikyta):

_____

_____

_____

3.3. Ar pranešta valstybės institucijoms, įgaliotoms atlikti ikiteisminį tyrimą, apie asmens duomenų saugumo pažeidimą, galimai turintį nusikalstamos veikos požymių (jeigu taip, nurodoma rašto data ir numeris):

_____

_____

_____	_____	_____
(pareigos)	(parašas)	(vardas ir pavardė)

Asmens duomenų saugumo pažeidimų
valdymo tvarkos aprašo
4 priedas

(Asmens duomenų saugumo pažeidimų žurnalo forma)

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ ŽURNALAS

Eil. Nr.	Pažeidimo nustatymo data, valanda (minučių tikslumu) ir vieta	Darbuotojas ar kitas subjektas, pranešęs apie pažeidimą (vardas, pavardė, pareigos)	Pažeidimo padarymo data ir vieta	Pažeidimo pradžia ir pabaiga, pobūdis, tipas, aplinkybės	Duomenų subjektų, kurių asmens duomenų saugumas pažeistas, kategorijos ir apytikslis skaičius	Asmens duomenų, kurių saugumas pažeistas, kategorijos ir apimtis	Tikėtinos pažeidimo pasekmės bei pavojus fizinių asmenų teisėms ir laisvėms	Priemonės, kurių buvo imtasi pažeidimui pašalinti ir (ar) neigiamoms pažeidimo pasekmėms sumažinti	Darbuotojas, ar kitas subjektas, pašalinęs pažeidimą (vardas, pavardė, pareigos)	Informacija, ar apie pažeidimą buvo pranešta Valstybinei duomenų apsaugos inspekcijai, ir priimto sprendimo motyvai	Informacija, ar apie pažeidimą buvo pranešta duomenų subjektui (-ams), ir priimto sprendimo motyvai
1.											
2.											
3.											
4.											
5.											
6.											
7.											
8.											
9.											
10.											