PATVIRTINTA
SĮ „Kretingos komunalininkas“ direktoriaus
2021 m. balandžio 13 d. įsakymu Nr. (1.1.) V1-17

SĮ „KRETINGOS KOMUNALININKAS“ ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ VALDYMO TAISYKLĖS

I SKYRIUS BENDROSIOS NUOSTATOS

1. Šios Taisyklės reglamentuoja asmens duomenų saugumo pažeidimų aptikimo, pašalinimo ir pranešimo apie juos SĮ „Kretingos komunalininkas“ (toliau – Įmonė) tvarką.

2. Taisyklės parengtos vadovaujantis 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) 33 ir 34 straipsniais, Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu (2018-06-30 įstatymo Nr. XIII-1426 redakcija, toliau – Įstatymas) ir kitais galiojančiais teisės aktais.

3. **Asmens duomenų saugumo pažeidimas** (toliau – Pažeidimas) – saugumo pažeidimas, dėl kurio netyčia arba neteisėtai sunaikinami, prarandami, pakeičiami, be leidimo atskleidžiami Įmonės tvarkomi asmens duomenys arba prie jų be teisinio pagrindo gaunama prieiga (BDAR 4 straipsnio 12 punktas).

4. **Atsakingas asmuo –** Įmonės vadovo įsakymu paskirtas asmuo ar struktūrinis padalinys, atsakingas už tinkamą pažeidimų valdymą (pažeidimų tyrimą, pranešimų teikimą, prevencinių priemonių įdiegimo kontrolę ir pan.).

5. **VDAI –** Valstybinė duomenų apsaugos inspekcija.

6. Kitos šiose Taisyklėse vartojamos sąvokos atitinka BDAR ir Įstatyme vartojamas sąvokas.

7. Šiose Taisyklėse nustatytų procedūrų privalo laikytis visi Įmonės darbuotojai.

8. Šios Taisyklės taikomos ir Įmonės duomenų tvarkytojams tik tais atvejais, kai tai aptarta su jais sudaromose duomenų tvarkymo sutartyse ir tiek, kiek su jais sudarytos duomenų tvarkymo sutartys ar galiojantys teisės aktai nenumato kitaip.

II SKYRIUS INFORMAVIMAS APIE GALIMĄ PAŽEIDIMĄ

9. Įmonės darbuotojas, sužinojęs ar pats nustatęs galimą Pažeidimą arba kai informacija apie galimą Pažeidimą gaunama iš duomenų tvarkytojo, žiniasklaidos ar bet kokio kito šaltinio, privalo nedelsdamas apie tai informuoti Atsakingą asmenį.

10. Pranešimas apie galimą Pažeidimą Atsakingam asmeniui pateikiamas žodžiu (tiesiogiai ar telefonu), raštu ar elektroninėmis priemonėmis.

11. Duomenų tvarkytojas, sužinojęs apie galimą Pažeidimą, privalo nedelsdamas (įprastai per 24 val.) apie tai pranešti Įmonei. Tuo atveju, jei terminas nuo momento, kai Duomenų tvarkytojui tapo žinoma apie galimą Pažeidimą iki pranešimo Įmonei yra ilgesnis nei 24 val., Duomenų tvarkytojas kartu su pranešimu pateikia Įmonei paaiškinimą dėl uždelsto informacijos pateikimo.

12. Duomenų tvarkytojas apie Pažeidimą gali pranešti tiesiogiai VDAI, jeigu tai yra aiškiai numatyta duomenų tvarkymo sutartyje su duomenų valdytoju. Tačiau bet kuriuo atveju teisinę prievolę pranešti VDAI turi ir Įmonė.

III SKYRIUS
PAŽEIDIMO TYRIMAS

13. Atsakingas asmuo, gavęs iš darbuotojo ar duomenų tvarkytojo informaciją apie galimą Pažeidimą, nedelsiant imasi šių veiksmų:

13.1. informuoja apie gautą informaciją dėl galimo pažeidimo Įmonėje paskirtą duomenų apsaugos pareigūną,

13.2. atlieka pirminį tyrimą.

14. Pirminis tyrimas atliekamas siekiant išsiaiškinti, ar Pažeidimas įvyko, kokio tipo Pažeidimas įvyko bei įvertinti su pažeidimu susijusią riziką.

15. Atsakingas asmuo privalo pirminį tyrimą atlikti per kuo trumpesnį terminą, kuris įprastai negali viršyti 72 val.

16. Galimi Pažeidimo tipai:

16.1. Konfidencialumo pažeidimas – kai tyčia ar netyčia be leidimo ar neteisėtai atskleidžiami asmens duomenys ar gaunama prieiga prie jų;

16.2. Prieinamumo pažeidimas – kai tyčia ar netyčia neteisėtai prarandama prieiga prie arba sunaikinami asmens duomenys;

16.3. Vientisumo pažeidimas – kai tyčia ar netyčia asmens duomenys be leidimo pakeičiami.

17. Pažeidimas tuo pat metu gali būti vieno ar kelių tipų, t.y., sietis su asmens duomenų konfidencialumu, prieinamumu ir vientisumu, taip pat su kuriuo nors jų deriniu.

18. Priklausomai nuo Pažeidimo tipo, atliekant pirminį tyrimą, turi būti išsaugomi esamos situacijos įrodymai bei vėliau naudojamos visos tinkamos techninės ir organizacinės priemonės.

19. Vertinant riziką dėl Pažeidimo, atsižvelgiama į konkrečias Pažeidimo aplinkybes, pavojaus duomenų subjekto teisėms ir laisvėms atsiradimo tikimybę ir rimtumą.

20. Rizika vertinama objektyviu įvertinimu ir atsižvelgiant į šiuos kriterijus:

20.1. Pažeidimo tipą;

20.2. Asmens duomenų pobūdį ir apimtis;

20.3. Kaip lengvai identifikuojamas fizinis asmuo;

20.4. Pasekmių rimtumą fiziniams asmenims;

20.5. Specialias fizinio asmens savybes;

20.6. Nukentėjusių fizinių asmenų skaičių;

20.7. Specialias Įmonės savybes.

21. Vertinant riziką, laikoma, kad Pažeidimas, galintis sukelti pavojų asmenų teisėms ir laisvėms yra tos, dėl kurio, laiku nesiėmus tinkamų priemonių, fiziniai asmenys gali patirti kūno sužalojimą, materialinę ar nematerialinę žalą.

22. Įvertinus riziką nustatoma vieno iš trijų tipų rizikos tikimybė:

22.1. Žema rizikos tikimybė;

22.2. Vidutinė rizikos tikimybė;

22.3. Didelė (aukšta) rizikos tikimybė.

23. Atlikęs šiose Taisyklėse nurodytą pirminį tyrimą, Atsakingas asmuo parengia Pažeidimo pirminio tyrimo išvadą pagal šių Taisyklių Priede Nr. 2 patvirtintą formą.

24. Pažeidimo pirminio tyrimo išvadą Atsakingas asmuo nepagrįstai nedelsdamas pateikia (raštu ar elektroninėmis priemonėmis) Įmonės vadovui, o išvados kopiją – Įmonėje paskirtam duomenų apsaugos pareigūnui. Įmonės vadovas priima sprendimą dėl tolimesnių veiksmų, susijusių su Pažeidimu.

25. Po pirminio tyrimo atlikimo Atsakingas asmuo privalo:

25.1. įvertinti, ar apie Pažeidimą būtina pranešti VDAI ar/ir duomenų subjektams ir

25.2. imtis visų tinkamų techninių ir organizacinių priemonių, kad Pažeidimas būtų išsamiai ištirtas ir pašalintas bei nepasikartotų.

26. Įmonė privalo pranešti VDAI apie visus asmens duomenų saugumo pažeidimus), išskyrus, kai tikėtina, kad toks Pažeidimas nekels pavojaus asmenų teisėms ir laisvėms.

27. Kai nustatoma, jog dėl Pažeidimo kyla didelė grėsmė fizinių asmenų teisėms ir laisvėms, Įmonė apie Pažeidimą privalo pranešti tiek VDAI, tiek duomenų subjektui.

IV SKYRIUS
PRANEŠIMAS APIE PAŽEIDIMĄ VDAI

28. Atsakingo asmens parengtoje pirminio tyrimo išvadoje nustačius, kad Pažeidimas buvo ir, kad yra rizika fizinių asmenų teisėms ir laisvėms, Atsakingas asmuo nedelsdamas, tačiau ne vėliau kaip per 72 val. nuo sužinojimo apie Pažeidimą, privalo pranešti apie tai VDAI.

29. Pranešimas apie Pažeidimą VDAI pateikiamas elektroniniu būdu arba kitomis teisės aktų nustatytomis priemonėmis.

30. Jeigu, įvertinus riziką, abejojama, ar ji yra ir ar reikia pranešti apie Pažeidimą VDAI, Atsakingam asmeniui taip pat rekomenduojama tokį pranešimą VDAI pateikti.

31. Jeigu, priklausomai nuo Pažeidimo pobūdžio, būtina atlikti išsamesnį tyrimą ir nustatyti visus svarbius faktus, susijusius su Pažeidimu ir per 72 val. nuo sužinojimo apie Pažeidimą pirminis tyrimas nėra baigiamas ir dėl objektyvių aplinkybių to padaryti neįmanoma, informaciją VDAI Atsakingas asmuo gali teikti etapais. Esant galimybei, apie informacijos teikimą etapais, VDAI turėtų būti informuota teikiant pirminį Pranešimą.

32. Jeigu po Pranešimo VDAI pateikimo, atlikus tolesnį tyrimą, yra nustatoma, kad saugumo incidentas buvo sustabdytas ir faktiškai nebuvo jokio Pažeidimo, Atsakingas asmuo apie tai nedelsiant praneša VDAI ir pažymi Žurnale.

V SKYRIUS

PRANEŠIMAS DUOMENŲ SUBJEKTUI

33. Nustačius, kad Pažeidimas buvo ir, kad yra didelė rizika fizinių asmenų teisėms ir laisvėms, Įmonė privalo nedelsiant, įprastai ne vėliau kaip per 72 valandas, apie tai pranešti duomenų subjektui, kurio teisėms ir laisvėms dėl šio Pažeidimo gali kilti didelis pavojus. Už šios Įmonės pareigos tinkamą įgyvendinimą atsako Atsakingas asmuo.

34. Tai, jog apie Pažeidimą buvo informuota VDAI, neatleidžia Įmonės, kaip duomenų valdytojo, nuo pareigos informuoti duomenų subjektą.

35. Pranešime duomenų subjektui aiškia ir paprasta kalba pateikiama:

35.1. Pažeidimo pobūdžio aprašymas;

35.2. Duomenų apsaugos pareigūno kontaktiniai duomenys;

35.3. Tikėtinų Pažeidimo pasekmių aprašymas;

35.4. Priemonių, kurių ėmėsi arba pasiūlė imtis duomenų valdytojas, kad būtų pašalintas Pažeidimas, įskaitant (kai tinkama) priemonių galimoms neigiamoms jo pasekmėms sumažinti, aprašymas;

35.5. Kita reikšminga informacija, susijusi su Pažeidimu.

36. Duomenų subjektai apie Pažeidimą informuojami tiesiogiai el. paštu, SMS, paštu ar kitais būdais. Šis pranešimas privalo būti atskirtas nuo kitos siunčiamos informacijos, tokios kaip nuolatiniai atnaujinimai ar standartiniai pranešimai.

37. Kai tiesioginio pranešimo duomenų subjektui pateikimas pareikalautų neproporcingai daug pastangų, apie įvykusį Pažeidimą gali būti paskelbiama viešai arba taikoma panaši priemonė, kuria duomenų subjektai būtų informuoti.

38. Įmonė pasirenka tokius pranešimo duomenų subjektui būdus, kurie maksimaliai didintų galimybę tinkamai pranešti informaciją visiems nukentėjusiems asmenims.

39. Įmonė gali pasirinkti kelis pranešimo duomenų subjektui apie Pažeidimą būdus.

40. Esant Pažeidimui, pranešimo duomenų subjektui teikti nereikia, jeigu:

40.1. Įmonė įgyvendino tinkamas technines ir organizacines apsaugos priemones ir tos priemonės taikytos asmens duomenims, kuriems Pažeidimas turėjo poveikio;

40.2. Iš karto po Pažeidimo Įmonė ėmėsi priemonių, kuriomis užtikrinama, kad nebegalėtų kilti didelis pavojus asmenų teisėms ir laisvėms;

40.3. Tai pareikalautų neproporcingai daug pastangų susisiekti su asmenimis. Tokiu atveju vietoj to apie Pažeidimą paskelbiama viešai arba taikoma panaši priemonė, kuria duomenų subjektai būtų informuojami taip pat efektyviai.

41. Įmonė turi galėti įrodyti VDAI, kad tinkamai vykdė pareigas informuoti duomenų subjektus arba sąlygos, kai duomenų subjektai neprivalėjo būti informuoti, iš tikrųjų egzistavo.

42. Jeigu tiriant Pažeidimą pradžioje nustatoma, kad nėra pavojaus fizinių asmenų teisėms ir laisvėms, tačiau detalesnio Pažeidimo tyrimo metu nustatoma, kad toks pavojus gali kilti, Įmonė riziką turi įvertinti iš naujo.

VI SKYRIUS
PAŽEIDIMŲ DOKUMENTAVIMAS

43. Visi Pažeidimai, nepriklausomai nuo to, ar apie juos buvo pranešta VDAI, ar ne, registruojami Asmens duomenų saugumo pažeidimų žurnale (toliau – Žurnalas). Rekomenduojama Žurnalą pildyti pagal šių Taisyklių Priede Nr. 1 patvirtintą formą. Žurnalas gali būti pildomas ir nesilaikant šios formos, tačiau bet kokiu atveju Žurnale privalo būti užfiksuota informacija, nurodyta formoje, įtvirtintoje šių Taisyklių Priede Nr. 1.

44. Informacija apie Pažeidimą į Žurnalą įvedama nedelsiant, kai tik atliekamas pirminis vertinimas (įprastai - ne vėliau kaip per 5 darbo dienas po pirminio vertinimo išvados surašymo). Esant būtinybei, Žurnale esanti informacija papildoma ir (ar) koreguojama.

45. Žurnale nurodoma:

45.1. Visi su Pažeidimu susiję faktai – Pažeidimo priežastis, kas įvyko ir kokie asmens duomenys pažeisti;

45.2. Pažeidimo poveikis ir pasekmės;

45.3. Techninės priemonės, kurių buvo imtasi;

45.4. Priežastys dėl su Pažeidimu susijusių sprendimų priėmimo;

45.5. Pranešimo VDAI pateikimo vėlavimo priežastys (jeigu Pranešimą vėluojama pateikti ar Pranešimas teikiamas etapais);

45.6. Informacija, susijusi su pranešimu duomenų subjektui;

45.7. Kita reikšminga informacija, susijusi su Pažeidimu.

46. Žurnalas tvarkomas raštu, įskaitant elektroninę formą, ir saugomas pagal Įmonės patvirtintą dokumentų saugojimo tvarką.

47. Įmonės paskirtas asmuo, atsakingas už Pažeidimų valdymą, laikomas atsakingu ir už Žurnalo pildymą.

48. Remdamasi Žurnale pateikta informacija, VDAI turi galėti patikrinti, kaip įgyvendinama Įmonės, kaip duomenų valdytojo, prievolė pranešti apie Pažeidimus.

49. Žurnale esantys įrašai esant reikalui peržiūrimi ir numatoma, kokios prevencijos priemonės turėtų būti įgyvendintos bei kaip bus kontroliuojamas šių prevencijos priemonių įdiegimas, kad ateityje analogiški Pažeidimai nesikartotų.

VII SKYRIUS
BAIGIAMOSIOS NUOSTATOS

50. Įmonė reguliariai, ne rečiau kaip kartą per 2 metus, atlieka pažeidimų analizę ir vertina, kokių reikėtų imtis Pažeidimų prevencijos priemonių.

Priedas Nr. 1

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ ŽURNALAS

Įrašo Nr.	

PRANEŠIMO APIE GALIMĄ PAŽEIDIMĄ GAVIMAS

Pranešimo apie galimą pažeidimą data		Asmuo, pranešęs apie galimą pažeidimą	
Pranešimo apie pažeidimą gavimo aplinkybės ir turinys			

PIRMINIS TYRIMAS

Pirminio tyrimo išvados data		Pirminio tyrimo metu naudotos techninės priemonės	
Pirminio tyrimo išvados santrauka	*(ar pažeidimas buvo, kokio tipo, kokia rizika)*		

PRANEŠIMAI VDAI IR DUOMENŲ SUBJEKTAMS APIE PAŽEIDIMĄ

Pranešimas VDAI	*Teiktas/neteiktas, jei teiktas – kada, jei neteiktas at teikiamas etapais – dėl kokių priežasčių*

Pranešimai duomenų subjektams	*Teiktas/neteiktas, jei teiktas – kada ir kokiais būdais, jei neteiktas at teikiamas etapais – dėl kokių priežasčių*

PAŽEIDIMO PASEKMĖS

Pažeidimo poveikis ir pasekmės	
Pažeidimo priežastis	
Taisomieji veiksmai	
Kita reikšminga informacija	

ĮRAŠO KOREKCIJOS

Data:	Korekcijų turinys:	
	Atsakingas asmuo:	

/Vardas, pavardė, parašas, data/

Priedas Nr. 2

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ PIRMINIO TYRIMO IŠVADA

Išvados data:		Pirminį tyrimą atliko:	
Pranešimo apie galimą pažeidimą data:		Asmuo, pranešęs apie galimą pažeidimą:	
Pranešimo apie pažeidimą gavimo aplinkybės ir turinys			
Pirminio tyrimo metu naudotos techninės priemonės:			

Išvados rezultatai:

Pažeidimo faktas:	/įvertinti pažeidimas iš tiktųjų įvyko/neįvyko (gal buvo tik saugumo incidentas), ir pagrįsti, dėl ko taip manoma/
Pažeidimo tipas:	/Konfidencialumo, prieinamumo, vientisumo – ar šių tipų derinys/
Rizikos vertinimo aprašymas:	/Aprašoma, kaip buvo vertinama rizika, atsižvelgiant į pažeidimo tipą, asmens duomenų pobūdį ir apimtis, kaip lengvai identifikuojamas fizinis asmuo, pasekmių rimtumą fiziniams asmenims, specialias fizinio asmens savybes, nukentėjusių fizinių asmenų skaičių, specialias Įmonės savybes/
Rizikos tikimybė	*Nėra/žema/vidutinė/aukšta*
Pranešta įmonės vadovui:	*Taip/ne/data*
Pranešimas VDAI:	

Pranešimas duomenų subjektams:	

Atsakingas asmuo:	

/Vardas, pavardė, parašas, data/