

ASMENS DUOMENŲ APSAUGOS POLITIKA

I. PAGRINDINĖS POLITIKOS SĄVOKOS

1. **Bendrovė** – UAB Klaipėdos regiono atliekų tvarkymo centras, juridinio asmens kodas 163743744, adresas: Liepų g. 15, Klaipėda.
2. **Darbuotojas** – pagal darbo sutartį Bendrovėje dirbantis asmuo.
3. **Vadovas** – Bendrovės direktorius.
4. **Asmens duomenys** – bet kuri informacija, susijusi su fiziniu asmeniu, kurio tapatybė yra žinoma arba gali būti tiesiogiai ar netiesiogiai nustatyta pasinaudojant tokiais duomenimis kaip asmens kodas, vienas arba keli asmeniui būdingi fizinio, fiziologinio, psichologinio, ekonominio, kultūrinio ar socialinio pobūdžio požymiai.
5. **Politika** reiškia šią Asmens duomenų tvarkymo politiką.

II. TIKSLAS IR APIMTIS

6. Asmens duomenų apsaugos politika parengta ir taikoma siekiant apsaugoti Bendrovės darbuotojus, partnerius ir klientus nuo neteisėtų ir žalą sukeliančių tiesioginių ar netiesioginių, sąmoningų ar nesąmoningų asmenų veiksmų, tvarkant jiems prieinamus asmens duomenis, taip pat šiais tikslais naudojant atitinkamą įrangą savo darbo funkcijoms atlikti.

7. Politika privalo būti taikoma Bendrovėje tvarkant bet kuriose sistemose esančią ar bet kurioje laikmenoje esamus asmens duomenis, nepriklausomai nuo to, ar jų tvarkymas yra susijęs su vidinėmis Bendrovės veiklos operacijomis ar su išoriniais Bendrovės ryšiais su bet kokiais trečiosiomis šalimis. Ji taip pat taikoma Darbuotojams jų darbinių pareigų atlikimo metu naudojant jiems suteiktą įrangą ir įrankius.

8. Bet kurie duomenys, kurie gali būti pripažinti Asmens duomenimis, kurie tampa prieinami ir žinomi Darbuotojams darbinių pareigų atlikimo metu, laikoma konfidencialia Bendrovei priklausančia informacija, kuri yra saugoma ir kuri negali būti atskleidžiama nei kitiems Darbuotojams, nei kitiems asmenims. Išimtis – tokie duomenys gali būti atskleidžiami tik tiems Darbuotojams, kurie pagal Bendrovės nustatytas tvarkas dėl jų atliekamų pareigų turi teisę susipažinti su tokiais duomenimis. Bendrovė nurodo, kad tokie duomenys privalo būti saugomi nepriklausomai nuo to, kokia forma jie pateko Darbuotojui (atspausdinti ar bet kokiame duomenų saugojimo įrenginyje, kaip garsinė/ vaizdinė medžiaga ar bet kokia kita forma).

III. DARBUOTOJŲ PAREIGOS

9. Visi Asmens duomenys ir kita informacija, pagal kurią galima nustatyti asmens tapatybę, renkama ir tvarkoma tik tada, kai tai reikalinga, ir tik tokia apimtimi, kokia reikalinga tam, kad Darbuotojas galėtų atlikti darbinės funkcijas jam suteiktų įgalinimų ribose ir prisilaikant įstatyminių reikalavimų duomenų apsaugai (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), Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas ir kiti teisės aktai, nustatantys asmens duomenų tvarkymą ir apsaugą, laikymąsi ir įgyvendinimą).

10. Asmens duomenys, patenkantys Darbuotojui darbinių pareigų atlikimo metu, yra laikomi ir traktuojami kaip konfidencialūs ir saugomi pagal šios Politikos nuostatas; jie negali būti atskleidžiami be teisėto pagrindo. Darbuotojas, abejojantys, ar turi teisę kitam Darbuotojui ar asmeniui atskleisti bet kokius Asmens duomenis, privalo kreiptis į Vadovą ar į Vadovo paskirtą įgaliotą asmenį, kad gautų patvirtinimą dėl tolimesnių veiksmų su Asmens duomenimis.

11. Kiekvienas Darbuotojas privalo laikytis šios Politikos, taip pat ir taikytinų įstatymų bei taisyklių, kuriomis nustatyti Asmens duomenų rinkimo, saugojimo bei tvarkymo reikalavimai. Politikos nesilaikymas bus laikomas šiurkščiu darbo pareigų pažeidimu ir, Bendrovės pasirinkimu, gali užtraukti drausmines sankcijas arba Darbuotojo atleidimą. Taip pat pažeidimą padariusiam Darbuotojui gali kilti administracinė arba baudžiamoji atsakomybė.

IV. KOMPIUTERINIŲ SISTEMŲ NAUDOJIMAS

12. Bet kokie kompiuteriniai įrenginiai bei elektroninės duomenų bazės Darbuotojams yra pasiekiami priklausomai nuo jų darbinių pareigų, atsakomybės ir vadovaujantis „būtinumo žinoti“ principu. Tuo pačiu Bendrovė pabrėžia, kad Darbuotojo priėjimas prie bet kokios duomenų bazės, nereiškia, kad Darbuotojas yra įgaliotas peržiūrėti ir naudoti visą toje bazėje esančią informaciją.

13. Bendrovėje gali būti taikomi naudotojų ID, jie yra unikalūs ir identifikuoja konkretų Darbuotoją. Kiekvienas Darbuotojas yra atsakingas už visus veiksmus, susijusius su jo asmenine ID paskyra, todėl pagrindinė pareiga yra užtikrinti, kad Darbuotojo ID yra neprieinamas trečiosioms šalims, netgi kitiems Darbuotojams, nebent Bendrovė būtų nustačiusi kitokią tvarką.

14. Kompiuterines sistemas ir duomenų bazes apsaugantys slaptažodžiai yra sudaromi atsakingai, tam kad nebūtų lengva juos atspėti, kad jie neapimtų asmens duomenų ir pagal poreikį būtų reguliariai keičiami. Kiekvienas Darbuotojas yra asmeniškai atsakingas už savo slaptažodžio saugojimą ir atitikimą šios Politikos nuostatomis ir bet kokioms kitoms Bendrovės taisyklėms.

15. Išskyrus konkrečiai nustatytas išimtis, jokiais atvejais ir jokiais aplinkybėmis Bendrovei, jos klientams ar bendradarbiavimo partneriams priklausantys įrenginiai ir/ar sistemos negali būti naudojami su Darbuotojo darbo pareigomis ar su Bendrovės veikla nesusijusiems tikslams.

V. SAUGUMO PRIEMONĖS

16. Visiems bet koku būdu surinktiems ir tvarkomiems bet kokios formos (popierinės, elektroninės ir kt.) Asmens duomenims ir su jais susijusiai informacijai yra taikomi šios Politikos ir bet kokių įstatymų reikalavimai dėl duomenų bei informacijos rinkimo, tvarkymo, apsaugos ir tolimesnio saugojimo, ir tokie dokumentai saugomi saugioje Bendrovės paskirtoje vietoje taikytinų įstatymų ir/ arba Bendrovės nustatytą laikotarpį.

17. Darbuotojams neleidžiama laikyti bet kokios su Asmens duomenimis susijusios informacijos savo įrenginiuose, išskyrus, kai jos laikinai reikia specifinei su darbu susijusiai veiklai. Visa reikalinga konfidenciali ir asmens tapatybę leidžianti nustatyti informacija turi būti saugoma tiktai Bendrovės specialiai nurodytoje nuotolinėje saugykloje. Reikėtų vengti bet kokio tokių bylų parsisiuntimo į vietinius įrenginius ir tokius veiksmus atlikti tik esant būtinybei, susijusiai su informacijos tvarkymu darbiniais tikslais.

18. Prisilaikydami taikytinų įstatymų ir taisyklių, tinkamai įgalioti Bendrovės atstovai gali filtruoti ir stebėti Darbuotojų interneto prieigą ir internete vykdomas operacijas.

19. Į Bendrovėje naudojamą įrangą gali būti instaliuojamos ir naudojamos tik Bendrovės leidžiamos sistemos ir licencijuota programinė įranga. Prieš parsisiunčiant ir instaliuojant bet kokią programinę įrangą į Darbuotojų turimus ir naudojamos įrenginius, dėl šioje Politikoje nurodytų

priežasčių reikalingas atitinkamo Bendrovės specialisto leidimas.

20. Tais atvejais, kai Darbuotojai prisijungdami prie darbinių Bendrovės išteklių (pvz., elektroninis paštas, internetinės/ nuotolinės duomenų bazės) naudoja namų įrenginius, Darbuotojai privalo laikytis šios Politikos reikalavimų taip pat, kaip ir naudodami Bendrovės suteiktą įrangą. Atitinkamai yra draudžiama saugoti bet kokius su Asmens duomenimis susijusius duomenis ir informaciją įrenginyje, bet koks duomenų tvarkymas leidžiamas tik per Bendrovės naudojamas nuotolines arba internetines saugyklas.

21. Visais atvejais griežtai draudžiama naudotis viešais prieigos įrenginiais (pvz., interneto kavinėse, bibliotekose, kt.), nebent tai ypatingai svarbus ir skubus darbas, ir Darbuotojas gauna aiškų rašytinį sutikimą dėl tokių veiksmų.

22. Tuo atveju, jeigu Darbuotojui suteikiama prieiga prie Bendrovės kliento ar paslaugų tiekėjo bylų saugojimo sistemos, Darbuotojas privalo naudoti kliento arba paslaugų tiekėjo suteiktus prieigos įrankius bei laikytis jam nurodytų informacijos/ duomenų tvarkymo saugumo taisyklių reikalavimų (įskaitant šifravimo sistemų, slaptažodžių, duomenų naudojimo apribojimų, nurodytų buvimo vietų naudojimą ir kt.)

23. Kai Bendrovės nuožiūra saugomi Asmens duomenys ir su jais susijusi informacija tampa nebereikalinga Bendrovės veikloje, tokie duomenys ir informacija ištrinama, visos jos kopijos sunaikinamos, o su atitinkamos informacijos ir duomenų tvarkymu susiję Darbuotojai atitinkamai informuojami apie jų pareigą ištrinti bei sunaikinti duomenis, kurių jiems nebereikia darbinių funkcijų vykdymui. Toks reikalavimas grąžinti Bendrovei, ištrinti ir sunaikinti kopijas automatiškai taikomas tuo atveju, kai nutraukiami atitinkamo Darbuotojo darbo santykiai.

VI. PRANEŠIMAS APIE SAUGUMO INCIDENTUS

24. Apie visus Asmens duomenų tvarkymo saugumo incidentus ar grėsusius incidentus turi būti nedelsiant pranešta Vadovui, ir turi būti nedelsiant imamasi priemonių išvengti galimos žalos, kilusią žalą panaikinti ir buvusią saugumo būseną atkurti.

25. Prireikus, Vadovas imasi pareigos užtikrinti, kad apie Asmens duomenų ir su jais susijusios informacijos saugumo pažeidimus būtų pranešta valdžios institucijoms ir susijusiems asmenims, kaip numatyta taikytinuose įstatymuose ir taisyklėse ir/ arba Europos Sąjungos įstatymuose.
