

DAIKTŲ SAUGOJIMO CENTRAS, UAB**ASMENS DUOMENŲ TVARKYMO POLITIKA IR JOS ĮGYVENDINIMO PRIEMONĖS****1. BENDROSIOS NUOSTATOS**

- 1.1. **Daiktų saugojimo centras, UAB**, juridinio asmens kodas 304784517, registruotos buveinės adresas Saliamono Banaičio g. 12, Vilnius (toliau – **Bendrovė**) Asmens duomenų saugojimo politika ir jos įgyvendinimo priemonės (toliau – **Politika**) nustato Bendrovės darbuotojų, kandidatų į darbuotojus, klientų, potencialių klientų, lankytojų (toliau vadinamų ir **duomenų subjektais**) asmens duomenų rinkimo, naudojimo ir saugojimo principus, tvarkymo tikslus, Bendrovėje įgyvendinamas organizacines ir technines priemones, skirtas apsaugoti asmens duomenims nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, taip pat asmens duomenų subjektų teisių įgyvendinimo taisyklės, poveikio duomenų apsaugos vertinimo procedūrą, asmens duomenų saugumo pažeidimų nagrinėjimo ir informavimo taisyklės Bendrovėje.
- 1.2. Šioje Politikoje vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamente (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo (toliau – **Reglamentas**), Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatyme (toliau – **Įstatymas**) ir kituose asmens duomenų tvarkymą reglamentuojančiuose teisės aktuose.
- 1.3. Bendrovė tvarko asmens duomenis kaip duomenų valdytojas ir kaip duomenų tvarkytojas.
- 1.4. Už tinkamą šios Politikos įgyvendinimą, jų vykdymo kontrolę ir asmens duomenų apsaugą Bendrovėje yra atsakingas darbuotojas / kitas asmuo, paskiriamas specialiu Bendrovės vadovo įsakymu (toliau – **Atsakingas asmuo**).

2. ASMENS DUOMENŲ TVARKYMO PRINCIPAI

- 2.1. Asmens duomenys Bendrovėje tvarkomi išimtinai vadovaujantis Reglamentu, Įstatymu, kitais teisės aktais ir Lietuvos bei tarptautiniais standartais, reglamentuojančiais asmens duomenų apsaugą ir informacijos saugumą.
- 2.2. Asmens duomenys Bendrovėje turi būti:
 - 2.2.1. duomenų subjekto atžvilgiu tvarkomi teisėtu, sąžiningu ir skaidriu būdu (teisėtumo, sąžiningumo ir skaidrumo principas);
 - 2.2.2. renkami ir tvarkomi apibrėžtais ir teisėtais tikslais, nustatytais prieš renkant asmens duomenis (tikslų apribojimo principas);
 - 2.2.3. yra adekvatūs ir tvarkomi tik tokia apimtimi, kuri būtina asmens duomenų tvarkymo tikslams pasiekti (duomenų kiekio mažinimo principas);
 - 2.2.4. tvarkomi tikslūs ir, jei reikia dėl asmens duomenų tvarkymo, nuolat atnaujinami; netikslūs ar neišsamūs duomenys yra ištaisomi, papildomi, sunaikinami arba sustabdomas jų tvarkymas (tikslumo principas);
 - 2.2.5. laikomi tokia forma, kad duomenų subjektų tapatybę būtų galima nustatyti ne ilgiau, negu to reikia tiems tikslams, dėl kurių šie duomenys buvo surinkti ir yra tvarkomi ir saugomi ne ilgiau nei to reikalauja nustatyti duomenų tvarkymo tikslai (saugojimo trukmės apribojimo principas);

- 2.2.6. tvarkomi tokiu būdu, kad taikant atitinkamas technines ar organizacines priemones būtų užtikrintas tinkamas asmens duomenų saugumas, įskaitant apsaugą nuo duomenų tvarkymo be leidimo arba neteisėto duomenų tvarkymo ir nuo netyčinio praradimo, sunaikinimo ar sugadinimo (vientisumo ir konfidencialumo principas).
- 2.3. Asmenys, tvarkantys asmens duomenis, privalo saugoti asmens duomenų paslaptį, nebent šie asmens duomenys yra vieši pagal įstatymus ar kitų teisės aktų nuostatas. Ši pareiga galioja ir pasibaigus darbo / kitiems šiuos asmenis ir Bendrovę siejusiems teisiniams santykiams.

3. ASMENS DUOMENŲ TVARKYMO TEISINIS PAGRINDAS, TIKSLAI IR APIMTIS

- 3.1. Bendrovėje asmens duomenys tvarkomi aiškiai apibrėžtais tikslais, kurie yra žinomi duomenų subjektui. Jei pasikeičia surinktų duomenų tvarkymo tikslas, apie tai informuojamas duomenų subjektas.
- 3.2. Bendrovė, kaip duomenų valdytojas, tvarko tokių kategorijų asmens duomenis, tokiais teisiniais pagrindais ir tikslais (detaliau Bendrovėje tvarkomi asmens duomenys gali būti aprašomi duomenų tvarkymo veiklos įrašuose, 4 priede):
- 3.2.1. darbuotojų duomenys tvarkomi vidaus administravimo tikslais (darbo sutarties vykdymas, struktūros tvarkymas, personalo valdymas, turimų materialinių ir finansinių išteklių valdymas ir naudojimas, raštvedybos tvarkymas ir kt.), Bendrovės kaip darbdavio pareigų, nustatytų teisės aktuose ir asmenų bei turto apsaugos tikslais;
- 3.2.2. kandidatų į darbuotojus duomenys tvarkomi su tikslu atrinkti tinkamą darbuotoją duomenų subjekto sutikimo pagrindu, arba siekiant imtis veiksmų duomenų subjekto prašymu prieš sudarant sutartį;
- 3.2.3. neatrinktų kandidatų į darbuotojus duomenys tvarkomi su tikslu pateikti naujus įdarbinimo pasiūlymus, jei asmuo yra davęs sutikimą;
- 3.2.4. klientų duomenys tvarkomi sutarčių vykdymo tikslais;
- 3.2.5. esamų klientų duomenys tvarkomi tiesioginės rinkodaros tikslais ir klientams yra suteikiama aiški, nemokama ir lengvai įgyvendinama galimybė nesutikti arba atsisakyti tokio kontaktinių duomenų naudojimo pirmiau nurodytais tikslais.
- 3.2.6. potencialių klientų duomenys tvarkomi tiesioginės rinkodaros tikslais, jei asmuo yra davęs sutikimą, o naudojant pašto adresą teisėto intereso pagrindu.
- 3.3. Bendrovė, kaip duomenų tvarkytojas, tvarko asmens duomenis vykdydama veiklą duomenų valdytojų vardu (detaliau Bendrovėje tvarkomi asmens duomenys gali būti aprašomi duomenų tvarkymo veiklos įrašuose, 5 priede). Tais atvejais, kai Bendrovė veikia kaip duomenų tvarkytojas duomenų valdytojo vardu, duomenų tvarkymas aprašomas susitarimuose dėl asmens duomenų tvarkymo.

4. ASMENS DUOMENŲ SAUGOJIMO TVARKA IR TERMINAI

- 4.1. Subjekto asmens duomenys saugomi tiek laiko, kiek pagal įstatymus ir kitus teisės aktus turi būti saugomi dokumentai ar bylos, kuriuose yra nurodomi asmens duomenys. Kai asmens duomenys nebereikalingi jų tvarkymo tikslams, jie yra sunaikinami, išskyrus tuos duomenis / dokumentus, kurie teisės aktų nustatytais atvejais ir tvarka turi būti perduoti valstybiniais archyvams.
- 4.2. Kandidatų į darbuotojus asmens duomenys tvarkomi atrankos į darbo vietą laikotarpiu ir pasibaigus šiam terminui sunaikinami, išskyrus tuos atvejus, kai neatrinktas kandidatas išreiškia sutikimą naudoti jo asmens duomenis kitiems darbo pasiūlymams Bendrovėje pateikti. Šie asmens duomenys tvarkomi sutikime nurodytu laikotarpiu. Sutikimas tvarkyti asmens duomenis gali būti bet kada atšauktas pateikus prašymą Bendrovei. Tokiu atveju gali būti naudojama 1 priede pateikta sutikimo forma.

- 4.3. Esamų klientų duomenys tiesioginės rinkodaros tikslais tvarkomi tol, kol duomenų subjektas yra Bendrovės klientu, išskyrus atvejus, kai klientas nesutinka arba atsisako tokio kontaktinių duomenų naudojimo pirmiau nurodytais tikslais.
- 4.4. Potencialių klientų duomenys tiesioginės rinkodaros tikslais tvarkomi nuo sutikimo pateikimo dienos iki tol, kol duomenų subjektas atšaukia savo sutikimą.
- 4.5. Bendrovė asmens duomenis tvarko popieriniu ir (ar) elektroniniu formatu.

5. PRIEIGA PRIE ASMENS DUOMENŲ

- 5.1. Prieigos teisės ir įgaliojimus tvarkyti asmens duomenis suteikia, naikina ir keičia Bendrovės vadovas, jo įgaliotas asmuo arba Atsakingas asmuo, atsižvelgęs į konkretaus asmens atliekamas funkcijas. Prieigos teisė gali būti reglamentuota vidaus teisės aktuose, darbo sutartyse, pareiginėse instrukcijose, susitarimuose ir kituose dokumentuose.
- 5.2. Prieiga prie asmens duomenų suteikiama tik tiems asmenims (Bendrovės darbuotojams ar kitų teisinių santykių pagrindu veikiančioms asmenims, įskaitant saugos tarnybos darbuotojus, atsakingus už Bendrovės patalpų fizinę apsaugą, asmenų įėjimo į patalpas kontrolę, darbų saugą, buhalterinę apskaitą vykdančius darbuotojus ir kt.), kuriems asmens duomenys yra reikalingi jų funkcijoms vykdyti.
- 5.3. Prieigos teisę bei įgaliojimus tvarkyti asmens duomenis turintys asmenys su asmens duomenimis gali atlikti tik tuos veiksmus, kuriems atlikti jiems yra suteiktos teisės, nurodytos darbo sutartyje, pareiginėse instrukcijose ir (ar) atskirai įformintame pavedime.
- 5.4. Visi Bendrovės darbuotojai ar kitų teisinių santykių pagrindu veikiančios asmenys, turintys prieigos teisę ir įgalioti tvarkyti asmens duomenis, privalo laikytis konfidencialumo įsipareigojimų, išskyrus atvejus, kai duomenis privaloma atskleisti valdžios institucijoms laikantis teisinės prievolės.
- 5.5. Visi Bendrovės darbuotojai ar kitų teisinių santykių pagrindu veikiančios asmenys, turintys prieigos teisę ir įgalioti tvarkyti asmens duomenis, privalo laikytis šios Politikos ir turi būti pasirašytinai arba kitu būdu, įrodančiu informavimo faktą, su ja supažindinti. Atsakingas asmuo organizuoja tokių asmenų supažindinimą su šia Politika.
- 5.6. Bendrovės darbuotojus / kitais teisinais santykiais veikiančius asmenis, kuriems suteiktos prieigos ir tvarkymo teisės, informuoja ir jų apmokymus organizuoja Bendrovės vadovas ir / arba Atsakingas asmuo, atsižvelgęs į teisinius reikalavimus, realius Bendrovės poreikius ir finansines galimybes.
- 5.7. Prieiga prie asmens duomenų apribojama ir duomenų tvarkymo įgaliojimai keičiami pasikeitus asmenų, turinčių prieigos teisę ir įgaliotų tvarkyti asmens duomenis, pareigoms, naikinami – nustačius, kad nesilaikyta šios Politikos nuostatų ar kitų reikalavimų, asmens duomenys buvo tvarkomi netinkamai, pažeisti įstatymai.
- 5.8. Asmenys, turintys prieigos teisę prie Bendrovėje tvarkomų asmens duomenų, privalo informuoti Atsakingą asmenį apie pagrįstą įtarimą dėl asmens duomenų saugumo pažeidimo. Jei nustatomas įvykęs asmens duomenų saugumo pažeidimas, asmuo turi veikti laikantis Politikos skirsnio „Asmens duomenų saugumo pažeidimo nustatymo ir informavimo procedūra“.
- 5.9. Bendrovė reguliariai peržiūri turimas prieigos teises prie asmens duomenų. Laikydamosi vientisumo ir konfidencialumo principo, Asmens duomenys tvarkomi taip, kad būtų užtikrintas tinkamas asmens duomenų saugumas ir konfidencialumas, be kita ko, užkertant kelią neteisėtai prieigai prie asmens duomenų ir jų tvarkymui skirtos įrangos ar neteisėtam jų naudojimui.

6. ASMENS DUOMENŲ SAUGUMO PRIEMONĖS

- 6.1. Tvarkydama ir saugodama asmens duomenis Bendrovė įgyvendina administracines, technines ir programines įrangos apsaugos bei komunikacijų ir kompiuterių tinklų apsaugos

priemonės, užtikrinančias asmens duomenų apsaugą nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, taip pat nuo bet kokie kito neteisėto tvarkymo.

6.2. Bendrovės įgyvendinamos priemonės apima:

6.2.1. administracines priemones, tokias kaip: saugaus dokumentų ir kompiuterinių duomenų bei jų archyvų tvarkymo, taip pat įvairių veiklos sričių darbo organizavimo tvarkos nustatymas, personalo supažindinimas su asmens duomenų tvarkymą reglamentuojančiais Bendrovėje patvirtintais dokumentais ir kt.;

6.2.2. technines ir programines įrangos apsaugos priemones, tokias kaip: licencijuotos programinės įrangos naudojimas, kompiuterinės įrangos apsaugos nuo kenksmingos programinės įrangos užtikrinimas, informacinių sistemų ir duomenų bazių administravimas, darbo vietų, Bendrovės patalpų priežiūra (įskaitant užtikrinimą, jog į patalpas, kuriose saugomi asmens duomenys, patektų tik įgalioti asmenys), operacinių sistemų apsauga, apsauga nuo kompiuterinių virusų ir kt. Asmens duomenų apsaugos techninės ir programinės priemonės turi užtikrinti: operacinių sistemų ir duomenų bazių kopijų saugyklos įrengimą, kopijavimo ir atkūrimo avarinio praradimo atveju technikos įdiegimą, nustatymų ir laikymosi kontrolę, atsarginių asmens duomenų kopijų (jei jos daromos) saugojimą kitoje patalpoje ar geografinėje vietoje negu aktyvi (veikianti) duomenų bazė, atsarginėse kopijose (jei daromos), archyvuose ir išorinėse duomenų laikmenose saugomų asmens duomenų šifravimą, nenutrūkstamo duomenų tvarkymo (apdorojimo) proceso technologiją, sistemų veiklos atnaujinimo nenumatytais atvejais strategiją (netikėtumų valdymas), programų testavimo aplinkos fizinį (loginį) atskyrimą nuo darbo režimo procesų, autorizuotą duomenų naudojimą, jų nepažeidžiamumą, registravimosi bei teisių gavimo pastangų fiksavimą ir kontrolę, leistinių nepavykusių prisijungimų skaičiaus nustatymą, prisijungimų prie asmens duomenų įrašų fiksavimą, asmens duomenų naudojimo tikslo nurodymą teikiamų asmens duomenų paieškos užklausoje, prisijungimų prie asmens duomenų įrašų fiksavimą bei saugojimą ne trumpiau nei 1 (vienerius) metus, asmens duomenų šifravimo ir saugos kontrolės užtikrinimą, duomenis gaunant / teikiant išorinėje duomenų laikmenoje, saugių protokolų (pvz., SSL) / slaptažodžių naudojimą, duomenis gaunant / teikiant išoriniais duomenų perdavimo tinklais;

6.2.3. komunikacijų ir kompiuterių tinklų apsaugos priemones, tokias kaip: bendro naudojimo duomenų, programų, nepageidaujamų duomenų paketų filtravimas (angl. *firewalling*), vidinio kompiuterių tinklo apsaugojimas veiksminga ugniasiene ir kt.;

6.3. Asmens duomenų saugumo pažeidimų valdymą Bendrovėje nuolat atlieka Atsakingas asmuo arba kitas Bendrovės vadovo įgaliotas asmuo. Nustatęs konkrečias asmens duomenų apsaugos Bendrovėje rizikas, jis nedelsiant imasi visų galimų techninių ir organizacinių priemonių joms pašalinti.

6.4. Asmens duomenų tvarkymo keliamos rizikos vertinimas Bendrovėje atliekamas ne rečiau kaip kartą per 1 (vienerius) metus. Atsižvelgiant į rizikos vertinimo rezultatus, įdiegiamos reikiamos duomenų saugumo priemonės. Vertinimo rezultatai įforminami tik tuo atveju, jei buvo nustatyta asmens duomenų apsaugos Bendrovėje trūkumų.

6.5. Avarinio asmens duomenų atkūrimo tvarka patikrinama atliekant praktinius bandymus ne rečiau kaip kartą per 1 (vienerius) metus.

6.6. Bendrovė užtikrina, kad informacinių sistemų testavimas nebūtų vykdomas su realiais asmens duomenimis.

6.7. Įgyvendintų organizacinių ir techninių duomenų saugumo priemonių įvertinimo auditas Bendrovėje atliekamas ne rečiau kaip kartą per 2 (dvejus) metus. Audito rezultatai įforminami tik tuo atveju, jei buvo nustatyta asmens duomenų apsaugos Bendrovėje trūkumų.

6.8. Prisijungimas prie Bendrovės kompiuterių, kompiuterių tinklo, duomenų bazės yra apsaugotas konfidencialiu slaptažodžiu. Slaptažodis privalo visada būti kuo sudėtingesnis. Slaptažodis sudaromas iš ne mažiau kaip 8 (aštuonių) simbolių, jį turi sudaryti kuo įvairesni simboliai (didžiosios, mažosios lotyniškos raidės, skaičiai, kt.). Slaptažodžiai keičiami ne rečiau kaip kartą per 3 (tris) mėnesius. Pirmojo prisijungimo metu naudotojo slaptažodis privalomai keičiamas.

- 6.9. Nustačius duomenų pažeidimus ar avarinio praradimo atvejus, asmens duomenys Bendrovėje atkuriami iš kopijų Bendrovės vadovo arba Atsakingo asmens sprendimu per įmanomai trumpiausią laiką.
- 6.10. Asmens duomenys Bendrovėje sunaikinami Bendrovės vadovo arba Atsakingo asmens sprendimu pasibaigus asmens duomenų saugojimo terminams ar kitais teisės aktuose ir šioje Politikoje numatytais pagrindais ir terminais. Atsiradus pagrindui, visais atvejais asmens duomenys Bendrovėje sunaikinami ne vėliau kaip per 10 (dešimt) darbo dienų.
- 6.11. Asmenys, tvarkantys darbuotojų asmens duomenis turi imtis priemonių, kad būtų užkirstas kelias atsitiktiniam ar neteisėtam asmens duomenų sunaikinimui, pakeitimui, atskleidimui, taip pat bet kokiam kitam neteisėtam tvarkymui, įskaitant tai, kad asmens duomenys būtų tinkamai ir saugiai tvarkomi bei būtų išvengiama nereikalingų jų kopijų darymo. Darbuotojai, palikdami darbo vietą, privalo užrakinti kompiuterį. Jei darbuotojo kompiuteris yra neaktyvus 5 (penkias) minutes, kompiuteris užrakinamas automatiškai.
- 6.12. Jei asmenys, kuriems taikoma ši Politika, abejoja įdiegtų saugumo priemonių patikimumu, jie turi nedelsiant kreiptis į Atsakingą asmenį, kad būtų įvertintos turimos saugumo priemonės ir, jei reikia, inicijuotas papildomų priemonių įsigijimas ir įdiegimas.
- 6.13. Asmenys, kuriems taikoma ši Politika, pastebėję, kad Bendrovėje tvarkomi asmens duomenys tapo ar gali tapti prieinami asmenims, neturintiems teisės tvarkyti tvarkomų asmens duomenų, nedelsiant imasi visų įmanomų priemonių neteisėtai prieigai prie tvarkomų asmens duomenų ar jos atsiradimo galimybei nutraukti, taip pat apie šiuos veiksmus informuoja Atsakingą asmenį.
- 6.14. Įvykus asmens duomenų saugumo pažeidimams Bendrovėje, kaip tai numatoma teisės aktų reikalavimuose, Atsakingas asmuo, įvertinęs asmens duomenų saugumo pažeidimo neigiamą poveikį, sprendžia klausimą apie pranešimo pateikimą Valstybinei asmens duomenų inspekcijai (priežiūros institucijai) ir (jei būtina) duomenų subjektui, kaip nurodyta Politikos skirsnyje „Asmens duomenų saugumo pažeidimo nustatymo ir informavimo procedūra“.

7. ASMENS DUOMENŲ SAUGUMO PAŽEIDIMO NAGRINĖJIMO IR INFORMAVIMO PROCEDŪRA

- 7.1. Jei Bendrovėje įvyksta asmens duomenų saugumo pažeidimas, dėl kurio netyčia arba neteisėtai sunaikinami, prarandami, pakeičiami, be leidimo atskleidžiami persiųsti, saugomi arba kitaip tvarkomi asmens duomenys arba prie jų be leidimo gaunama prieiga, tai nustatęs asmuo nedelsiant informuoja Atsakingą asmenį arba Bendrovės vadovą.
- 7.2. Atsakingas asmuo arba Bendrovės vadovas, priklausomai nuo asmens duomenų saugumo pažeidimo pobūdžio, informuoja kompetentingą asmenį apie asmens duomenų saugumo pažeidimą, kad pastarasis imtųsi priemonių pašalinti asmens duomenų saugumo pažeidimą, įskaitant, kai tinkama, imtųsi priemonių galimoms neigiamoms jo pasekmėms sumažinti.
- 7.3. Atsakingas asmuo ar Bendrovės vadovas pasitikrina pagal pažeidimo nustatymo ir veikimo procedūros schemą, pridėdamą prie Politikos 2 priedą. Jei Atsakingas asmuo ar Bendrovės vadovas nustato, kad Bendrovės, kaip duomenų valdytojo tvarkomų asmens duomenų saugumo pažeidimas gali sukelti ar sukėlė pavojų fizinių asmenų teisėms ir laisvėms, apie tai nedelsdamas ir, jei įmanoma, praėjus ne daugiau kaip 72 (septyniasdešimt dviem) valandoms nuo tada, kai sužino apie asmens duomenų saugumo pažeidimą, apie tai praneša Valstybinei asmens duomenų inspekcijai. Pranešime Valstybinei asmens duomenų inspekcijai turi būti pateikta bent tokia informacija (kai ir jeigu informacijos neįmanoma pateikti tuo pačiu metu, informacija toliau nepagrįstai nedelsiant gali būti teikiama etapais):
 - 7.3.1.1. aprašytas asmens duomenų saugumo pažeidimo pobūdis, įskaitant, jeigu įmanoma, atitinkamų duomenų subjektų kategorijas ir apytikslį skaičių, taip pat atitinkamų asmens duomenų įrašų kategorijas ir apytikslį skaičių;
 - 7.3.2. nurodyta duomenų apsaugos pareigūno (jei toks paskirtas) arba kito kontaktinio asmens, galinčio suteikti daugiau informacijos, vardas bei pavardė (pavadinimas) ir kontaktiniai duomenys;
 - 7.3.3. aprašytos tikėtinos asmens duomenų saugumo pažeidimo pasekmės;

- 7.3.4. aprašytos priemonės, kurių ėmėsi arba pasiūlė imtis duomenų valdytojas, kad būtų pašalintas asmens duomenų saugumo pažeidimas, įskaitant, kai tinkama, priemonės galimoms neigiamoms jo pasekmėms sumažinti.
- 7.4. Pranešimas Valstybinei asmens duomenų inspekcijai pildomas pagal Politikos 2 priede pateiktą formą arba pagal priežiūros institucijos patvirtintą formą (jei tokia yra).
- 7.5. Jei dėl asmens duomenų saugumo pažeidimo gali kilti didelis pavojus duomenų fizinių asmenų teisėms ir laisvėms, Bendrovė, kaip duomenų valdytojas, nepagrįstai nedelsdama praneša apie asmens duomenų saugumo pažeidimą duomenų subjektui.
- 7.6. Pranešimas duomenų subjektui parengiamas aiškia ir paprasta kalba, aprašomas asmens duomenų saugumo pažeidimo pobūdis ir pateikiama bent Politikos 7.3.1. – 7.3.2. punktuose nurodyta informacija ir priemonės.
- 7.7. Bendrovė gali neteikti pranešimo duomenų subjektui, jeigu įvykdomos bet kurios toliau nurodytos sąlygos:
- 7.7.1. Bendrovė, kaip duomenų valdytojas, įgyvendino tinkamas technines ir organizacines apsaugos priemones ir tos priemonės taikytos asmens duomenims, kuriems asmens duomenų saugumo pažeidimas turėjo poveikio, visų pirma tas priemones, kuriomis užtikrinama, kad asmeniui, neturinčiam leidimo susipažinti su asmens duomenimis, jie būtų nesuprantami, pavyzdžiui, šifravimo priemonės;
- 7.7.2. Bendrovė, kaip duomenų valdytojas, vėliau ėmėsi priemonių, kuriomis užtikrinama, kad nebegalėtų kilti didelis pavojus duomenų subjektų teisėms ir laisvėms;
- 7.7.3. tai pareikalautų neproporcingai daug pastangų. Tokiu atveju vietoj to apie tai viešai paskelbiama arba taikoma panaši priemonė, kuria duomenų subjektai būtų informuojami taip pat efektyviai.
- 7.8. Jei Bendrovė veikia kaip duomenų tvarkytojas ir įvyksta asmens duomenų saugumo pažeidimas, Atsakingas asmuo ar Bendrovės vadovas nepagrįstai nedelsdamas, bet ne vėliau nei nurodyta susitarime dėl duomenų tvarkymo su duomenų valdytoju, praneša apie tai duomenų valdytojui.
- 7.9. Bendrovė dokumentuoja visus asmens duomenų saugumo pažeidimus, įskaitant su asmens duomenų saugumo pažeidimu susijusius faktus, jo poveikį ir taisomuosius veiksmus, kurių buvo imtasi. Remdamasi tais dokumentais, Valstybinė asmens duomenų inspekcija turi galėti patikrinti, ar laikomasi Reglamento.

8. DUOMENŲ SUBJEKTŲ TEISĖS

- 8.1. Duomenų subjektas turi šias teises ir jų įgyvendinimo priemones, susijusias su jo asmens duomenų tvarkymu Bendrovėje:
- 8.1.1. žinoti (būti informuotas) apie savo asmens duomenų rinkimą ir tvarkymą. Duomenų valdytojas asmens duomenų gavimo metu duomenų subjektui pateikia visą šią informaciją:
- 8.1.1.1. duomenų valdytojo (ir duomenų apsaugos pareigūno, jei toks yra) kontaktinius duomenis;
- 8.1.1.2. duomenų tvarkymo tikslus;
- 8.1.1.3. duomenų tvarkymo teisinį pagrindą;
- 8.1.1.4. teisėtus interesus, jei tokie yra;
- 8.1.1.5. duomenų gavėjus arba atitinkamų asmens duomenų kategorijas;
- 8.1.1.6. apie ketinimą perduoti asmens duomenis į trečiąją valstybę arba tarptautinei organizacijai ir taikomas su duomenų perdavimu susijusias apsaugos priemones;
- 8.1.1.7. kai įmanoma, numatomas asmens duomenų saugojimo laikotarpis arba, jei neįmanoma, kriterijus, taikomus tam laikotarpiui nustatyti;

- 8.1.1.8. apie teisę prašyti duomenų valdytojo ištaisyti arba ištrinti asmens duomenis ar apriboti su duomenų subjektu susijusių asmens duomenų tvarkymą arba nesutikti su tokiu tvarkymu;
 - 8.1.1.9. apie teisę pateikti skundą priežiūros institucijai;
 - 8.1.1.10. apie asmens duomenų tvarkymo teisinį pagrindą, nurodant, ar asmens duomenų pateikimas yra teisės aktais ar sutartyje numatytas reikalavimas, ir informaciją apie galimas tokių duomenų nepateikimo pasekmes;
 - 8.1.1.11. apie automatizuotą sprendimų priėmimą, įskaitant profiliavimą, jo pagrindimą, taip pat tokio duomenų tvarkymo reikšmę ir numatomas pasekmes duomenų subjektui;
 - 8.1.1.12. kai asmens duomenys renkami ne iš duomenų subjekto, papildomai privaloma pateikti visą turimą informaciją apie jų šaltinius ir, jei taikoma, ar duomenys gauti iš viešai prieinamų šaltinių. Tokiu atveju duomenų valdytojas privalo pateikti aukščiau nurodytą informaciją per pagrįstą laikotarpį nuo asmens duomenų gavimo, bet ne vėliau kaip per 1 (vieną) mėnesį.
- 8.1.2. susipažinti su savo asmens duomenimis ir kaip jie yra tvarkomi gaunant toliau nurodytą informaciją:
- 8.1.2.1. duomenų tvarkymo tikslus;
 - 8.1.2.2. atitinkamų asmens duomenų kategorijas;
 - 8.1.2.3. duomenų gavėjus arba duomenų gavėjų kategorijas, kuriems buvo arba bus atskleisti asmens duomenys, visų pirma duomenų gavėjai trečiojoje valstybėje arba tarptautinės organizacijos;
 - 8.1.2.4. kai įmanoma, numatomas asmens duomenų saugojimo laikotarpis arba, jei neįmanoma, kriterijus, taikomus tam laikotarpiui nustatyti;
 - 8.1.2.5. apie teisę prašyti duomenų valdytojo ištaisyti arba ištrinti asmens duomenis ar apriboti su duomenų subjektu susijusių asmens duomenų tvarkymą arba nesutikti su tokiu tvarkymu;
 - 8.1.2.6. apie teisę pateikti skundą priežiūros institucijai;
 - 8.1.2.7. kai asmens duomenys renkami ne iš duomenų subjekto, visą turimą informaciją apie jų šaltinius;
 - 8.1.2.8. apie automatizuotą sprendimų priėmimą, įskaitant profiliavimą, jo pagrindimą, taip pat tokio duomenų tvarkymo reikšmę ir numatomas pasekmes duomenų subjektui;
 - 8.1.2.9. apie taikomas su duomenų perdavimu susijusias apsaugos priemones, kai asmens duomenys perduodami į trečiąją valstybę arba tarptautinę organizaciją.
- 8.1.3. reikalauti ištaisyti netikslius, neišsamius duomenis;
- 8.1.4. reikalauti ištrinti duomenis („teisė būti pamirštam“), jei yra bent viena iš šių priežasčių:
- 8.1.4.1. asmens duomenys nebėra reikalingi, kad būtų pasiekti tikslai, kuriais jie buvo renkami arba kitaip tvarkomi;
 - 8.1.4.2. asmens duomenų subjektas atšaukia sutikimą, kuriuo grindžiamas duomenų tvarkymas, ir nėra jokio kito teisinio pagrindo tvarkyti duomenis;
 - 8.1.4.3. asmens duomenų subjektas nesutinka su duomenų tvarkymu;
 - 8.1.4.4. asmens duomenys buvo tvarkomi neteisėtai;
 - 8.1.4.5. asmens duomenys turi būti ištrinti laikantis Europos Sąjungos arba duomenų valdytojui taikytinoje teisėje nustatytos teisinės prievolės;
 - 8.1.4.6. asmens duomenys buvo surinkti informacinės visuomenės paslaugų siūlymo vaikui kontekste.
- 8.1.5. reikalauti apriboti duomenų tvarkymą (išskyrus saugojimą), kai:

- 8.1.5.1. duomenų subjektas užginčija duomenų tikslumą;
 - 8.1.5.2. asmens duomenų tvarkymas yra neteisėtas ir duomenų subjektas nesutinka, kad duomenys būtų ištrinti;
 - 8.1.5.3. bendrovei nebereikia asmens duomenų asmens duomenų tvarkymo tikslais, tačiau jų reikia duomenų subjektui siekiant pareikšti, vykdyti arba apginti teisinius reikalavimus;
 - 8.1.5.4. duomenų subjektas paprieštaravo duomenų tvarkymui, kol bus patikrinta, ar duomenų valdytojo teisėtos priežastys yra viršesnės už duomenų subjekto priežastis.
- 8.1.6. nesutikti, kad būtų tvarkomi Bendrovei neprivalomi jo asmens duomenys, arba, kad sprendimų priėmimas būtų grindžiamas tik automatizuotu duomenų tvarkymu, įskaitant profiliavimą, dėl kurio kyla teisinės pasekmės arba kuris daro jam didelį poveikį;
- 8.1.7. gauti su juo susijusius asmens duomenis, kuriuos jis pateikė duomenų valdytojui susistemintu, įprastai naudojamu ir kompiuterio skaitomu formatu, ir turi teisę prašyti vieno valdytojo persiųsti duomenis kitam valdytojui, kai tai techniškai įmanoma.
- 8.2. Bendrovė, gavusi duomenų subjekto paklausimą dėl jo asmens duomenų tvarkymo, privalo atsakyti ne vėliau kaip per 30 (trisdešimt) kalendorinių dienų nuo duomenų subjekto kreipimosi dienos. Duomenų subjekto prašymu tokie duomenys turi būti pateikiami raštu. Jei duomenų subjektas pageidauja susipažinti su vaizdo duomenimis, tuomet jam sudaroma galimybė Bendrovės patalpose peržiūrėti vaizdo įrašą, arba, duomenų subjekto prašymu, pateikiama vaizdo įrašo kopija išorinėje duomenų laikmenoje ar nuotrauka. Įgyvendinant duomenų subjekto teisę susipažinti su savo vaizdo duomenimis, užtikrinama trečiųjų asmenų teisė į privatų gyvenimą, t. y. duomenų subjektui susipažįstant su vaizdo įrašu, jeigu vaizdo įrašė matomi kiti asmenys, kurių tapatybė gali būti nustatyta, ar kita informacija, kuri gali pažeisti trečiųjų asmenų privatumą (pavyzdžiui, transporto priemonės valstybinis numeris), šie vaizdai turi būti retušuoti ar kitais būtais panaikinama galimybė identifikuoti trečiuosius asmenis.
- 8.3. Neatlygintinai duomenų subjektui pateikiama viena tvarkomų asmens duomenų kopija. Už bet kokias kitas duomenų subjekto prašomas kopijas, Bendrovė gali imti pagrįstą mokestį, nustatomą pagal administracines išlaidas. Kai duomenų subjektas pateikia prašymą elektroninėmis priemonėmis ir išskyrus atvejus, kai duomenų subjektas paprašo ją pateikti kitaip, informacija pateikiama įprastai naudojama elektronine forma.
- 8.4. Jeigu duomenų subjektas, susipažinęs su savo asmens duomenimis, nustato, kad jo asmens duomenys yra neteisingi, neišsamūs ar netikslūs, jis gali kreiptis į Bendrovę, o ši nedelsdama asmens duomenis patikrina ir duomenų subjekto prašymu per 10 (dešimt) darbo dienų ištaiso neteisingus, neišsamius, netikslus asmens duomenis.
- 8.5. Jeigu duomenų subjektas, susipažinęs su savo asmens duomenimis, nustato, kad jo asmens duomenys yra tvarkomi neteisėtai, nesąžiningai, ir kreipiasi dėl to į Bendrovę, Bendrovė nedelsdama neatlygintinai patikrina asmens duomenų tvarkymo teisėtumą, sąžiningumą ir duomenų subjekto rašytiniu prašymu sunaikina neteisėtai ir nesąžiningai sukauptus asmens duomenis.
- 8.6. Bendrovė nedelsdama praneša duomenų subjektui apie duomenų subjekto prašymu atliktą ar neatliktą asmens duomenų ištaisymą, sunaikinimą.
- 8.7. Be duomenų subjekto žinios ir sutikimo naikinami netikslūs duomenys (pavyzdžiui, gavus pranešimą, kad elektroninio pašto adresas netikslus, todėl negali nueiti laiškas; grįžus korespondencijai dėl neegzistuojančio ar netikslaus gyvenamosios vietos adreso). Tokie duomenys sunaikinami per 10 (dešimt) darbo dienų po to, kai buvo išsiaiškinta, kad duomenys netikslūs.

9. KONFIDENCIALUMAS

- 9.1. Asmenys, kuriems suteikiama prieiga prie Bendrovės tvarkomų asmens duomenų, privalo laikytis konfidencialumo principo ir laikyti paslapyje bet kokią su asmens duomenimis susijusią

informaciją, nebent tokia informacija būtų vieša pagal taikytinos teisės nuostatas arba asmens duomenis privaloma būtų atskleisti valdžios institucijoms laikantis teisinės prievolės.

- 9.2. Konfidencialumo principo užtikrinimo pareiga galioja ir panaikinus atitinkamą priegios prie Bendrovės tvarkomų asmens duomenų teisę, pasibaigus darbo / kitiems teisinimas santykiams.

10. POVEIKIO DUOMENŲ APSAUGAI VERTINIMO PROCEDŪRA

- 10.1. Poveikio duomenų apsaugai vertinimas (**PDAV**) – tai procesas, skirtas duomenų tvarkymui aprašyti ir tokio tvarkymo reikalingumui ir proporcingumui įvertinti, padedantis valdyti pavojų, kuris kyla fizinių asmenų teisėms ir laisvėms tvarkant asmens duomenis, nustatant pavojaus pašalinimo priemones.
- 10.2. Laikytina, kad PDAV būtina atlikti prieš diegiant naujas duomenų tvarkymo technologijas ir (ar), kai dėl duomenų tvarkymo fizinių asmenų teisėms ir laisvėms gali kilti didelis pavojus. Tokiems atvejams priskirtini:
 - 10.2.1. sistemingas ir išsamus su fiziniais asmenimis susijusių asmeninių aspektų vertinimas, kuris yra grindžiamas automatizuotu tvarkymu, įskaitant profiliavimą, ir kuriuo remiantis priimami sprendimai, kuriais padaromas su fiziniu asmeniu susijęs teisinis poveikis arba kurie daro panašų didelį poveikį fiziniam asmeniui (pvz., nagrinėjami ar prognozuojami su asmens darbo rezultatais, ekonomine padėtimi, sveikatos būkle, asmeniniais pomėgiais ar interesais, patikimumu arba elgesiu, vieta arba judėjimu susiję aspektai);
 - 10.2.2. specialių kategorijų duomenų arba asmens duomenų apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas tvarkymas dideliu mastu; arba
 - 10.2.3. sistemingas viešos vietos stebėjimas dideliu mastu;
 - 10.2.4. duomenų tvarkymo operacijos, kurias Valstybinė duomenų apsaugos inspekcija įtraukia į sąrašą (jei toks paviešinamas) operacijų, kurioms taikomas reikalavimas atlikti poveikio duomenų apsaugai vertinimą.
- 10.3. Tais atvejais, kai Bendrovėje planuojama diegti naujas duomenų tvarkymo operacijas, atitinkančias Politikos 10.2 punkte nurodytą bent vieną sąlygą, informuojamas Atsakingas asmuo, kuris turi įvertinti, ar reikia atlikti PDAV. Šiuo tikslu Atsakingas asmuo pirminį patikrinimą atlieka atsakydamas į 3 priedo klausimus. Jei nustatomas poreikis atlikti poveikio duomenų apsaugai vertinimą, PDAV turi būti atliktas užpildant Politikos 3 priedą.
- 10.4. Atlikdamas PDAV Bendrovė konsultuojasi su duomenų apsaugos pareigūnu, jei toks yra paskirtas.
- 10.5. Atlikus PDAV, užpildomas 3 priedas, pateikiant šią informaciją:
 - 10.5.1. sistemingas numatytų duomenų tvarkymo operacijų aprašymas ir duomenų tvarkymo tikslai, įskaitant, kai taikoma, teisėtus interesus, kurių siekia duomenų valdytojas;
 - 10.5.2. duomenų tvarkymo operacijų reikalingumo ir proporcingumo, palyginti su tikslais, vertinimas;
 - 10.5.3. duomenų subjektų teisėms ir laisvėms kylančių pavojų vertinimas; ir
 - 10.5.4. pavojams pašalinti numatytos priemonės, įskaitant apsaugos priemones, saugumo priemones ir mechanizmus, kuriais užtikrinama asmens duomenų apsauga;
 - 10.5.5. suderintą veiksmų planą, atsakingą asmenį už priemonių įgyvendinimą ir priemonių įgyvendinimo datą.
- 10.6. Jeigu atlikus PDAV nustatoma, kad tvarkant duomenis kiltų didelis pavojus, jei Bendrovė nesiimtų priemonių pavojui sumažinti, Bendrovė, prieš pradėdama tvarkyti asmens duomenis, privalo konsultuotis su Valstybine asmens duomenų inspekcija. Konsultuodamasi su priežiūros institucija, Bendrovė priežiūros institucijai nurodo:
 - 10.6.1. kai taikoma, atitinkamas duomenų tvarkymo procese dalyvaujancio duomenų valdytojo, bendrų duomenų valdytojų ir duomenų tvarkytojų atsakomybės sritis, visų pirma, kai duomenys tvarkomi įmonių grupėje;

- 10.6.2. numatyto duomenų tvarkymo tikslus ir priemones;
 - 10.6.3. nustatytas priemones bei apsaugos priemones duomenų subjektų teisėms ir laisvėms apsaugoti pagal šį reglamentą;
 - 10.6.4. kai taikoma, duomenų apsaugos pareigūno kontaktinius duomenis;
 - 10.6.5. poveikio duomenų apsaugai vertinimą; ir
 - 10.6.6. bet kokią kitą priežiūros institucijos prašomą informaciją.
- 10.7. Prireikus Bendrovė atlieka peržiūrą, kad įvertintų, ar duomenys tvarkomi laikantis PDAV, ypatingai tais atvejais, kai pakinta tvarkymo operacijų keliamas pavojus.

11. BAIGIAMOSIOS NUOSTATOS

- 11.1. Reikalavimai nustatyti Reglamente taikytini nuo 2018 m. gegužės 25 d.
- 11.2. Visi priedai prie Politikos yra laikomi sudėtine Politikos dalimi.
- 11.3. Ši Politika, jos papildymai ir / ar pakeitimai įsigalioja juos patvirtinus Bendrovės vadovo / jo įgalioto asmens.
- 11.4. Bendrovės darbuotojai ar kiti asmenys, įgalioti tvarkyti darbuotojų asmens duomenis su Politika supažindinami pasirašytinai ar kitomis elektroninėmis priemonėmis, kuriomis gali būti fiksuojamas susipažinimo faktas.
- 11.5. Kandidatai į darbuotojus, kurių duomenys tvarkomi Bendrovėje, gali supažindinami su Politika Bendrovės Personalo skyriuje.
- 11.6. Pagrindines asmens duomenų tvarkymo, asmens duomenų subjekto teisių įgyvendinimo technines ir organizacines priemones, naudojant informacines sistemas bei duomenų bazes, nustato šių sistemų nuostatai, duomenų saugos nuostatai bei kiti teisės aktai.
- 11.7. Šios Politikos nesilaikymas, atsižvelgiant į pažeidimo sunkumą, gali būti laikomas darbo pareigų pažeidimu, už kurį darbuotojams gali būti taikoma atsakomybė, numatyta Lietuvos Respublikos darbo kodekse. Kiti asmenys, veikiantys kitų teisinių santykių pagrindu, už asmens teisių pažeidimus atsako sutartyse ir taikytinose teisės normose nustatyta tvarka.
- 11.8. Šioje Politikoje nurodytos tik svarbiausios asmens duomenų saugumo priemonės, kurių privaloma laikytis tvarkant asmens duomenis. Siekdama užtikrinti aukštesnį duomenų apsaugos lygį, Bendrovė turi teisę imtis papildomų apsaugos priemonių.
- 11.9. Bendrovė turi teisę pakeisti Politiką supažindinant darbuotojus ir kitus asmenis, įgaliotus tvarkyti asmens duomenis, pasirašytinai ar kitomis elektroninėmis priemonėmis, kuriomis gali būti fiksuojamas susipažinimo faktas.
- 11.10. Bendrovėje periodiškai, ne rečiau kaip kartą per 2 (dvejus) metus arba įsigaliojus teisės aktų pakeitimams, atliekamas Politikos ir jos nuostatų vykdymo kontrolės peržiūrėjimas, esant poreikiui Politika yra atnaujinama ir patvirtinama Bendrovės vadovo ar jo įgalioto asmens.

KANDIDATO Į DARBUOTOJUS SUTIKIMAS DĖL ASMENS DUOMENŲ TVARKYMO

(data)

Aš, _____,

(kandidato vardas, pavardė)

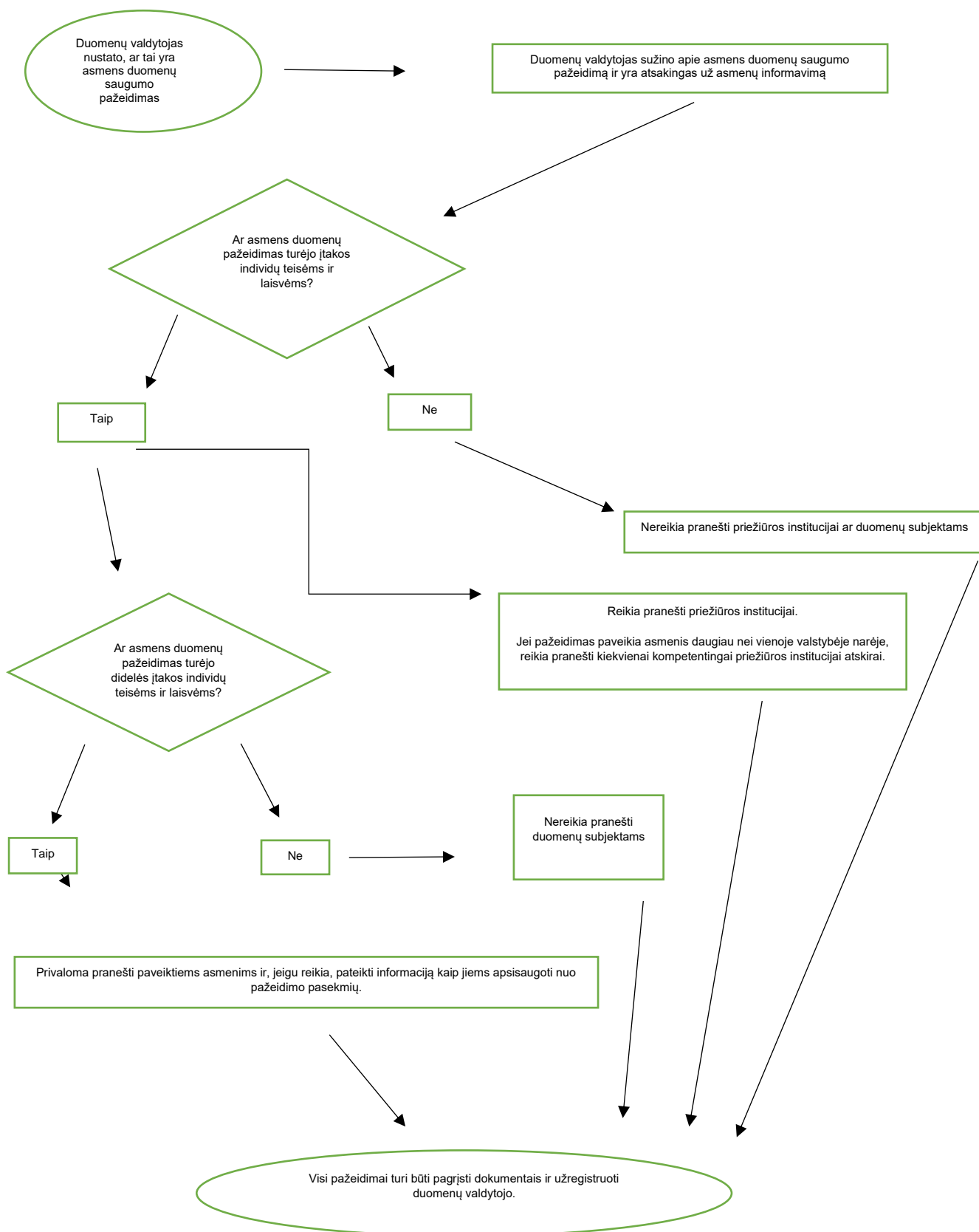
1. Sutinku, kad **Daiktų saugojimo centras, UAB**, kodas 304784517, (Bendrovė) tvarkytų šiuos mano asmens duomenis:
 - 1.1. vardą ir pavardę;
 - 1.2. išsilavinimą;
 - 1.3. profesinę kvalifikaciją;
 - 1.4. telefono numerį;
 - 1.5. elektroninio pašto adresą.
2. Mano asmens duomenys bus naudojami siekiant atrinkti tinkamiausią darbuotoją Bendrovei ir pateikti pasiūlymus dėl darbo vietų Bendrovėje.
3. Mano asmens duomenis galima tvarkyti _____ .
(trukmė)
4. Esu informuotas, kad galiu bet kada išreikšti nesutikimą tvarkyti mano asmens duomenis šiame sutikime nurodytais tikslais, informuodamas apie nesutikimą elektroniniu paštu: [nurodyti kontaktinį paštą] arba pateikdamas atsisakymą raštu Bendrovės Personalo skyriui.
5. Mano asmens duomenys bus tvarkomi Daiktų saugojimo centras, UAB Asmens duomenų saugojimo politikoje ir jos įgyvendinimo priemonėse nustatyta tvarka.

Kandidato į darbuotojus _____

(parašas)

(vardas, pavardė)

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMO NUSTATYMO IR PRANEŠIMO PROCEDŪRA



Sužinoję apie asmens duomenų saugumo pažeidimą – sureaguokite kaip įmanoma greičiau ir nedelsdami informuokite Atsakingą asmenį arba Bendrovės vadovą.

Atsakingas asmuo arba Bendrovės vadovas ar jų įgaliotas asmuo turi užpildyti šias lenteles. Jei lenteles pildo ne Atsakingas asmuo, lenteles užpildęs asmuo turi pateikti Atsakingam asmeniui el. pašto adresu: viskastilps@boxinn.lt.

Asmens duomenų saugumo pažeidimo nustatymo forma vidiniam naudojimui	
Asmens, pildančio asmens duomenų saugumo pažeidimo formą, kontaktiniai duomenys	
Saugumo pažeidimo data, laikas (jei žinoma)	
Kaip sužinojote apie saugumo pažeidimą?	
Saugumo pažeidimo vieta	
Saugumo pažeidimo aplinkybės / detalizavimas	
Nurodykite duomenų subjektų kategorijas ir apytikslį skaičių	
Nurodykite duomenų įrašų kategorijas ir apytikslį skaičių	
Ar saugumo pažeidimas susijęs su šiais asmens duomenimis:	
rasine ar etnine kilme	
politinėmis pažiūromis, religiniais ar filosofiniais įsitikinimais	
naryste profesinėse sąjungose	
genetiniais, biometriniais duomenimis, sveikatos duomenimis	
lytiniu gyvenimu ar lytine orientacija	
apkaltinamaisiais nuosprendžiais ar nusikalstamomis veikomis	
pažeidžiamais suaugusiais asmenimis ar vaikais	

Dėl saugumo pažeidimo asmens duomenys gali būti panaudoti tapatybės vagystei (pvz.: pasinaudota asmenine banko sąskaita, pasu ir pan.)	
Ar duomenų subjektai žino apie saugumo pažeidimą?	
Kokių priemonių ėmėtės, kad sumažinti žalą / neigiamas pasekmes duomenų subjektams?	
Sekantys reikalingi veiksmai/rekomendacijos:	
Pranešimų apie pažeidimą fiksavimas	
Pranešta Valstybinei asmens duomenų inspekcijai (priežiūros institucijai)	<p style="text-align: center;">Taip/Ne</p> <p style="text-align: center;"><i>Jei taip, kada pranešta (data):</i></p> <p style="text-align: center;">Detalės:</p>
Pranešta asmenims, kurių duomenys atskleisti:	<p style="text-align: center;">Taip/Ne</p> <p style="text-align: center;"><i>Jei taip, kada pranešta (data):</i></p> <p style="text-align: center;">Detalės:</p>
Pranešta kitiems suinteresuotiems asmenims / institucijoms (pvz., policijai)	<p style="text-align: center;">Taip/Ne</p> <p style="text-align: center;"><i>Jei taip, kada pranešta (data):</i></p> <p style="text-align: center;">Detalės:</p>

Pranešimo apie asmens duomenų saugumo pažeidimą priežiūros institucijai forma

Atsakingas asmuo arba Bendrovės vadovas privalo pateikti priežiūros institucijai nedelsiant ir, jei įmanoma, ne vėliau kaip 72 (septyniasdešimt dvi) valandas pranešimą apie asmens duomenų saugumo pažeidimą. Pranešime turi būti pateikta žemiau nurodyta informacija.

Kontroliniai klausimai	Šią skiltį pildo Atsakingas asmuo / Bendrovės vadovas / jų įgaliotas asmuo:
Duomenų valdytojas	
Duomenų apsaugos pareigūno (jei toks yra) arba kito atsakingo kontaktinio asmens, kuris gali priežiūros institucijai suteikti daugiau informacijos, duomenys:	<i>[vardas, pavardė, el. paštas, telefonas].</i>
Kada buvo nustatytas asmens duomenų saugumo pažeidimas?	
Kada įvyko asmens duomenų saugumo pažeidimas?	
Pažeidimo vieta	
Asmens, kuris pranešė apie pažeidimą, vardas ir pavardė, kontaktiniai duomenys	
Trumpas pažeidimo aprašymas	
Nurodykite duomenų subjektų kategorijas ir apytikslį skaičių	
Nurodykite duomenų įrašų kategorijas ir apytikslį skaičių	
Nurodykite tikėtinas asmens duomenų saugumo pažeidimo pasekmes	
Nurodykite priemones, kurių ėmėsi, ar pasiūlė imtis duomenų valdytojas, kad būtų pašalintas asmens duomenų saugumo pažeidimas, įskaitant priemones neigiamoms pasekmėms sumažinti.	
PRIEŽIŪROS INSTITUCIJOS NAUDOJIMUI	
Pranešimą priėmė	
Priėmimo data ir laikas	
Asmuo, į kurį nukreipta	

Nukreipimo data ir laikas	
----------------------------------	--

[PROJEKTO PAVADINIMAS]
POVEIKIO DUOMENŲ APSAUGAI VERTINIMO ATASKAITA

[DATA]

1. Poreikio atlikti Poveikio duomenų apsaugai vertinimą (PDAV) nustatymas. Atrankos klausimai.

Klausimai yra skirti padėti nuspręsti ar PDAV reikalingas. Kiekvienas atsakymas "taip", į bet kuriuos iš pateiktų klausimų, yra požymis, kad PDAV jums būtų naudingas. Visų pirma, įsivertinkite, ar projektu bus renkami asmens duomenys, ar renkami nauju tikslu, ar bus tvarkomi nauju būdu, kurio anksčiau nenaudojote. Plėtojantis projektui, jūs galėsite pildyti savo atsakymus. Jeigu vertindami projektą pastebėsite, kad jums labiau tinka kiti patikros metodai, jūs galite keisti šiuos patikros metodus.

Nr.	Klausimai	Taip	Ne
1.1.	Ar projekto metu bus vykdomas sistemingas ir išsamus su fiziniiais asmenimis susijusių asmeninių aspektų vertinimas, kuris yra grindžiamas automatizuotu tvarkymu, įskaitant profiliavimą, ir kuriuo remiantis priimami sprendimai, kuriais padaromas su fiziniu asmeniu susijęs teisinis poveikis arba kurie daro panašų didelį poveikį fiziniam asmeniui (pvz., nagrinėjami ar prognozuojami su asmens darbo rezultatais, ekonomine padėtimi, sveikatos būkle, asmeniniais pomėgiais ar interesais, patikimumu arba elgesiu, vieta arba judėjimu susiję aspektai)?	<input type="checkbox"/>	<input type="checkbox"/>
1.2.	Ar projektu metu bus vykdomas sistemingas viešos vietos stebėjimas dideliu mastu?	<input type="checkbox"/>	<input type="checkbox"/>
1.3.	Ar informacija apie asmenis bus atskleista organizacijoms ar asmenims, kurie anksčiau neturėjo pastovios prieigos prie asmens duomenų?	<input type="checkbox"/>	<input type="checkbox"/>
1.4.	Ar projekto metu asmens duomenys bus tvarkomi nauju tikslu ar nauju būdu, kurio Bendrovė anksčiau nenaudojo?	<input type="checkbox"/>	<input type="checkbox"/>
1.5.	Ar projekto metu jūs naudosite naują technologiją, kuri galimai pažeistų privatumą? Pavyzdžiui, biometrinės ar veido atpažinimo technologijos.	<input type="checkbox"/>	<input type="checkbox"/>
1.6.	Ar projekto metu jūs priimsite asmenų atžvilgiu sprendimus / imsitės veiksmų, kurie darytų lemiamą poveikį tiems asmenims?	<input type="checkbox"/>	<input type="checkbox"/>
1.7.	Ar informacija apie asmenis galimai padidins susirūpinimą privačiais duomenimis? Pvz.: sveikatos išrašai, kriminaliniai išrašai ar kita informacija, kurią asmuo norėtų laikyti privačia.	<input type="checkbox"/>	<input type="checkbox"/>
1.8.	Ar projekto metu jūs kontaktuosite su asmenimis taip, kad toks elgesys galėtų būti palaikytas privatumo pažeidimu?	<input type="checkbox"/>	<input type="checkbox"/>

2. Projekto detalės

Žemiau esančioje lentelėje pateikiama pagrindinė projekto informacija:

Pagrindinė informacija		
2.1.	Duomenų valdytojas	<i>Organizacijos pavadinimas</i> <i>Organizacija, kuri atliks šį duomenų poveikio privatumui vertinimą, paprastai bus suprantama kaip duomenų valdytojas, tačiau esant daugiau valdytojų, ar esant kitų aplinkybių, pažymėkite tai šioje skiltyje.</i>
2.2.	Projekto aprašymas	<i>Trumpai aprašykite, koks tai projektas. Pvz., darbuotojų darbo vietos vaizdo stebėjimas, siekiant apsaugoti turtą ir asmenų saugumą.</i>
2.3.	Projekto tikslas	<i>Užtikrinti turto ir asmenų apsaugą.</i>
2.4.	Kontekstas, apimtis ir pagrindas	<i>Turėkite omenyje, kad čia turi būti numatyta ne tik pati apimtis ir kontekstas, bet ir trumpi jų aprašymai.</i>
2.5.	Duomenų subjektai	<i>Subjektai, kuriems yra rengiamas poveikio privatumui vertinimas, pvz.:</i> <ul style="list-style-type: none"> • <i>Darbuotojams</i> • <i>Klientams</i> • <i>Partneriams</i> • <i>Konsultantams</i> • <i>Kandidatams</i>
2.6.	Asmens duomenų rūšys	<i>Vaizdo stebėjimo lauke esantys vaizdai.</i>
2.7.	Specialių kategorijų duomenys	<i>Specialių kategorijų duomenys nėra numatyti.</i> <i>Pakeiskite, jei jūs tvarkote specialių kategorijų duomenis, tokius kaip rasė, religija, ar kiti jautrūs duomenys.</i>
2.8.	Apibūdinkite, kaip juda asmens duomenys sistemoje	<i>Pvz., vaizdo stebėjimo duomenys įrašomi ir 2 mėnesius saugomi Bendrovės duomenų saugykloje. Suėjus saugojimo terminui, ištrinami.</i>
2.9.	Asmens duomenų gavėjai: kas turės galimybę matyti duomenis ir prieigą prie vertinimo rezultatų	<i>Užpildykite, kas turės galimybę matyti asmens duomenis, pavyzdžiui, jūsų vidaus komanda ir bet kokie išorėje veikiantys duomenų tvarkytojai, kurie galės susipažinti su asmens duomenimis.</i>

3. Privatumo vertinimas

Bendrovė turės vadovautis teisės aktuose ir Politikoje nustatytais principais ir teisiniais pagrindais tvarkant asmens duomenis. Ši dalis leis sprendimus priimantiems asmenims įvertinti, ar projektas atitinka teisės aktus ir Politiką.

Sekančioje lentelėje kiekvienoje eilutėje bus apibūdinami esminiai kiekvieno iš principų reikalavimai ir išskirti pagrindiniai klausimai bei jums reikšmingi aspektai. Prie kiekvieno principo pasižymėkite, ar projektas jį atitinka ar ne. Atsižvelgdami į rekomendacijas, pasitvirtinkite veiksmų planą, paskirkite atsakingą asmenį ir rekomendacijų įgyvendinimo terminą. Jeigu jums patogiau, rekomendacijas, veiksmų planą, atsakingus asmenis ir rekomendacijų įgyvendinimo terminus, galite surašyti atskiroje lentelėje.

Nr.	Privatumo principo apibūdinimas	Asmens duomenų tvarkymo proceso santrauka	Atitikimo BDAR vertinimas	Rizikos vertinimas	Rekomendacijos, skirtos sumažinti poveikį privatumui
1.	Sąžiningumo ir teisėtumo principas	<p><i>Kaip asmenys bus informuoti apie jų asmens duomenų naudojimą?</i></p> <p><i>Ar jums reikia pakeisti privatumo pranešimus?</i></p> <p><i>Ar jūs nustatėte, kokios sąlygos bus taikomos duomenų tvarkymui?</i></p> <p><i>Jei jūs remiatės sutikimu dėl asmens duomenų tvarkymo, tai kaip tokia informacija bus renkama ir ką jūs darysite nesutikimo atveju?</i></p>			
2.	Tikslo apribojimo principas Rinkti tik tą informaciją, kurios tikrai reikia	<p><i>Identifikuokite kiekvieną asmens duomenų elementą ir įsitinkinkite, kad tai yra būtina projektui įgyvendinti.</i></p> <p><i>Koks asmens duomenų rinkimo tikslas?</i></p> <p><i>Kaip tai paveiks Bendrovę daryti tai, kas yra būtina?</i></p> <p><i>Ar jūs tikrai renkate tik tą informaciją, kurios jums reikia? Pvz., ar jums tikrai reikia „gimimo datos“ ar „amžiaus“, jei būtų pakankama „pilnametis asmuo“?</i></p>			

Nr.	Privatumo principo apibūdinimas	Asmens duomenų tvarkymo proceso santrauka	Atitikimo BDAR vertinimas	Rizikos vertinimas	Rekomendacijos, skirtos sumažinti poveikį privatumui
3.	<p>Duomenų mažinimo principas</p> <p>Tvarkoma asmeninė informacija turėtų būti adekvati, susijusi ir neperteklinė atsižvelgiant į informacijos gavimo tikslą.</p>	<p><i>Kokių asmens duomenų naudojimo galėtumėte išvengti, tačiau tai nepakenktų projektui?</i></p> <p><i>Būkite atviri dėl informacijos turėjimo ir naudojimo tikslų.</i></p> <p><i>Ar to tikisi duomenų subjektas?</i></p> <p><i>Ar naudojate informaciją kitam tikslui, negu tam, kuriam ją gavote? Jei taip, kokia to pateisinama priežastis?</i></p>			
4.	<p>Tikslumo principas</p> <p>Asmens duomenys turi būti tvarkomi tiksliai ir, esant poreikiui, turi būti atnaujinami.</p>	<p><i>Ar įsigijus naują programinę įrangą, jums leidžiama esant būtinybei pakeisti duomenis?</i></p> <p><i>Kaip jūs užtikrinate, kad iš fizinių asmenų ar kitų organizacijų gauti duomenys yra tikslūs?</i></p> <p><i>Aktualūs veiksniai: Koks yra procesas, norint patikrinti ar gauta informacija yra teisinga?</i></p> <p><i>Ar informacija buvo pateikta tiesiogiai pačio asmens?</i></p> <p><i>Ar informacija buvo patikrinta tiesiogiai su pačiu pateikusiu asmeniu?</i></p> <p><i>Ar šis procesas automatizuotas, ar jūs turite galimybę remtis žmogaus sprendimais?</i></p> <p><i>Kaip bus atlyginama žala asmenims tais atvejais, kai informacija yra neteisinga ar klaidinanti? (Kuo didesnė žala bus sukeliama, tuo išsamesnė patikra turi būti vykdoma, nustatant informacijos tikslumą)</i></p> <p><i>Kaip Bendrovė spręs klausimą dėl reikalavimų pakeisti asmens duomenis?</i></p>			

Nr.	Privatumo principo apibūdinimas	Asmens duomenų tvarkymo proceso santrauka	Atitikimo BDAR vertinimas	Rizikos vertinimas	Rekomendacijos, skirtos sumažinti poveikį privatumui
5.	<p>Saugojimo trukmės apribojimo principas</p> <p>Asmeninė informacija panaudojama tam tikriems tikslams ir nebeturi būti ilgiau laikoma, jeigu tai nebereikalinga tų tikslų pasiekimui.</p>	<p><i>Koks informacijos saugojimo laikas yra tinkamas?</i></p> <p><i>Ar yra kokių nors įsipareigojimų saugoti informaciją tam tikrą laiką pagal teisinį reguliavimą? Jei tokio įsipareigojimo nėra, kas būtų laikoma protingu laikotarpiu informacijos laikymui?</i></p> <p><i>Kaip jūs sunaikinsite nereikalingus asmens duomenis</i></p> <p><i>Ar jūs esate įsigijęs programinę įrangą, kuri leis ištrinti informaciją?</i></p> <p><i>Kai informacija dalinamasi su trečiaja šalimi, apsvarstykite, kiek ilgai jie galės turėti informaciją ir kam bei kaip jūs užtikrinsite, kad informacija bus sunaikinta po to, kai panaudota verslo tikslais.</i></p>			
6.	<p>Tinkamos techninės ir organizacinės priemonės turėtų būti tokios, kad užkirstų kelią neteisėtam duomenų panaudojimui, praradimui.</p>	<p><i>Kokie mokymai ir instrukcijos yra reikalingi užtikrinti, kad darbuotojai žinotų, kaip saugiai ir taisyklingai naudoti naująją sistemą?</i></p> <p><i>Turi būti keli skirtingi metodai, kurie padėtų jums užtikrinti asmens duomenų, kuriuos jūs turite, saugumą, tokie kaip: vidinės tvarkos ir taisyklės, kurios reglamentuoja, kaip darbuotojai užtikrina asmens duomenų saugumą. Naudinga pateikti nuorodas į dokumentus ar informaciją, kurioje aprašoma plačiau.</i></p> <p><i>Apsauga galėtų susidaryti iš: fizinės apsaugos; IT apsaugos; darbuotojų mokymų; reguliavimų, kuriuos turi stebėti darbuotojai; konfidencialumo išlygos sutartyse ir pan.</i></p>			

Nr.	Privatumo principo apibūdinimas	Asmens duomenų tvarkymo proceso santrauka	Atitikimo BDAR vertinimas	Rizikos vertinimas	Rekomendacijos, skirtos sumažinti poveikį privatumui
7.	<p>Asmens duomenų šaltinis</p> <p>Gaunamas tiesiogiai iš asmenų, kuriuos liečia, jei tai įmanoma.</p>	<p><i>Kaip informacija yra renkama ir iš kokių subjektų?</i></p> <p><i>Jei asmeninė informacija yra surenkama iš kito šaltinio, o ne iš duomenų subjekto, tai įvertinkite, ar tai tinkama ir teisėta?</i></p>			
8.	<p>Duomenų subjektų teisės</p> <p>Prieiga prie asmeninės informacijos.</p>	<p><i>Kaip pranešate duomenų subjektams, kad jų informacija yra renkama, ką su ja ruošiamasi daryti, ar tai privaloma ar ne ir kokios pasekmės, jeigu jie nesuteikia tokios informacijos?</i></p> <p><i>Ko imasi Bendrovė, kad suteiktų galimybę asmeniui susipažinti su savo informacija ir kaip Bendrovė susitvarko su užklausu peržiūrėti informaciją?</i></p> <p><i>Ar sistema gali būti sutvarkyta taip, jog asmenims būtų lengva gauti informaciją apie juos, pvz., sistema sugeneruoja informaciją apie asmenį pateiktus užklausus?</i></p>			
9.	<p>Asmens duomenų rinkimo būdas</p>	<p><i>Čia turėtų būti apibūdinta, kaip informacija yra renkama ir turi būti įvertinta, ar rinkimo metodai yra tinkami ir teisingi pagal aplinkybes.</i></p>			

Nr.	Privatumo principo apibūdinimas	Asmens duomenų tvarkymo proceso santrauka	Atitikimo BDAR vertinimas	Rizikos vertinimas	Rekomendacijos, skirtos sumažinti poveikį privatumui
10.	<p>Asmens duomenų perdavimo / atskleidimo apribojimai</p> <p>Atskleidimas leidžiamas tik tada, kai tam yra tinkama priežastis, nebent yra išimčių</p>	<p><i>Reikia įvardinti tikslą, kuriuo asmens duomenys yra atskleidžiami. Įvardykite kiekvieną subjektą, kuris gaus tą informaciją.</i></p> <p><i>Ar atskleidimas yra vienas iš tikslų, kuriuo asmens duomenys buvo surinkti? Jei taip, ar duomenų subjektas buvo apie tai informuotas?</i></p> <p><i>Jei atskleidžiate asmens duomenis kitu tikslu negu numatyta, ar yra kažkokia išimtis pateisinti jūsų veiksmus?</i></p>			
11.	<p>Asmens duomenys neturėtų būti perduoti už Europos Ekonominės Zonos (EEE) ribų, nebent ta teritorija užtikrina saugų duomenų apsaugos lygį ir asmens teisių bei laisvių apsaugą.</p>	<p><i>Ar projektas reikalauja perduoti duomenis už EEZ ribų?</i></p> <p><i>Jei vis dėlto bus vykdomi duomenų perdavimai, kaip jūs užtikrinsite, kad duomenys yra tinkamai apsaugojami?</i></p>			

4. Išvados ir rekomendacijų, skirtų sumažinti poveikį privatumui, įgyvendinimo veiksmų planas.

Nr.	Rekomendacijos, skirtos sumažinti poveikį privatumui	Patvirtintas veiksmų planas	Atsakingas asmuo	Užbaigimo data

Duomenų valdytojo, Daiktų saugojimo centras, UAB, juridinio asmens kodas 304784517, registruotos buveinės adresas Saliamono Banaičio g. 12, Vilnius, kontaktai el. p.: viskastilps@boxinn.lt, tel.: +370686 88951 veiklos įrašai

Nr.	Duomenų tvarkymo tikslai	Duomenų subjektų kategorijos	Duomenų kategorijos	Tvarkymo teisinis pagrindas	Duomenų gavėjai	Duomenų perdavimas į trečiąsias valstybes/tarptautines organizacijas /perdavimo dokumentas	Duomenų saugojimo terminai	Techninės ir organizacinės priemonės
	Nurodykite konkretų duomenų tvarkymo tikslą. Jei tie patys duomenys tvarkomi keliais tikslais, pildykite atskiras eilutes.	Pvz., darbuotojas, klientas, kt.	Pvz., vardas, pavardė, el. paštas, kt.	Pvz., sutikimas, teisinė prievolė, sutartis, teisėtas interesas.	Nurodykite prieigos gavėjus Bendrovės viduje ir išorėje, pvz., Personalo skyriaus vadovas, buhalterinės apskaitos įmonė.	Nurodykite valstybę, organizaciją ir duomenų perdavimo dokumentą.	Nurodykite konkretų saugojimo terminą. Jei neįmanoma, pateikite kriterijus tam laikotarpiui nustatyti.	Pvz., ribota prieiga, duomenų šifravimas, atsarginių kopijų darymas ir pan.

Duomenų valdytojo, Daiktų saugojimo centras, UAB, juridinio asmens kodas 304784517, registruotos buveinės adresas Saliamono Banaičio g. 12, Vilnius, kontaktai el. p.: viskastilps@boxinn.lt, tel.: +370686 88951 veiklos įrašai

Nr.	Duomenų valdytojo pavadinimas, kontaktiniai duomenys (duomenų apsaugos pareigūnas, jei yra)	Duomenų tvarkymo kategorijos	Nuoroda į sutartį su duomenų valdytoju	Duomenų perdavimas į trečiąsias valstybes/tarptautines organizacijas/perdavimo dokumentas	Techninės ir organizacinės priemonės
Pvz.		Pvz., darbo užmokestis, buhalterinė apskaita, turto valdymas ir kt.	Saugojimo paslaugų sutartis Nr. [...] ir Susitarimas dėl asmens duomenų tvarkymo	Nurodykite valstybę, organizaciją ir duomenų perdavimo dokumentą.	Pvz., ribota prieiga, duomenų šifravimas, atsarginių kopijų darymas ir pan.