PATVIRTINTA
uždarosios akcinės bendrovės „Grinda“ direktoriaus
2025 m. gegužės 9 d. įsakymu Nr. V-25-0069

UŽDAROSIOS AKCINĖS BENDROVĖS „GRINDA“ ASMENS DUOMENŲ APSAUGOS POLITIKA

I SKYRIUS BENDROSIOS NUOSTATOS

1. Ši Uždarosios akcinės bendrovės „Grinda“ (toliau – Bendrovė) asmens duomenų apsaugos politika (toliau – Politika) nustato Bendrovės asmens duomenų tvarkymo tikslus bei principus, reglamentuoja tokių duomenų rinkimo, naudojimo ir saugojimo tvarką, įtvirtina duomenų subjektų teises bei nustato jų įgyvendinimą, taip pat nustato Bendrovės naudojamas asmens duomenų saugumo užtikrinimo technines ir organizacines priemones.

2. Ši Politika yra privaloma visiems Bendrovės darbuotojams. Bendrovė ir kiekvienas Bendrovės darbuotojas, kuriam yra suteikta teisė tvarkyti asmens duomenis, privalo laikytis konfidencialumo ir užtikrinti, kad Bendrovės tvarkomi asmens duomenys išliktų konfidencialūs visą jų tvarkymo laikotarpį ir jam pasibaigus.

3. Pažeidus 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentą (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrąjį duomenų apsaugos reglamentą) (toliau – BDAR) ar šią Politiką, Politikos 1 punkte nurodytiems asmenims gali būti taikoma drausminė ir (ar) civilinė atsakomybė. Jei tam yra pagrindas, taip pat gali būti taikoma sutartinė, administracinė ar baudžiamoji atsakomybė ir apie tokį įvykį (jei egzistuoja pagrindas) gali būti pranešama teisėsaugos institucijoms, priežiūros institucijai ir bet kuriai kitai kompetentingai įstaigai.

4. Šios Politikos tikslai yra:

4.1. nustatyti asmens duomenų tvarkymo, įskaitant saugojimą, Bendrovėje bendruosius principus ir taisykles;

4.2. įgyvendinti BDAR įtvirtintus realios asmens duomenų apsaugos ir atskaitomybės principus;

4.3. palengvinti tinkamą BDAR, Lietuvos Respublikos Asmens duomenų teisinės apsaugos įstatymo (toliau – Įstatymas), kitų Europos Sąjungos ir Lietuvos Respublikos teisės aktų, reglamentuojančių asmens duomenų apsaugą, reikalavimų įgyvendinimą;

4.4. sukurti tarpusavio supratimą bei teisinį aiškumą tarp Bendrovės ir jos darbuotojų dėl veiksmų, kuriais Bendrovė siekia apsaugoti tvarkomus asmens duomenis;

4.5. padėti Bendrovės darbuotojams įgyvendinti Teisės aktų reikalavimus.

II SKYRIUS POLITIKOJE NAUDOJAMOS SĄVOKOS

5. Toliau nurodytos sąvokos šioje Politikoje turi šias reikšmes, išskyrus atvejus, kai kontekstas reikalauja kitos reikšmės:

5.1. **Teisės aktai** – visi Bendrovei taikomi duomenų apsaugos teisės aktai, įskaitant BDAR, Įstatymą ir kitus Bendrovei taikomus nacionalinius ir tarptautinius teisės aktus.

5.2. **Įstatymas** – Lietuvos **Respublikos** asmens duomenų teisinės apsaugos įstatymas.

5.3. **Duomenų subjektas –** fizinis asmuo, kurio tapatybę galima nustatyti (tiesiogiai ir netiesiogiai), visų pirma pagal **identifikatorių**, kaip antai vardą ir pavardę, asmens identifikavimo numerį, buvimo vietos duomenis ir interneto identifikatorių arba pagal vieną ar kelis to fizinio asmens fizinės, fiziologinės, genetinės, psichinės, ekonominės, kultūrinės ar socialinės tapatybės požymius.

5.4. **Asmens duomenys** arba **Duomenys** – bet kokia informacija apie fizinį asmenį, kurio tapatybė nustatyta arba kurio tapatybę **galima** nustatyti (Duomenų subjektą).

5.5. **Duomenų subjekto prašymas** arba **Prašymas** – bet kuris iš žemiau nurodytų:

5.5.1. prašymas būti informuotam ir susipažinti su Duomenimis apie Duomenų subjektą;

5.5.2. prašymas ištaisyti netikslius Duomenų subjekto Duomenis;

5.5.3. prašymas ištrinti Duomenis apie Duomenų subjektą;

5.5.4. prašymas apriboti Duomenų apie Duomenų subjektą tvarkymą;

5.5.5. prašymas perkelti Duomenis apie Duomenų subjektą;

5.5.6. prieštaravimas dėl Duomenų apie Duomenų subjektą tvarkymo Bendrovėje, kai Duomenys tvarkomi tam, kad būtų įvykdyta viešojo intereso užduotis arba dėl Bendrovės teisėto intereso;

5.5.7. prašymas atšaukti sutikimą, jeigu Duomenų subjekto Duomenys Bendrovėje tvarkomi sutikimo pagrindu;

5.5.8. prieštaravimas dėl bet kokio automatinio sprendimo priėmimo dėl Duomenų subjekto ar Duomenų subjekto profiliavimo Bendrovėje (jei taikoma);

5.5.9. Bet kuris kitas prašymas ir (arba) skundas dėl bet kokio klausimo, susijusio su Duomenų apsauga Bendrovėje.

6. **Duomenų subjektų prašymų valdymas** – procesas, kuriuo metu analizuojami, tiriami Bendrovėje gauti Duomenų subjekto prašymai ir j juos atsakoma.

7. **Bendrovė** – UAB „Grinda“, atsakinga už Duomenų rinkimą, naudojimą ir saugojimą, Teisės aktų laikymąsi. Teisės aktuose apibrėžiama kaip duomenų valdytojas.

8. **Darbuotojas** – bet kuris Bendrovės darbuotojas, praktikantas, savanoris, arba kitas personalo narys, prilyginamas darbuotojui, ir turintis tiesioginę ar netiesioginę prieigą prie Duomenų.

9. **Duomenų apsaugos pareigūnas** – Bendrovės skiriamas darbuotojas arba išorės paslaugų teikėjas (fizinis arba juridinis asmuo), padedantis Bendrovei užtikrinti teisinę atitiktį Teisės aktams, prižiūrintis visus su Duomenų apsauga susijusius klausimus Bendrovėje.

10. **Duomenų tvarkymas –** bet kokia automatizuotomis arba neautomatizuotomis priemonėmis su Duomenimis ar Duomenų rinkiniais atliekama operacija ar operacijų seka, kaip antai rinkimas, įrašymas, rūšiavimas, sisteminimas, saugojimas, adaptavimas ar keitimas, išgava, susipažinimas, naudojimas, atskleidimas persiunčiant, platinant ar kitu būdu sudarant galimybę jais naudotis, taip pat sugretinimas ar sujungimas su kitais duomenimis, apribojimas, ištrynimas arba sunaikinimas.

11. **Poveikio duomenų apsaugai vertinimas (PDAV) –** pasitelktos priemonės ir vertinimai duomenų tvarkymo veiklos rizikai nustatyti ir sumažinti. PDAV gali būti vykdomas kaip

pritaikytosios asmens duomenų apsaugos dalis ir turi būti atliekamas visoms pagrindinėms sistemoms ar esminiams verslo pokyčiams, susijusiems su duomenų tvarkymu.

12. **IKT** – Informacinės ir komunikacinės technologijos, kurias Bendrovė suteikia Darbuotojams arba kurias Darbuotojai naudoja siekdami atlikti savo pareigas Bendrovėje, įskaitant, bet neapsiribojant, kompiuteriais, planšetiniais kompiuteriais, išmaniaisiais telefonais, USB įrenginiais ar kitomis duomenų laikmenomis, nutolusiomis duomenų saugyklomis, interneto svetainėmis bei kita programine įranga.13. **Asmens duomenų saugumo pažeidimas** – bet kuris iš toliau nurodytų įvykių:

12.1. Bendrovės IKT, dokumentų ir (arba) kitų priemonių, kuriuose yra Duomenų, praradimas, vagystė arba nesuplanuotas sunaikinimas;

12.2. atsitiktinis ar tyčinis Duomenų siuntimas, įkėlimas ar dalinimasis su trečiaisiais asmenimis, neturinčiais teisės jų gauti;

12.3. trečiųjų asmenų neteisėta prieiga prie Bendrovės IKT, dokumentų ir (ar) kitu priemonių, kuriose yra Duomenų;

12.4. kenkėjiškos atakos prieš Bendrovės IKT ir (ar) kitas priemones, kuriose yra Duomenų;

12.5. klaidos, susijusios su kuriamomis, naudojamomis ir konfigūruojamomis IKT ir (ar) kitomis priemonėmis, kurios gali kelti pavojų Asmens duomenų saugumui;

12.6. bet kokie kiti saugumo pažeidimai, lemiantys atsitiktinį ar neteisėtą Duomenų sunaikinimą, praradimą, nutekėjimą, pakeitimą, neleistiną atskleidimą arba prieigos prie Bendrovei perduodamų, saugojamų ar kitaip renkamų, naudojamų ar saugojamų Duomenų suteikimą.

13. **Asmens duomenų saugumo pažeidimo valdymas** – procesas, kurio metu Bendrovėje analizuojami, registruojami Asmens duomenų saugumo pažeidimai ir, jei reikia, teikiami pranešimai Inspekcijai ar Duomenų subjektams, kurių Duomenys buvo paveikti.

14. **Duomenų tvarkymo veiklos įrašai** – elektroninis dokumentas, išsamiai apibūdinantis Bendrovėje renkamus, naudojamus ir saugomus Duomenis.

15. **EEE** – Europos Ekonominė Erdvė (visos ES valstybės narės bei Islandija, Norvegija, Lichtenšteinas).

16. **Inspekcija** – nepriklausoma valdžios institucija, kurią pagal BDAR 51 straipsnį įsteigė ES valstybė narė. Lietuvos Respublikoje priežiūros institucija yra Valstybinė duomenų apsaugos inspekcija, L. Sapiegos g. 17, LT-10312 Vilnius, Lietuvos Respublika, tel. Nr. +370 5 271 2804 / 279 1445, el. paštas ada@ada.lt.

17. **Inspekcijos paklausimas** – bet kuris laiškas, pranešimas, užklausa ar kitas dokumentas, kurį pateikia Valstybinė duomenų apsaugos inspekcija ir kuris yra adresuotas Bendrovei.

18. **Inspekcijos paklausimų valdymas –** procesas, kurio metu nagrinėjami Inspekcijos paklausimai, renkama atsakymui reikalingai informacija ir Inspekcijai pateikiamas atsakymas.

19. **Specialių kategorijų asmens duomenys –** Teisės aktuose nurodyti duomenys, kurių tvarkymui keliami padidinti reikalavimai (pvz., duomenys, atskleidžiantys rasinę ar etninę kilmę, politines pažiūras, religinius ar filosofinius įsitikinimus ar narystę profesinėse sąjungose, sveikatos duomenys arba duomenys apie fizinio asmens lytini gyvenimą ir lytinę orientaciją, genetiniai, biometriniai identifikatoriai, duomenys apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas).

20. **Paslaugų teikėjas** – konkretus paslaugos teikėjas ar kitas išorės juridinis ar fizinis asmuo, kuris turi prieigą prie Bendrovės Duomenų ir juos tvarko pagal Bendrovės nurodymus. Teisės aktuose apibrėžiamas kaip duomenų tvarkytojas.

21. **Politika –** ši Asmens duomenų apsaugos politika.

22. **Tretieji asmenys** – visi fiziniai arba juridiniai asmenys, išskyrus Darbuotojus.

23. Kitos šioje Politikoje neapibrėžtos sąvokos suprantamos taip, kaip jos apibrėžtos Teisės aktuose.

24. Administracijos darbuotojai su šia Politika yra supažindinami vidine duomenų valdymo sistema, o kiti darbuotojai (pvz. darbininkai) supažindinami pasirašytinai.

III SKYRIUS
DUOMENŲ TVARKYMO PRINCIPAI

25. Duomenys Bendrovėje turi būti tvarkomi vadovaujantis šiais principais:

25.1. Asmens duomenys Duomenų subjekto atžvilgiu turi būti tvarkomi teisėtu, sąžiningu ir skaidriu būdu (teisėtumo, sąžiningumo ir skaidrumo principas). Bendrovė gali rinkti, tvarkyti ir dalintis Asmens duomenimis tik skaidriai bei teisėtai ir aiškiai apibrėžtais tikslais. Pagal BDAR tvarkyti Asmens duomenis galima tik turint tinkamą teisinį pagrindą, pvz.:

25.1.1. Duomenų subjektas davė sutikimą, kad jo Asmens duomenys būtų tvarkomi vienu ar keliais konkrečiais tikslais,

25.1.2. tvarkyti Duomenis būtina siekiant įvykdyti sutartį, kurios šalis yra Duomenų subjektas, arba siekiant imtis veiksmų Duomenų subjekto prašymu prieš sudarant sutartį,

25.1.3. tvarkyti Duomenis būtina, kad būtų įvykdyta Bendrovei taikoma teisinė prievolė,

25.1.4. tvarkyti Duomenis būtina siekiant apsaugoti gyvybinius Duomenų subjekto ar kito fizinio asmens interesus,

25.1.5. tvarkyti Duomenis būtina siekiant atlikti užduotį, vykdomą viešojo intereso labui arba vykdant Bendrovei pavestas viešosios valdžios funkcijas,

25.1.6. tvarkyti Duomenis būtina siekiant teisėtų Bendrovės arba trečiosios šalies interesų, išskyrus atvejus, kai tokie Duomenų subjekto interesai arba pagrindinės teisės ir laisvės, dėl kurių būtina užtikrinti Asmens duomenų apsaugą, yra už juos viršesni, ypač kai Duomenų subjektas yra vaikas.

25.1.7. Bendrovė taip pat gali tvarkyti Specialiųjų kategorijų asmens duomenis, jei taikomas bent vienas iš šios Politikos 25.1 punkte nurodytų pagrindų bei BDAR 9 straipsnyje nustatyta išimtis, pvz., Darbuotojų Specialių kategorijų asmens duomenys, įskaitant sveikatos duomenis, gali būti tvarkomi tik ta apimtimi, kiek yra būtina siekiant įgyvendinti teises ar pareigas darbo ir socialinės apsaugos teisės srityse arba pagal kolektyvines sutartis; kitų asmenų Specialiųjų kategorijų asmens duomenys – tik ta apimtimi, kiek Duomenų subjektas galėjo laisvai pasirinkti, ar duoti sutikimą tvarkyti Specialiųjų kategorijų asmens duomenis, be jokių neigiamų pasekmių Duomenų subjektui bei davė tokį sutikimą raštu arba elektronine forma. Duomenys apie Duomenų subjektų ar Trečiųjų asmenų teistumą gali būti tvarkomi tik, kai tai numato specialūs teisės aktai ir tik ta apimtimi, kiek tai reikalinga atitinkamų teisės aktų įgyvendinimui, pvz., prireikus tokių Duomenų viešajame pirkime ar projekto konkurse.

25.1.8. Bendrovė kiekvienai duomenų tvarkymo operacijai turi nustatyti bei dokumentuoti tinkamą teisinį pagrindą.

25.1.9. Pagal BDAR privaloma Duomenų subjektui pateikti detalią, konkrečią informaciją priklausomai nuo to, ar Duomenys gauti tiesiogiai iš Duomenų subjekto, ar iš kitų šaltinių. Ši informacija turi būti pateikta glausta, skaidria, suprantama ir lengvai prieinama forma, aiškia ir

paprasta kalba tam, kad Duomenų subjektas galėtų lengvai ją suprasti. Duomenų subjektams pateiktinos informacijos sąrašas yra nurodytas BDAR 13-14 straipsniuose.

25.1.10. Jei (a) pradedama nauja Duomenų tvarkymo operacija, (b) pasikeičia jau vykdoma Duomenų tvarkymo operacija, arba (c) nutraukiama bet kokia Duomenų tvarkymo operacija, apie tokius pasikeitimus privaloma nedelsiant informuoti Duomenų apsaugos pareigūną bei iš anksto juos suderinti (jai to nėra įmanoma padaryti iškart – nedelsiant, kai tai tampa įmanoma).

25.1.11. Jei Bendrovė siekia tvarkyti Asmens duomenis sutikimo pagrindu, prašymas duoti sutikimą pateikiamas tokiu būdu, kad jis būtų aiškiai atskirtas nuo kitų klausimų, pateiktas suprantama ir lengvai prieinama forma, aiškia ir paprasta kalba. Tam, kad sutikimas būtų teisėtas, jis privalo būti laisvai duotas, konkretus, informuotas ir nedviprasmiškas.

25.1.12. Laikoma, kad Duomenų subjektas suteikė sutikimą, jei jis tai išreiškia pareiškimu ar aktyviais veiksmais. Teisėtas sutikimas reikalauja aktyvaus Duomenų subjekto veiksmo, tad tylėjimas, iš anksto pažymėti langeliai ar neveikimas nėra laikomi sutikimu.

25.1.13. Duomenų subjektai turi teisę bet kada atšaukti savo sutikimą ir Bendrovė privalo nedelsiant nutraukti sutikimu grįstą Asmens duomenų tvarkymą. Atšaukti sutikimą turi būti taip pat lengva kaip jį duoti. Sutikimo atšaukimas nedaro poveikio sutikimu pagrįsto Duomenų tvarkymo, atlikto iki sutikimo atšaukimo, teisėtumui.

25.1.14. Jei Bendrovė ketina tvarkyti Duomenis kitu ir nesuderinamu tikslu, kuris nebuvo nurodytas Duomenų subjektui duodant pirminį sutikimą, reikia gauti naują sutikimą.

25.1.15. Bendrovė privalo registruoti gautus sutikimus, kad galėtų įrodyti savo atitiktį susijusiems reikalavimams.

25.1.16. Jei atitinkama Asmens duomenų tvarkymo operacija yra grindžiama sutikimu, Darbuotojai, prieš pradėdami atitinkamą Duomenų tvarkymą, privalo įsitikinti, jog yra gautas šios Politikos 25.1.10-25.1.12 punktuose nurodytus reikalavimus atitinkantis sutikimas.

25.2. Asmens duomenys turi būti renkami nustatytais, aiškiai apibrėžtais bei teisėtais tikslais ir toliau netvarkomi su tais tikslais nesuderinamu būdu (tikslo apribojimo principas):

25.2.1. Darbuotojai privalo užtikrinti, kad Asmens duomenys gali būti renkami tik nustatytais, aiškiais apibrėžtais bei teisėtais tikslais ir toliau netvarkomi su tais tikslais nesuderinamu būdu, pvz., jei Asmens duomenys renkami siekiant iš atitinkamo asmens įsigyti paslaugas, jie negali būti naudojami siunčiant jam tiesioginės rinkodaros pranešimus;

25.2.2. Bendrovė negali naudoti Asmens duomenų naujais, skirtingais ar nesuderinamais tikslais palyginus su tais, kurie buvo atskleisti Duomenų subjektams renkant Asmens duomenis, nebent Bendrovė apie tai informavo Duomenų subjektus ir jie davė naują sutikimą, kai būtina.

25.3. Asmens duomenys tyri būti adekvatūs, tinkami ir tik tokie, kurių reikia siekiant tikslų, dėl kurių jie tvarkomi (duomenų kiekio mažinimo principas):

25.3.1. Darbuotojai gali tvarkyti Asmens duomenis tik tada ir tik tokia apimtimi, kai tai reikalinga jų darbo funkcijoms atlikti. Draudžiama tvarkyti Asmens duomenis su darbo funkcijomis nesusijusiais tikslais;

25.3.2. Darbuotojai privalo užtikrinti, kad renkami Asmens duomenys nėra pertekliniai ir yra būtini konkretiems tikslams;

25.3.3. Darbuotojai privalo užtikrinti, kad tuo atveju, jei Asmens duomenys nebėra reikalingi konkretiems tikslams, jie bus ištrinami arba nuasmeninti;

25.3.4. Darbuotojai privalo užtikrinti, kad nėra renkami pertekliniai Asmens duomenys, pvz., jei Duomenys renkami siekiant sudaryti sutartį, darbuotojai negali prašyti nesusijusių,

perteklinių Asmens duomenų, pvz., nuotraukos, nebent tai būtina kitam Asmens duomenų tvarkymo tikslui ir egzistuoja tinkamas teisinis pagrindas.

25.4. Asmens duomenys turi būti tikslūs ir prireikus atnaujinami; turi būti imamasi visų pagrįstų priemonių užtikrinti, kad asmens duomenys, kurie nėra tikslūs, atsižvelgiant į jų tvarkymo tikslus, būtų nedelsiant ištrinami arba ištaisomi (tikslumo principas):

25.4.1. Asmens duomenys turi būti tikslūs ir, kai būtina, atnaujinami. Jei nustatomi neatitikimai, būtina ištaisyti arba ištrinti susijusius Asmens duomenis.

25.4.2. Bendrovė turi pareigą patikrinti Asmens duomenų tikslumą juos renkant bei periodiškai jų tvarkymo laikotarpiu. Be to, Bendrovė privalo imtis pagrįstų veiksmų, kad būtų ištrinti ar ištaisyti netikslūs ar pasenę Asmens duomenys.

25.5. Asmens duomenys turi būti laikomi tokia forma, kad Duomenų subjektų tapatybę būtų galima nustatyti ne ilgiau nei tai yra būtina tais tikslais, kuriais Asmens duomenys yra tvarkomi (saugojimo trukmės apribojimo principas):

25.5.1. Bendrovė turi pareigą užtikrinti, kad Asmens duomenys būtų ištrinami arba nuasmeninami, kai jie nebėra reikalingi tais tikslais, kuriais yra tvarkomi, nebent taikomi teisės aktai nustato konkretų Asmens duomenų saugojimo laikotarpį (pvz., Vidaus dokumentų saugojimo terminų rodyklė (Lietuvos vyriausiojo archyvaro tarnyba, Valstybės žinios, 2011 m. kovo 17 d., Nr. 32-1534)). Ši pareiga taip pat apima ir prievolę informuoti trečiąsias šalis apie poreikį ištrinti Duomenis, kai taikoma.

25.5.2. Bendrovė taip pat privalo informuoti Duomenų subjektus apie Asmens duomenų saugojimo laikotarpį.

25.5.3. Jei atitinkami Asmens duomenys nėra ištrinami automatiškai, Darbuotojai turi pasirūpinti, kad Asmens duomenys būtų negrįžtamai ištrinti pagal šios Politikos 26.5.1. nurodytus reikalavimus.

25.6. Asmens duomenys turi būti 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):

25.6.1. Asmens duomenys turi būti apsaugoti nuo neteisėto ar neteisėto tvarkymo, taip pat nuo netyčinio praradimo, sunaikinimo ar sugadinimo atitinkamomis techninėmis ir organizacinėmis priemonėmis.

25.6.2. Bendrovė nustato, įgyvendina ir taiko apsaugos priemones, atitinkančias jos dydį, apimtį ir veiklą, turimus išteklius, Asmens duomenų, kuriuos ji valdo ar tvarko kitų vardu, kiekį ir nustatytas rizikas (įskaitant šifravimo ir pseudonimizacijos naudojimą, kai taikoma). Konkretūs reikalavimai, susiję su tokiomis apsaugos priemonėmis, yra pateikiami atskiruose Bendrovės dokumentuose, reglamentuojančiuose informacijos saugumo reikalavimus (pvz., Bendrovės duomenų tvarkymo veiklos įrašuose, Kibernetinio ir informacijos saugumo politikoje, Informacinių technologijų saugumo taikymo, valdymo ir atsakomybių paskirstymo taisyklėse).

25.6.3. Bendrovė reguliariai vertina ir tikrina šios Politikos 25.6.2. punkte nurodytų apsaugos priemonių efektyvumą, kad užtikrintų Duomenų tvarkymo saugumą;

25.6.4. Bendrovė gali perduoti Asmens duomenis tik tiems trečiųjų šalių paslaugų teikėjams, kurie įsipareigoja laikytis reikalaujamos tvarkos ir procedūrų bei sutinka imtis atitinkamų priemonių, kurių reikalauja Bendrovė;

25.6.5. Bendrovė užtikrina Asmens duomenų saugumą, saugodama asmens duomenų konfidencialumą, vientisumą ir prieinamumą: (a) konfidencialumas reiškia tai, kad tik tie asmenys, kuriems būtina žinoti atitinkamus Asmens duomenis, gali juos pasiekti ir naudoti, b) vientisumas reiškia tai, kad asmens duomenys turi būti tikslūs ir tinkami tikslui, dėl kurio yra tvarkomi, c) prieinamumas reiškia tai, kad įgalioti naudotojai turi turėti prieigą prie asmens duomenų, kai ji yra reikalinga nustatytiems tikslams.

25.7. Bendrovė yra atsakinga už tai, kad būtų laikomasi aukščiau šiame Politikos skyriuje nurodytų principų, ir turi sugebėti įrodyti, kad jų laikomasi (atskaitomybės principas). Jei Bendrovė pažeis nors vieną iš aukščiau nurodytų principų, toks duomenų tvarkymas bus laikomas pažeidžiančiu BDAR reikalavimus.

25.8. Jei Bendrovės Darbuotojas turi bet kokių abejonių dėl šiame Politikos skyriuje nurodytų principų įgyvendinimo, turi nedelsiant kreiptis į Duomenų apsaugos pareigūną.

IV SKYRIUS
DUOMENŲ TVARKYMO VEIKLOS ĮRAŠAI

26. Siekdama užtikrinti Duomenų tvarkymo teisėtumą, Bendrovė sudaro Duomenų tvarkymo veiklos įrašus, kuriuose nurodoma, įskaitant, bet neapsiribojant:

26.1. Duomenų subjektų kategorijos;

26.2. Asmens duomenų kategorijos;

26.3. Asmens duomenų tvarkymo tikslai ir teisinis pagrindas;

26.4. Asmens duomenų gavėjų kategorijos;

26.5. Asmens duomenų saugojimo terminai;

26.6. kitą informacija, susijusi su Asmens duomenų tvarkymu, nurodyta BDAR 30 straipsnyje, ar pateikiama Bendrovės nuožiūra.

V SKYRIUS
BENDROSIOS DARBUOTOJŲ PAREIGOS DUOMENŲ APSAUGOS SRITYJE

27. Kiekvienas Darbuotojas privalo:

27.1. tvarkydamas Duomenis, įsitikinti, kad yra laikomasi visų reikalavimų, numatytų šioje Politikoje;

27.2. tvarkyti Duomenis tik tam, kad atliktų savo darbo funkcijas, ir tik ta apimtimi, kiek tai reikalinga jų vykdymui;

27.3. visais atvejais identifikuoti Duomenis, kurie yra tvarkomi Darbuotojo veikloje bei žinoti, kad veiklai, susijusiai su Duomenimis, yra taikomi šios Politikos ir Teisės aktų reikalavimai;

27.4. visais atvejais įsitikinti, kad tvarkoma Duomenų kategorija yra įtraukta į Duomenų tvarkymo veiklos įrašus, o Duomenų tvarkymo tikslas atitinka bent vieną iš Duomenų tvarkymo veiklos įrašuose nurodytų tikslų; apie poreikį tvarkyti naujas Duomenų kategorijas ir (ar) naujais tikslais informuoti Bendrovės Duomenų apsaugos pareigūną. Duomenų apsaugos pareigūnas įvertina poreikį informuoti Bendrovės vadovą ir, prireikus, informuoja;

27.5. visais atvejais prieš perduodant Duomenis Tretiesiems asmenims įsitikinti, kad tokia Duomenų gavėjų kategorija yra įtraukta į Duomenų tvarkymo veiklos įrašus, o jei ketinama Duomenis perduoti Duomenis už EEE ribų – kad atitinkamas Duomenų gavėjas yra įtrauktas į

Duomenų tvarkymo veiklos įrašus; apie poreikį perduoti Duomenis Duomenų tvarkymo veiklos įrašuose nenurodytai Duomenų gavėjų kategorijai arba už EEE ribų veikiančiam Trečiajam asmeniui, nenurodytam Duomenų tvarkymo veiklos įrašuose, informuoti Duomenų apsaugos pareigūną. Duomenų apsaugos pareigūnas įvertina poreikį informuoti Bendrovės vadovą ir, prireikus, informuoja;

27.6. įsitikinti, kad kiekvienas Duomenų subjektas, su kuriuo jie susiduria pirmą sykį Bendrovėje, buvo informuotas apie jo Duomenų tvarkymą, o Duomenų tvarkymo veiklos įrašuose numatytais atvejais yra davęs sutikimą Duomenų tvarkymui; jei Duomenų subjektas nebuvo informuotas apie jo Duomenų tvarkymą ir(ar) nebuvo gautas jo sutikimas, įteikti informacinį pranešimą ir (ar) paprašyti Duomenų subjekto sutikimo;

27.7. atsižvelgiant į atliekamų darbo funkcijų pobūdį imtis protingų pastangų, kad užtikrintų, jog visi Bendrovėje valdomi Duomenys būtų tikslūs ir prireikus atnaujinami;

27.8. tvarkydami Duomenis, elgtis rūpestingai ir atsargiai, turint omenyje tai, kad Darbuotojo veiksmai, susiję su Duomenimis, kelia pavojų Bendrovei ir Duomenų subjektams;

27.9. įgyvendinti ir naudoti technines ir organizacines Duomenų apsaugos priemones, užtikrinančias Duomenų apsaugą nuo neleistinos prieigos, neteisėto rinkimo, naudojimo ir saugojimo, netyčinio praradimo, sunaikinimo ar sugadinimo, kaip tai nustatyta šioje Politikoje ir kituose Bendrovės dokumentuose;

27.10. neatskleisti informacijos apie Bendrovės taikomas technines ir organizacines Duomenų apsaugos priemones, įskaitant bet neapsiribojant Bendrovės vidaus dokumentais, jokiems Tretiesiems asmenims, prieš tai neįsitikinus jų teise ir teisėtu pagrindu gauti tokią informaciją;

27.11. nesaugoti Asmens duomenų jokiose Darbuotojui priklausančiose asmeninėse atmintinėse, kompiuterinėje ar programinėje įrangoje (internetinėse duomenų saugyklose, atmintinėse, kompiuteriuose, telefonuose ir pan.), nebent konkrečiu atveju Bendrovė leistų Darbuotojui naudoti konkrečias asmenines priemones darbo funkcijų vykdymui;

27.12. kreiptis į Duomenų apsaugos pareigūną ir gauti jo konsultaciją:

27.12.1. esant bet kokiems netikslumams, abejonėms ar klausimams, susijusiems su šios Politikos taikymu, aiškinimu, pažeidimu ar atitikimu Politikai;

27.12.2. ketinant Bendrovėje sukurti, diegti ar naudoti naujas IKT ir (ar) kitus metodus Duomenų tvarkymui;

27.12.3. ketinant pirmą kartą Bendrovėje pasitelkti naują Paslaugų teikėją.

27.12.4. su Duomenų subjektų prašymais elgtis rūpestingai ir atidžiai; gavę bet kokį Duomenų subjekto prašymą nedelsdami, ne vėliau kaip per 3 (tris) darbo dienas nuo Duomenų subjekto prašymo gavimo, pranešti apie tai Duomenų apsaugos pareigūnui;

27.13. nedelsiant, bet ne vėliau kaip per 12 (dvylika) valandų, sužinoję apie Asmens duomenų saugumo pažeidimą:

27.13.1. informuoti Bendrovės direktorių ir Duomenų apsaugos pareigūną apie Asmens duomenų saugumo pažeidimą;

27.13.2. imtis pagrįstų veiksmų, kad Asmens duomenų saugumo pažeidimas būtų sustabdytas;

27.13.3. imtis pagrįstų veiksmų, kad Asmens duomenų saugumo pažeidimas nepasikartotų (situacijos analizė, pakartotinis rizikos įvertinimas, pakartotiniai darbuotojų mokymai ir pan.).

27.14. bendradarbiauti su Duomenų apsaugos pareigūnu, kitais Darbuotojais ir (ar) Paslaugų teikėjais atliekant Asmens duomenų saugumo pažeidimo valdymą.

28. Nė vienam Darbuotojui neturi būti suteikta prieiga prie Duomenų, jei šie Duomenys nėra reikalingi jų darbo funkcijoms atlikti.

VI SKYRIUS
DUOMENŲ SUBJEKTŲ TEISIŲ ĮGYVENDINIMAS

29. Darbuotojas, gavęs Duomenų subjekto prašymą, nedelsdamas, ne vėliau kaip per 1 (vieną) darbo dieną nuo Duomenų subjekto prašymo gavimo dienos kreipiasi į Duomenų apsaugos pareigūną.

30. Kiekvienas Duomenų subjekto prašymas turi būti registruojamas Duomenų subjektų prašymų registre.

31. Duomenų apsaugos pareigūnas atlieka gautų Duomenų subjektų prašymų valdymą vadovaudamasis šia Politika ir Teisės aktais:

31.1. peržiūri prašymą;

31.2. nustato prašymą pateikusio Duomenų subjekto tapatybę – siekdama užtikrinti duomenų apsaugą ir tinkamai įgyvendinti duomenų subjektų teises, Bendrovė turi teisę prašyti duomenų subjektų pateikti savo tapatybės įrodymą (pvz., kai Prašymas teikiamas elektroninių ryšių priemonėmis, jis turi būti pasirašytas elektroniniu parašu), jei Bendrovė negali identifikuoti prašymą pateikusio asmens. Šiuo atveju Bendrovė neturi teisės prašyti perteklinės informacijos, pvz., asmens tapatybės kortelės/paso kopijos gali būti prašoma tik labai išimtiniais ir pagrįstais atvejais, pvz., jei Duomenų subjektas prašo informacijos apie savo Specialiųjų kategorijų asmens duomenis;

31.3. surenka prašymo nagrinėjimui reikalingą informaciją;

31.4. įvertina prašymo teisinį pagrįstumą;

31.5. paruošia ir pateikia Duomenų subjektui atsakymą į prašymą; ir

31.6. esant reikalui duoda reikiamus pavedimus Darbuotojams dėl prašymą pateikusio Duomenų subjekto Duomenų tolesnio tvarkymo.

31.7. Jei Duomenų apsaugos pareigūnas nustato, kad reikalinga papildoma informacija iš Darbuotojų, Trečiųjų asmenų ir (ar) Duomenų subjekto, pateikusio prašymą, Duomenų apsaugos pareigūnas prašo pateikti šią informaciją, o Darbuotojai per nedelsdami per protingą terminą Duomenų apsaugos pareigūnui pateikia bet kurią informaciją, kurios yra prašoma.

32. Duomenų apsaugos pareigūnas užtikrina, kad:

32.1. Duomenų subjekto prašymą būtų atsakyta per 1 (vieną) mėnesį nuo jo gavimo dienos; jei Duomenų subjektų prašymų sudėtingumas ar skaičius yra didelis, Duomenų apsaugos pareigūnas turi teisę pratęsti terminą atsakymui pateikti iki 2 (dviejų) mėnesių informuodamas apie tai Duomenų subjektą ir nurodydamas termino pratęsimo priežastis;

32.2. Duomenų subjektui būtų pateikta tik ta informacija, kuri yra susijusi su juo;

32.3. Duomenų subjektui būtų pateikiama tik tiek informacijos, kiek reikalauja Teisės aktai;

32.4. Teisės aktų numatytais atvejais, kai Duomenų subjektas neturi teisės pasinaudoti savo kaip duomenų subjekto teise, Duomenų subjekto prašymas nebūtų tenkinamas;

32.5. Duomenų subjektams nebūtų atskleista jokia Bendrovės konfidenciali informacija, ypatingai Bendrovės komercinės paslaptys.

32.6. Duomenų subjekto prašymą tenkinti atsisakoma, kai:

32.6.1. Duomenų subjekto prašymas nesusijęs su Teisės aktų numatytomis teisėmis;

32.6.2. Duomenų subjekto prašymas susijęs su informacija, kuri nėra Duomenys;

32.6.3. Duomenų subjekto prašymas susijęs su informacija apie kitą Duomenų subjektą;

32.6.4. Duomenų subjektas neturi teisės pasinaudoti atitinkamomis duomenų subjekto teisėmis pagal Teisės aktų nustatytus reikalavimus bei išimtis;

33. Duomenų subjekto prašymas yra akivaizdžiai neproporcingas, įskaitant bet neapsiribojant šiais atvejais:

33.1. Duomenų subjekto prašymas yra pasikartojantis - tas pats Duomenų subjektas jau yra pateikęs tokį patį Prašymą per 1 (vienus) metus iki Prašymo gavimo;

33.2. Duomenų subjekto prašymas susijęs su dideliu kiekiu pasikartojančių Duomenų;

33.3. aplinkybės rodo, kad vienintelis Duomenų subjekto prašymo tikslas yra sutrikdyti Bendrovės veiklą.

34. Duomenų apsaugos pareigūnas į Duomenų subjekto prašymą atsako elektroninėmis priemonėmis glausta ir Duomenų subjektui suprantama forma, vartodamas aiškią ir suprantamą kalbą, išskyrus atvejus, kai Duomenų subjektas prašo žodinio atsakymo ar ne elektroninio atsakymo raštu.

35. Bendrovė turi teisę paprašyti Duomenų subjekto sukonkretinti pateiktą Prašymą, jeigu ji tvarko didelį kiekį susijusios su Duomenų subjektu informacijos ir nėra galimybės jos visos pateikti.

36. Jei Duomenų subjekto prašymą tenkinti atsisakoma visiškai arba iš dalies, atsakyme turi būti nurodomos atsisakymo priežastys ir informuojama apie galimybę pateikti skundą Inspekcijai ir (ar) imtis teisminės gynybos priemonių.

37. Jei Duomenų subjekto prašymas tenkinamas, Duomenų apsaugos pareigūnas koordinuoja ir planuoja Duomenų subjekto prašymo įgyvendinimą Bendrovėje, teikia nurodymus bei konsultacijas Darbuotojams ir Paslaugų teikėjams, kurie turi dalyvauti Duomenų subjekto prašymo įgyvendinime.

VII SKYRIUS
PASLAUGŲ TIEKĖJAI – DUOMENŲ TVARKYTOJAI

38. Bendrovė gali įgalioti duomenų tvarkytojus – pvz., informacinių, buhalterinių ir elektroninių ryšių Paslaugų teikėjus ir kitus asmenis, kurie tvarko Bendrovės valdomus Asmens duomenis jos nustatytais tikslais ir pagal jos nurodymus – tvarkyti Bendrovės valdomus Asmens duomenis.

39. Darbuotojas, prieš ketindamas pasitelkti Paslaugos teikėją, privalo:

40. patikrinti ir įsitikinti, kad Paslaugų teikėjas imasi tinkamų techninių ir organizacinių Duomenų apsaugos priemonių ir atitinka kitus Teisės aktų reikalavimus. Kilus klausimams, darbuotojas konsultuojasi su Duomenų apsaugos pareigūnu;

41. pasirūpinti, kad Bendrovė prieš dalindamasi Duomenimis su Paslaugų teikėju sudarytų su juo Asmens duomenų tvarkymo sutartį (arba įtrauktų atitinkamas nuostatas į esamas sutartis, įskaitant paslaugų teikimo sąlygas), kurioje nustatoma, kad duomenų tvarkytojai tvarko Duomenis tik pagal Bendrovės nurodymus. Tokios sutartys turi apimti visus BDAR ir Teisės aktuose nustatytus reikalavimus; (sutarties forma pridedama kaip Politikos 1 priedas).

42. Jei Paslaugų teikėjas pateikia Bendrovei savo Asmens duomenų tvarkymo sutarties formą, įskaitant paslaugų teikimo sąlygas, tokiais atvejais darbuotojas, prieš ketindamas pasitelkti

Paslaugos teikėją, privalo pranešti apie tai Duomenų apsaugos pareigūnui. Duomenų apsaugos pareigūnas, prieš Bendrovei sudarant tokią sutartį, turi įsitikinti, kad ji atitinka Teisės aktų nustatytus reikalavimus.

43. Darbuotojai turi prisidėti užtikrinant, kad tvarkydami Duomenis duomenų tvarkytojai laikytųsi šiame Politikos skyriuje nurodytų reikalavimų. Kilus įtarimams, kad duomenų tvarkytojai nesilaiko nurodytų reikalavimų, šie įtarimai turi būti nedelsiant adresuojami Duomenų apsaugos pareigūnui.

44. Prieš perduodant Asmens duomenis naujam duomenų tvarkytojui, Darbuotojai privalo užtikrinti, kad yra vykdomi visi šiame Politikos skyriuje nurodyti reikalavimai.

VIII SKYRIUS
DUOMENŲ PERDAVIMAS

45. Paprastai Bendrovėje nėra leidžiama dalytis duomenimis su trečiosiomis šalimis, išskyrus atvejus, kai įdiegtos tam tikros apsaugos priemonės ir Duomenų subjektui apie tokį perdavimą iš anksto pranešta laikantis šioje Politikoje nustatytų reikalavimų.

46. Paprastai Darbuotojai gali dalytis turimais Duomenimis su kitais Darbuotojais tik tada, jei šios informacijos žinojimas yra būtinas darbo funkcijoms atlikti.

47. Bendrovė taip pat gali dalintis Asmens duomenimis su Paslaugų teikėjais, jei tenkinamos visos šios sąlygos:

47.1. jie turi žinoti atitinkamus Asmens duomenis, kad galėtų teikti paslaugas pagal sutartį;

47.2. Duomenų perdavimas atitinka Duomenų subjektui pateiktą informaciją ir, jei reikia, gautas Duomenų subjekto sutikimas;

47.3. Paslaugų teikėjas sutiko laikytis reikiamų Asmens duomenų saugumo standartų ir procedūrų bei imtis tinkamų saugumo priemonių,;

47.4. perdavimas atitinka visus taikomus tarpvalstybinio duomenų perdavimo apribojimus, ir sudaryta BDAR reikalavimus atitinkanti sutartis, kurioje aptarti Asmens duomenų perdavimo klausimai.

47.5. Asmens duomenų perdavimas į trečiąją valstybę (už EEE ribų) arba tarptautinei organizacijai gali būti vykdomas, jei Europos Komisija nusprendžia, kad trečioji valstybė, teritorija ar vienas ar keli tam tikri sektoriai trečiojoje valstybėje arba atitinkamoje tarptautinėje organizacijoje užtikrina tinkamą apsaugos lygį (sprendimas dėl tinkamumo).

47.6. Tuo atveju, jei gavėjo atžvilgiu nėra priimtas sprendimas dėl tinkamumo, Bendrovė gali perduoti Asmens duomenis į trečiąją valstybę arba tarptautinei organizacijai tik tuo atveju, jei numatytos atitinkamos apsaugos priemonės, ir su sąlyga, kad yra užtikrinamos Duomenų subjekto teisės ir veiksmingos teisių gynimo priemonės. Šios aplinkybės turėtų būti vertinamos kiekvienu konkrečiu atveju jei nėra sprendimo dėl tinkamumo.

47.7. Prieš atliekant bet kokį Asmens duomenų perdavimą į trečiąją valstybę arba tarptautinei organizacijai, jei nėra priimtas sprendimas dėl tinkamumo, privaloma apie tai informuoti Duomenų apsaugos pareigūną ir gauti jo patvirtinimą.

47.8. Tuo atveju, jei nėra sprendimo dėl tinkamumo, Bendrovė gali pasitelkti šias apsaugos priemones:

47.8.1. įmonėms privalomas taisykles pagal BDAR 47 straipsnį;

47.8.2. standartines duomenų apsaugos sąlygas, kurias priėmė Europos Komisija;

47.8.3. standartines duomenų apsaugos sąlygas, kurias priėmė priežiūros institucija ir patvirtino Europos Komisija;

47.8.4. patvirtintą elgesio kodeksą pagal BDAR 40 straipsnį kartu su privalomais ir vykdytinais duomenų valdytojo arba duomenų tvarkytojo trečiojoje valstybėje įsipareigojimais taikyti tinkamas apsaugos priemones, be kita ko, susijusias su duomenų subjektų teisėmis;

47.8.5. patvirtintą sertifikavimo mechanizmą pagal BDAR 42 straipsnį kartu su privalomais ir vykdytinais duomenų valdytojo arba duomenų tvarkytojo įsipareigojimais trečiojoje valstybėje taikyti tinkamas apsaugos priemones, be kita ko, susijusias su duomenų subjektų teisėmis.

47.8.6. Bendrovė taip pat gali remtis BDAR 49 straipsnyje įtvirtintomis nuostatomis, konkrečiais atvejais leidžiančiomis nukrypti nuo aukščiau aptartų reikalavimų. Šios nuostatos negali būti taikomos reguliariems ir sisteminiams Asmens duomenų perdavimams.

IX SKYRIUS
DARBUOTOJŲ STEBĖSENOS IR KONTROLĖS DARBO VIETOJE TVARKA

48. Duomenys apie Darbdaviui priklausančių Darbuotojo žinioje esančių transporto priemonių, kitų įrenginių buvimo vietą (lokaciją) gali būti renkami ir tvarkomi Duomenų tvarkymo veiklos įrašuose numatytais tikslais ir teisiniais pagrindais laikantis šių taisyklių:

48.1. Darbuotojas yra informuojamas apie transporto priemonių, kitų įrenginių lokacijos nustatymą perduodant atitinkamą transporto priemonę ar kitą įrengimą Darbuotojo žinion;

48.2. Jei Darbuotojui transporto priemone yra leidžiama naudotis ne darbo laiku, Darbuotojui parodoma, kaip išjungti lokaciją, tačiau išjungti lokaciją yra leidžiama tik ne darbo laiku (visas komandiruotės laikas šiuo tikslu yra laikomas darbo laiku);

48.3. Duomenys apie transporto priemonių ar kitų įrengimų lokaciją yra prieinami tik Darbuotojams, pagal atliekamų funkcijų pobūdį atsakingiems už Duomenų tvarkymo veiklos įrašuose numatytų lokacijos duomenų tvarkymo tikslų įgyvendinimą;

48.4. Duomenys apie transporto priemonių ar kitų įrengimų lokaciją gali būti panaudoti kaip įrodymas nustatant Darbuotojo darbo pareigų pažeidimus.

49. Vaizdo stebėjimo duomenys gali būti renkami išskirtinai siekiant apsaugoti Darbdavio turtą nuo vagysčių ir panašių nusikaltimo požymių turinčių veikų laikantis šių taisyklių:

49.1. 50.1. Vaizdo stebėjimo kameros ir jų stebima teritorija paženklinama aiškiai matomais ir suprantamais ženklais, juose turi būti nuoroda, kur galima susipažinti su stebėjimo duomenimis ir jų tvarkymo sąlygomis;

49.2. Vaizdo stebėjimas organizuojamas Bendrovei patvirtinus atskiras vaizdo duomenų tvarkymo taisykles;

49.3. Vaizdo stebėjimo duomenys yra prieinami tik specialiai Darbdavio paskirtam Darbuotojui (-ams) arba Bendrovei saugos paslaugas teikiančiai Bendrovei; nustatęs įtariamą vagystę ar panašią nusikaltimo požymių turinčią veiką, už vaizdo stebėjimą atsakingas asmuo perduoda atitinkamą vaizdo įrašo fragmentą Bendrovės vadovui ar kitam jo paskirtam Darbuotojui; kai įtariamas Darbuotojas, jis yra supažindinamas su atitinkamu vaizdo įrašo fragmentu ir jo paprašoma pateikti paaiškinimus, kitais atvejais Bendrovės vadovo sprendimu atitinkamas vaizdo įrašo fragmentas yra perduodamas teisėsaugos institucijoms;

49.4. Vaizdo stebėjimo duomenys saugomi 14 kalendorinių dienų, išskyrus atvejus, kai jų prireikia siekiant pareikšti reikalavimus ar gintis nuo reikalavimų, pareikštų teisme, baudžiamojo proceso, administracinėje ar kitokioje teisinėje procedūroje;

49.5. Vaizdo stebėjimo duomenys gali būti panaudoti kaip įrodymas nustatant Darbuotojo darbo pareigų pažeidimus tik ta apimtimi, kiek tokie pažeidimai turi vagystės ar panašių nusikalstamų veikų požymių.

50. Bendrovė, siekdama valdyti savo IKT infrastruktūrą bei užtikrinti jos saugumą, suteikia nuotolinio prisijungimą prie savo IKT (kompiuterių, planšečių, telefonų ir pan.) jų techninę priežiūrą vykdantiems Darbuotojams arba išoriniams paslaugų teikėjams – programinės įrangos diegimui, atnaujinimui, gedimų šalinimui ir panašios techninės pagalbos darbams. Nors šiuo atveju nėra renkama įrenginyje saugoma informacija, teikiant techninę priežiūrą gali būti nustatyti Darbuotojo darbo pareigų pažeidimai (pvz., neteisėtai instaliuota programinė įranga) ir tokia informacija gali būti panaudota kaip įrodymas nustatant Darbuotojo darbo pareigų pažeidimus.

51. Darbuotojo susirašinėjimo su kitais Darbuotojais ir Trečiaisiais asmenimis (klientais, tiekėjais ir pan.) naudojant Bendrovės elektroninio pašto, socialinių tinklų ar panašią paskyrą Duomenys yra saugomi Bendrovės pasitelkto atitinkamų elektroninių paslaugų tiekėjo informacinėse sistemose siekiant užtikrinti Bendrovės teisėtus interesus - sudarytų sutarčių vykdymą, ypač atsižvelgiant į tai, kad toks susirašinėjimas laikomas sutarčių dalimi, informacijos pateikimą kontrahentams, efektyvų darbo organizavimą, taip pat ir paties Darbuotojo darbo palengvinimui. Šie Duomenys tvarkomi laikantis tokių taisyklių:

51.1. Bendrovės komunikacijos sistemos, įskaitant elektroninį paštą, socialinius tinklus ir pan., technologiškai yra sukurtos informacijos saugojimui, t. y. vien dėl techninių priežasčių jos saugo visą įkeltą informaciją, jei ji nėra specialiai ištrinama;

51.2. Darbuotojai keldami bet kokią informaciją į Bendrovės IKT, įskaitant elektroninių pranešimų siuntimą naudojant Bendrovės elektroninį paštą, socialinių tinklų ir kitas panašias paskyras, gali ir privalo suprasti, kad tokia informacija neišvengiamai bus išsaugota. Darbdavio naudojamos technologijos neleidžia pažymėti keliamos informacijos, įskaitant elektroninio pašto žinutes, kaip asmeninių, todėl įkėlus asmeninio pobūdžio informaciją ji gali būti atsitiktinai tapti žinoma kitiems asmenims. Atitinkamai Darbuotojai neturi naudoti Bendrovės IKT asmeninėms reikmėms, o tą darydami prisiima atitinkamą riziką.

52. Darbuotojo susirašinėjimo Duomenys siekiant užtikrinti Bendrovės veiklos nepertraukiamumą ir tęstinumą yra prieinami atitinkamą Darbuotoją jo atostogų, nedarbingumo ar panašiais laikotarpiais pavaduojantiems Darbuotojams, o taip pat Darbuotojui nutraukus darbo sutartį bus prieinami naujam Darbuotojui, perimsiančiam atleisto Darbuotojo darbą.

53. Darbuotojo susirašinėjimo Duomenys gali būti peržiūrėti atsiradus pagrįstiems įtarimams dėl Darbuotojo konfidencialumo pareigų pažeidimo. Šiuo atveju Bendrovė paskiria ne daugiau trijų Darbuotojų, susipažinsiančių su susirašinėjimo Duomenimis, Darbuotojas yra įspėjamas dėl susirašinėjimo peržiūrėjimo ir, jam pageidaujant, sudaromos galimybės dalyvauti peržiūrint susirašinėjimą. Šiuo atveju faktinių aplinkybių konstatavimui taip pat gali būti pasitelkiamas antstolis.

54. Darbuotojo susirašinėjimo Duomenys gali būti panaudoti kaip įrodymas nustatant Darbuotojo darbo pareigų pažeidimus.

55. Bendrovė nevykdo nuolatinio, sistemingo IKT stebėjimo, t. y. nerenka Darbuotojų Duomenų IKT, tačiau Bendrovės paskirti Darbuotojai turi teisę atlikti IKT patikrinimą, įskaitant

bet neapsiribojant Darbuotojo žinioje esančių kompiuterių, planšetinių kompiuterių ir kitos įrangos patikrinimą, šiais atvejais:

55.1. kai yra nustatoma arba tiriama nusikalstama veika, kiti rimti teisės ir (ar) darbo tvarkos taisyklių pažeidimai;

55.2. kai yra nustatomas arba tiriamas konfidencialios informacijos nutekėjimas, intelektinės nuosavybės pažeidimas ir (ar) nesąžiningos konkurencijos atvejis;

55.3. kai vyksta bylinėjimasis;

55.4. kai reikia atlikti Asmens duomenų saugumo pažeidimo valdymą;

55.5. kai reikia užtikrinti Bendrovės IKT saugumą;

55.6. kitais atvejais, kai Duomenų apsaugos pareigūnas nustato Bendrovės teisėtą interesą dėl IKT tikrinimo.

55.7. Bendrovė tikrina IKT tais atvejais, kai nėra kitų priemonių 55 punkte nurodytiems tikslams pasiekti. Sprendimą dėl IKT tikrinimo priima Bendrovės vadovas (Politikos 2 priedas).

55.8. Tikrindami IKT, Bendrovės paskirti Darbuotojai turi kiek įmanoma labiau sumažinti renkamų, naudojamų ir saugojamų Duomenų kiekį. Tikrindami IKT, Bendrovės paskirti Darbuotojai renka, naudoja ir saugoja tik tokius Duomenis, kurie yra būtini IKT tikrinimui. Jei tikrinant IKT pertekliniai Duomenys buvo surinkti, Darbuotojai nedelsdami juos ištrina.

56. Bendrovės paskirti Darbuotojai gali pradėti tikrinti IKT po to, kai atliko žemiau išvardintus veiksmus:

56.1. nustatė konkrečias priežastis, įtarimus ar informaciją, dėl kurių reikia tikrinti IKT, ir konkrečius IKT tikrinimo tikslus remdamiesi šios Politikos 55 punktu;

56.2. nustatė, kad kitų priemonių pasiekti tikslinimo tikslams nėra arba šios priemonės yra neveiksmingos;

56.3. informavo Duomenų apsaugos pareigūną ir gavo jo konsultaciją dėl numatomo IKT tikrinimo;

56.4. reikiamais atvejais pasitelkė IKT ekspertą ir (ar) antstolį;

56.5. pasirūpino, kad būtų priimtas raštiškas sprendimas dėl IKT tikrinimo.

57. Bendrovės paskirti Darbuotojai turi informuoti konkrečius Darbuotojus, kurių IKT yra tikrinamos, ir sudaryti jiems galimybę stebėti IKT tikrinimą, nebent minėtos informacijos atskleidimas sutrukdytų pasiekti tikrinimo tikslus.

58. Atlikę IKT patikrinimą, Bendrovės paskirti Darbuotojai turi raštu įforminti IKT tikrinimo rezultatus.

X SKYRIUS
ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ VALDYMAS

59. BDAR reikalauja, kad Bendrovė tam tikrais atvejais praneštų apie Asmens duomenų saugumo pažeidimą Inspekcijai ir Duomenų subjektams, pvz., bet kuri iš šių situacijų gali lemti Asmens duomenų saugumo pažeidimą:

59.1. įsilaužimas į kompiuterines sistemas arba Duomenų viliojimo (phishing) atakos;

59.2. Duomenų subjekto informacijos išsiuntimas netinkamam gavėjui, arba įrenginio ar įrašų, kuriuose yra Asmens duomenys, praradimas ar vagystė.

60. Asmens duomenų saugumo pažeidimas paprastai gali būti susijęs su tokiais incidentais:

60.1. **sunaikinimas** – kai Duomenų nebelieka arba jie nebeegzistuoja tokia forma, kuri yra naudinga Bendrovei;

60.2. **žala** – kai Duomenys pakeičiami, sugadinami arba tampa nebeišsamūs,

60.3. **praradimas** – kai Duomenys vis dar gali egzistuoti, tačiau Bendrovė prarado kontrolę ar prieigą prie jų;

60.4. **neteisėtas Duomenų tvarkymas** – tai gali apimti Duomenų atskleidimą (arba prieigą) gavėjams, kurie nėra įgalioti gauti (ar prieiti prie) Duomenų, arba bet kokią kitą Duomenų tvarkymo formą, kuri pažeidžia BDAR reikalavimus.

61. Asmens duomenų saugumo pažeidimai skirstomi pagal šiuos 3 informacijos saugumo principus:

61.1. Asmens duomenų konfidencialumo pažeidimas – neteisėtas ar atsitiktinis Duomenų atskleidimas ar prieigos prie jų suteikimas,

61.2. Asmens duomenų vientisumo pažeidimas – neteisėtas ar atsitiktinis Duomenų pakeitimas,

61.3. Asmens duomenų prieinamumo pažeidimas – atsitiktinis ar neteisėtas prieigos prie Duomenų praradimas arba jų sunaikinimas.

62. Priklausomai nuo aplinkybių, Asmens duomenų saugumo pažeidimas gali būti susijęs su konfidencialumu, vientisumu ir prieinamumu tuo pačiu metu, taip pat su bet kokiu jų deriniu.

63. Nors Asmens duomenų konfidencialumo ir vientisumo pažeidimų atvejai yra aiškūs ir nesunkiai nustatomi, Asmens duomenų prieinamumo pažeidimai gali būti mažiau akivaizdūs. Todėl bet koks Duomenų pažeidimas visada bus laikomas ir Asmens duomenų prieinamumo pažeidimu, kai Duomenys yra prarandami arba sunaikinami.

64. Darbuotojas, nustatęs ar sužinojęs apie (galimą) Asmens duomenų saugumo pažeidimą Bendrovėje, nedelsdamas Bendrovės suteiktu elektroniniu paštu, bet ne vėliau kaip per 2 (dvi) valandas, turi apie tai informuoti Duomenų apsaugos pareigūną ir pateikti visą jam žinomą informaciją, kuri gali turėti įtakos Asmens duomenų saugumo pažeidimo tyrimui. Šis terminas taip pat taikomas tais atvejais, kai Asmens duomenų saugumo pažeidimas nustatomas savaitgalį, švenčių dienomis arba likus mažiau nei 2 valandoms iki darbo laiko pabaigos. Tai, kad Darbuotojas nežino tam tikros informacijos apie Asmens duomenų saugumo pažeidimą, nėra pateisinama priežastis vėluoti apie tai pranešti Duomenų apsaugos pareigūnui. Tokiu atveju Darbuotojas privalo nedelsdamas informuoti Duomenų apsaugos pareigūną apie patį pažeidimo faktą ir pateikti trūkstamą informaciją vėliau, kai to paprašo Duomenų apsaugos pareigūnas. Kai informacija apie Asmens duomenų saugumo pažeidimą gaunama ne darbo funkcijų kontekste (pvz., spaudoje pateikiama informacija apie Asmens duomenų saugumo pažeidimą), Darbuotojas apie tokią informaciją taip pat privalo pranešti Duomenų apsaugos pareigūnui.

65. Bendrovė privalo nepagrįstai nedelsdama ir, jei įmanoma, praėjus ne daugiau kaip per 72 valandoms nuo tada, kai sužino apie Asmens duomenų saugumo pažeidimą, apie tai pranešti Inspekcijai. Taip pat privaloma įvertinti, ar būtina pranešti atitinkamiems Duomenų subjektams ir, jei būtina, nepagrįstai nedelsiant apie tai jiems pranešti (BDAR 34 straipsnis). Nebūtina pranešti apie visus Asmens duomenų saugumo pažeidimus.

66. Duomenų apsaugos pareigūnas vykdo Asmens duomenų saugumo pažeidimų valdymą vadovaudamasis šia Politika ir Teisės aktais ir pildo Asmens duomenų saugumo pažeidimo registro įrašo formą (Politikos 3 priedas).

67. Duomenų apsaugos pareigūnas, gavęs informaciją apie Asmens duomenų saugumo pažeidimą, turi nustatyti dėl to Duomenų subjektų teisėms ir laisvėms kylančias rizikas ir pasekmių

tikimybę bei sunkumą, kad įvertintų, ar apie Asmens duomenų saugumo pažeidimą reikia pranešti Duomenų subjektams ir (ar) Inspekcijai:

67.1. jei dėl Asmens duomenų saugumo pažeidimo gali kilti pavojus fizinių Duomenų subjektų teisėms ir laisvėms būtina pranešti Inspekcijai,

67.2. jei dėl Asmens duomenų saugumo pažeidimo gali kilti didelis pavojus Duomenų subjektų teisėms ir laisvėms, būtina pranešti Inspekcijai ir Duomenų subjektams.

68. Duomenų apsaugos pareigūnas, gavęs informaciją apie (galimą) Asmens duomenų saugumo pažeidimą iš Darbuotojo ar pats jį pastebėjęs, nedelsdamas atlieka pirminę Asmens duomenų saugumo pažeidimo analizę:

68.1. peržiūrėti informaciją apie Asmens duomenų saugumo pažeidimą;

68.2. nustatyti Asmens duomenų saugumo pažeidimo valdymo (įskaitant reikalingos informacijos rinkimą, konsultavimąsi su Darbuotojais ir (arba) Paslaugų teikėjais) terminus;

68.3. nustatyti, ar ir kokia papildoma informacija iš Darbuotojų yra reikalinga vykdant Asmens duomenų saugumo pažeidimo valdymą, bei paprašyti šios informacijos;

68.4. nustatyti, ar ir kokie Paslaugų teikėjai, išorės Duomenų apsaugos pareigūnai, IT saugumo konsultantai ir (ar) kiti Tretieji asmenys turi būti įtraukti į Asmens duomenų saugumo pažeidimų valdymo procesą bei prireikus prašyti jų pagalbos.

69. Vertinant riziką taip pat būtina atsižvelgti į šiuos kriterijus:

69.1. Asmens duomenų saugumo pažeidimo tipas. Šie kriterijai aprašyti Politikos 59 - 61 punktuose ir gali daryti įtaką rizikos lygiui;

69.2. duomenų pobūdis, jautrumas ir apimtis. Paprastai kuo jautresni Duomenys, tuo didesnė žalos rizika paveiktiems žmonėms, tačiau reikėtų atsižvelgti ir į kitus Duomenis, kurie jau gali būti prieinami apie Duomenų subjektą. Be to, Duomenų derinys paprastai yra jautresnis nei pavienis Duomuo;

69.3. asmenų identifikavimo paprastumas. Svarbus veiksnys, į kurį reikia atsižvelgti, yra tai, kaip lengva šaliai, turinčiai prieigą prie paveiktų Duomenų, identifikuoti konkrečius asmenis arba suderinti Duomenis su kita informacija, kad būtų galima juos identifikuoti;

69.4. pasekmių sunkumas asmenims. Atsižvelgiant į Duomenų, susijusių su Asmens duomenų saugumo pažeidimu, pobūdį, pvz., Specialiųjų kategorijų asmens duomenis, fiziniams asmenims galinti kilti žala gali būti ypač didelė, visų pirma tais atvejais, kai dėl Asmens duomenų saugumo pažeidimo gali būti pavogta tapatybė, padaryta fizinė žala, patirtas psichologinis stresas, pažeminimas ar žala reputacijai;

69.5. ypatingos asmens savybės. Asmens duomenų saugumo pažeidimas gali turėti įtakos Duomenims, susijusiems su vaikais ar kitais pažeidžiamais asmenimis, kuriems dėl to gali kilti didesnis pavojus;

69.6. Bendrovės ypatumai. Bendrovės ir jos veiklos pobūdis ir vaidmuo gali turėti įtakos nustatant Asmens duomenų saugumo pažeidimo riziką;

69.7. nukentėjusių asmenų skaičius. Kuo didesnis paveiktų asmenų skaičius, tuo didesnis tikėtinas Asmens duomenų saugumo pažeidimo poveikis.

70. Duomenų apsaugos pareigūnas, nustatęs, kad Asmens duomenų saugumo pažeidimo valdymui reikalinga papildoma informacija, paprašo Darbuotojų ir (ar) Paslaugų teikėjų suteikti reikiamą informaciją ne vėliau kaip per 4 (keturias) valandas. Darbuotojai turi laiku suteikti Duomenų apsaugos pareigūnui visą prašomą informaciją.

71. Duomenų apsaugos pareigūnas ne vėliau kaip per 72 (septyniasdešimt dvi) valandas nuo momento, kai sužinojo apie Asmens duomenų saugumo pažeidimą, turi užbaigti Asmens duomenų saugumo pažeidimo valdymą, įskaitant Asmens duomenų saugumo pažeidimo užregistravimą ir, jei reikia, pranešimų pateikimą Inspekcijai ir (ar) Duomenų subjektui.

72. Duomenų apsaugos pareigūnas vykdo Asmens duomenų saugumo pažeidimo valdymą:

72.1. pildydamas Asmens duomenų saugumo pažeidimų registro įrašo formą ir joje aprašydamas kiekvieną Asmens duomenų saugumo pažeidimą;

72.2. teikdamas pranešimus Inspekcijai ir Duomenų subjektams apie Asmens duomenų saugumo pažeidimus;

72.3. teikdamas rekomendacijas ir nurodymus Darbuotojams dėl Asmens duomenų saugumo pažeidimų pasekmių šalinimo ar švelninimo.

73. Pranešimas apie Asmens duomenų saugumo pažeidimą yra būtinas, išskyrus atvejus, kai mažai tikėtina, kad Asmens duomenų saugumo pažeidimas keltų pavojų Duomenų subjektų teisėms ir laisvėms, o pagrindinis veiksnys, dėl kurio apie jį reikia pranešti Duomenų subjektams, yra tie atvejai, kai jis gali sukelti didelę riziką Duomenų subjektų (fizinių asmenų) teisėms ir laisvėms. Ši rizika kyla, kai dėl Asmens duomenų saugumo pažeidimo Duomenų subjektai, kurių Duomenys buvo paveikti, gali patirti fizinę, materialinę ar neturtinę žalą, pvz., diskriminaciją, tapatybės vagystę ar sukčiavimą, finansinius nuostolius, žalą reputacijai ir kt. Kai Asmens duomenų saugumo pažeidimas susijęs su Specialiųjų kategorijų asmens duomenimis, turėtų būti laikoma, kad tokia žala gali atsirasti.

74. Duomenų apsaugos pareigūnas raštu praneša Inspekcijai apie kiekvieną Duomenų saugumo pažeidimą, išskyrus atvejus, kai Asmens duomenų saugumo pažeidimų registro įrašas rodo, jog atitinkamas Asmens duomenų saugumo pažeidimas nekelia pavojaus Duomenų subjektams. Jei užpildytas Asmens duomenų saugumo pažeidimų registro įrašas rodo, jog atitinkamas Asmens duomenų saugumo pažeidimas kelia didelį pavojų Duomenų subjektams, kurių Duomenys buvo paveikti, Duomenų apsaugos pareigūnas raštu praneša Duomenų subjektams apie Asmens duomenų saugumo pažeidimą, išskyrus atvejus, kai Asmens duomenų saugumo pažeidimų registro įrašas įrodo, jog Duomenų subjektai buvo apsaugoti nuo pavojaus, pvz., Bendrovė 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, pvz., šifravimo priemones; taip pat Bendrovė vėliau ėmėsi priemonių, kuriomis užtikrinama, kad nebegalėtų kilti didelis pavojus Duomenų subjektų teisėms ir laisvėms.

75. Jei užpildytas Asmens duomenų saugumo pažeidimų registro įrašas pagrindžia, jog Duomenų subjektų informavimas apie jų Asmens duomenų saugumo pažeidimą pareikalautų neproporcingai daug pastangų, Duomenų apsaugos pareigūnas neprivalo pranešti Duomenims apie Asmens duomenų saugumo pažeidimą. Šiuo atveju Duomenų apsaugos pareigūnas, derindamas su Bendrovės vadovu, turi imtis kitų veiksmingų priemonių, skirtų informuoti Duomenų subjektus, kurių Duomenys buvo paveikti Asmens duomenų saugumo pažeidimo (pvz., informaciją paskelbti internete ar žiniasklaidoje), bei šias priemones nurodyti Asmens duomenų saugumo pažeidimo registro įraše.

76. Duomenų apsaugos pareigūnui atlikus vertinimą ir padarius išvadą, kad apie Asmens duomenų saugumo pažeidimą turi būti pranešta Duomenų subjektams ir (ar) Inspekcijai, jis užpildo

Inspekcijos parengtą Asmens duomenų saugumo pažeidimo formą (prieiga: https://vdai.lrv.lt/lt/adsp-ir-dap/pranesimas-apie-asmens-duomenu-saugumo-pazeidima/), kai pranešimas, skirtas Inspekcijai. Bendrovė apie Asmens duomenų saugumo pažeidimą turi pranešti Inspekcijai nepagrįstai nedelsdama ir, jei įmanoma, ne vėliau kaip per 72 valandas nuo to momento, kai apie jį sužinojo. Laikoma, kad Bendrovė sužinojo apie Asmens duomenų saugumo pažeidimą, kai Bendrovė yra pakankamai įsitikinusi, kad įvyko saugumo incidentas, dėl kurio buvo paveikti Asmens duomenys. Jei pranešimas Inspekcijai nepateikiamas per 72 valandas, kartu su juo turi būti nurodomos vėlavimo priežastys. Atsižvelgiant į Asmens duomenų saugumo pažeidimo aplinkybės, Bendrovė gali vertinti galimybę apie Asmens duomenų saugumo pažeidimą informuoti kitas valstybės ar savivaldybės institucijas ar kitus viešuosius subjektus;

77. Duomenų subjektai turėtų būti tiesiogiai informuojami apie Asmens duomenų saugumo pažeidimą pvz., siunčiant jiems pranešimą el. paštu, paštu, SMS žinute ir pan. Šis pranešimas turėtų būti atskirtas nuo kitos siunčiamos informacijos, pvz., komercinių pranešimų. Tais atvejais, kai tiesioginis pranešimas Duomenų subjektui pareikalautų neproporcingų pastangų, pranešimas gali būti skelbiamas viešai arba taikant panašias priemones, kuriomis Duomenų subjektai informuojami vienodai veiksmingai, pvz., garsių interneto svetainių reklamjuostės ar reklamos populiarioje spaudoje. Informavimas tik paskelbiant pranešimą spaudai ar naujieną įmonės tinklaraštyje nėra veiksminga priemonė pranešti Duomenų subjektui apie Asmens duomenų saugumo pažeidimą. Priklausomai nuo aplinkybių, Bendrovė gali naudoti kelis komunikacijos būdus. Duomenų subjektams turi būti pateikta bent ši informacija: Duomenų apsaugos pareigūno vardas ir kontaktiniai duomenys; galimos Asmens duomenų saugumo pažeidimo pasekmės; priemonės, kurių ėmėsi arba pasiūlė imtis Bendrovė, kad būtų pašalintas Asmens duomenų saugumo pažeidimas, įskaitant, kai tinkama, priemones galimoms neigiamoms jo pasekmėms sumažinti;

78. Visi Asmens duomenų saugumo pažeidimai, nepriklausomai nuo to, ar apie juos pranešta Inspekcijai arba Duomenų subjektams, turi būti registruojami Asmens duomenų saugumo pažeidimų registre (Politikos 4 priedas). Remdamasi jame pateikta informacija, Inspekcija turi turėti galimybę patikrinti, kaip įgyvendinamas įpareigojimas pranešti apie Asmens duomenų saugumo pažeidimus. Asmens duomenų saugumo pažeidimų registras turi apimti faktus, susijusius su Asmens duomenų saugumo pažeidimu, jo poveikiu ir taisomaisiais veiksmais, kurių buvo imtasi.

79. Informacija apie Asmens duomenų saugumo pažeidimą turėtų būti įvesta į Asmens duomenų saugumo pažeidimų registrą, kai tik nustatomas Asmens duomenų saugumo pažeidimas ir įvertinama rizika (Politikos 4 priedas). Jei reikia, Asmens duomenų saugumo pažeidimo informacija registre vėliau turėtų būti papildyta ir (arba) ištaisyta.

80. Duomenų apsaugos pareigūnas yra atsakingas už Asmens duomenų saugumo pažeidimų registro pildymą ir atnaujinimą. Asmens duomenų saugumo pažeidimas pildomas ir saugomas elektroniniu formatu.

XI SKYRIUS
INSPEKCIJOS PAKLAUSIMAI

81. Darbuotojas gavęs Inspekcijos paklausimą, nedelsiant, bet ne vėliau kaip per 1 (vieną) darbo dieną, informuoja Duomenų apsaugos pareigūną apie tokį paklausimą.

82. Duomenų apsaugos pareigūnas vykdo Inspekcijos paklausimų valdymą vadovaudamasis šia Politika ir Teisės aktais.

83. Duomenų apsaugos pareigūnas, gavęs Inspekcijos paklausimą, turi nedelsdamas atlikti pirminę Inspekcijos paklausimo analizę:

83.1. peržiūrėti Inspekcijos paklausimą;

83.2. nustatyti atsakymo į Inspekcijos paklausimą terminus (įskaitant reikalingos informacijos surinkimą, konsultacijas su Darbuotojais ir (ar) Paslaugų teikėjais). Duomenų apsaugos pareigūnas turi patikslinti šiame Politikos skyriuje nurodytus terminus, jei to reikia, kad būtų laikomasi Inspekcijos nustatytų terminų;

83.3. jei reikia, kreiptis į Inspekciją dėl termino pateikti atsakymą pratęsimo;

83.4. nustatyti, ar yra reikalinga papildoma informacija iš Darbuotojų ir, jei taip, - paprašyti tokią informaciją pateikti;

83.5. nustatyti, ar Paslaugų teikėjai, išoriniai Duomenų apsaugos pareigūnai, IT saugumo konsultantai ir (ar) Tretieji asmenys yra susiję su Inspekcijos paklausimu ir, jei taip, paprašyti jų pagalbos rengiant atsakymą į Inspekcijos paklausimą.

84. Duomenų apsaugos pareigūnas, nustatęs, kad Inspekcijos paklausimo valdymui reikalinga papildoma informacija, paprašo Darbuotojų, Paslaugų teikėjų ir (ar) Trečiųjų šalių suteikti tokią informaciją. Darbuotojai turi laiku suteikti Duomenų apsaugos pareigūnui visą jo prašomą informaciją.

85. Surinkęs visą atsakymui į Inspekcijos paklausimą reikalingą informaciją, tačiau jokiu būdu ne vėliau kaip per Inspekcijos nustatytą terminą, Duomenų apsaugos pareigūnas parengia ir pateikia Inspekcijai atsakymą į paklausimą.

XII SKYRIUS
DUOMENŲ APSAUGOS PAREIGŪNAS

86. Bendrovė paskiria Duomenų apsaugos pareigūną, kuris padeda prižiūrėti kaip Bendrovėje laikomasi Teisės aktų reikalavimų.

87. Duomenų apsaugos pareigūnas turi būti tinkamai ir laiku (kuo anksčiau) įtrauktas į visus klausimus, susijusius su Duomenų apsauga Bendrovėje.

88. Duomenų apsaugos pareigūno vardas bei pavardė (pavadinimas) ir kontaktiniai duomenys turi būti nurodyti Duomenų tvarkymo veiklos įrašuose.

89. Duomenų apsaugos pareigūnas tiesiogiai atskaitingas Bendrovės vadovybei.

90. Duomenų apsaugos pareigūnas neturi gauti jokių nurodymų dėl užduočių vykdymo. Bendrovė negali atleisti Duomenų apsaugos pareigūno arba bausti jo dėl jam nustatytų užduočių atlikimo.

91. Bendrovė padeda Duomenų apsaugos pareigūnui vykdyti nurodytas užduotis suteikdama būtinus išteklius, taip pat suteikdama galimybę susipažinti su Duomenimis, dalyvauti Duomenų tvarkymo operacijose ir išlaikyti savo ekspertines žinias.

92. Bendrovė paskelbia viešai Duomenų apsaugos pareigūno kontaktinius duomenis ir praneša apie juos Inspekcijai.

93. Duomenų apsaugos pareigūnas atlieka šias užduotis:

94.1. informuoja Bendrovę, jos Darbuotojus ir valdymo organų narius apie jų prievoles pagal Teisės aktus, taip pat apie Duomenų apsaugą Bendrovėje ir konsultuoja juos šiais klausimais;

93.1. stebi, kaip Bendrovėje laikomasi Teisės aktų reikalavimų;

93.2. rūpinasi Duomenų rinkimo, naudojimo ir saugojimo veikloje dalyvaujančių Darbuotojų sąmoningumo ugdymu bei mokymu;

93.3. atlieka ir (arba) koordinuoja Bendrovės atitikties Teisės aktams auditus;

93.4. koordinuoja, atlieka ir (ar) stebi poveikio Duomenų apsaugai vertinimus Bendrovėje;

93.5. stebi, ar Bendrovė kuria, diegia ir (ar) naudoja IKT Duomenų tvarkymui laikantis Teisės aktų reikalavimų;

93.6. atlieka kontaktinio asmens funkcijas Duomenų subjektams, kurie kreipiasi į Bendrovę su Duomenų tvarkymu susijusiais klausimais;

93.7. konsultuoja Bendrovę dėl Duomenų perdavimo konkretiems Paslaugų teikėjams ar kitiems subjektams, įsisteigusiems už EEE ribų;

93.8. esant poreikiui dalyvauja šios Politikos, duomenų tvarkymo veiklos įrašų, kitų su duomenų apsauga susijusių vidaus taisyklių, procedūrų rengimo procese, konsultuoja Bendrovės darbuotojus;

93.9. koordinuoja, kad Bendrovė su visais Paslaugų teikėjais sudarytų Duomenų tvarkymo sutartis, įskaitant sąlygas dėl paslaugų teikimo (arba sutartis su Paslaugų teikėjais atitinkamomis nuostatomis);

93.10. praneša apie esamus ar galimus Teisės aktų pažeidimus, keliančius pavojus Bendrovės veiklai, bei konsultuoja Darbuotojus, atsakingus už šiuos pažeidimus;

93.11. praneša Bendrovės vadovybei, kai Bendrovėje nesivadovaujama Duomenų apsaugos pareigūno nuomone;

93.12. atlieka Asmens duomenų saugumo pažeidimų valdymą;

93.13. atlieka Duomenų subjektų teisių įgyvendinimo valdymą;

93.14. atlieka kontaktinio asmens funkcijas Inspekcijai kreipiantis į Bendrovę;

93.15. teikia metinę ataskaitą Bendrovės vadovybei už praėjusius metus apie savo veiklą ir Bendrovės atitiktį Teisės aktams.

XIII SKYRIUS
PRITAIKYTOJI DUOMENŲ APSAUGA IR POVEIKIO DUOMENŲ APSAUGAI VERTINIMAS

94. Bendrovė privalo užtikrinti pritaikytąją duomenų apsaugą įgyvendinama tinkamas technines ir organizacines priemones, skirtas užtikrinti Duomenų apsaugos principų laikymąsi.

95. Bendrovė turi įvertinti, kokias pritaikytosios Duomenų apsaugos priemones galima įgyvendinti visose programose, sistemose ar procesuose, kuriuose tvarkomi Asmens duomenys, atsižvelgdama į techninių galimybių išsivystymo lygį, įgyvendinimo sąnaudas, Duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus, ir Duomenų tvarkymo keliamus įvairios tikimybės ir rimtumo pavojus fizinių asmenų teisėms ir laisvėms.

96. PDAV yra būdas Bendrovei, kai ji veikia kaip duomenų valdytoja, sistemingai ir išsamiai analizuoti Duomenų tvarkymą ir padėti nustatyti ir sumažinti Asmens duomenų saugumo pažeidimų riziką. Atliekant PDAV daugiausia dėmesio turėtų būti skiriama ne tik atitikties rizikoms, bet ir platesnėms rizikoms asmenų teisėms ir laisvėms, įskaitant bet kokių didelių socialinių ar ekonominių neigiamų pasekmių galimybę. Bendrovė turėtų įvertinti galimą žalą – individualiems asmenims ar visuomenei apskritai, nepriklausomai nuo to, ar žala yra fizinė, materialinė ar

nemateriali. PDAV neprivaloma nurodyti, kad visos rizikos buvo panaikintos. Tačiau tai turėtų padėti Bendrovei jas dokumentuoti ir įvertinti, ar likusios rizikos yra priimtinos.

97. Net jei nėra konkrečių didelės rizikos požymių, patartina atlikti PDAV bet kokiam dideliam naujam projektui, susijusiam su Asmens duomenų naudojimu. PDAV reikėtų pradėti projekto pradžioje prieš pradedant Duomenų tvarkymą ir atlikti lygiagrečiai su planavimo ir vystymo procesais.

98. Darbuotojai privalo prieš protingą terminą informuoti Duomenų apsaugos pareigūną, kai ketinama Bendrovėje kurti, diegti ar naudoti tam tikras IKT ir (ar) kitus metodus, skirtus tvarkyti Duomenis, šiais atvejais:

98.1. naujos rūšies informacinės technologijos, kurios pirmą kartą diegiamos Bendrovėje;

98.2. Duomenų subjektų automatinio vertinimo ir profiliavimo įrankiai;

98.3. vaizdo stebėjimo priemonės;

98.4. IKT tikrinimo priemonės;

98.5. įrankiai, skirti Duomenų subjektus sekti internete;

98.6. debesų kompiuterijos įrankiai;

98.7. daiktų interneto įrankiai (t. y., įrankiai, sujungiantys į interneto tinklą kasdieninius objektus ir leidžiantys jiems siųsti ir gauti Duomenis);

98.8. dirbtinio intelekto įrankiai;

98.9. blokų grandinės (angl. blockchain) įrankiai;

98.10. socialinių tinklų įrankiai;

98.11. įrankiai, dėl kurių naudojimo Duomenys tampa prieinami Paslaugų teikėjams, įsteigtiems už EEE ribų;

98.12. kitos konkrečios IKT ir (ar) kiti metodai, skirti Bendrovėje tvarkyti Duomenis, kurie kelia pavojų Duomenų subjektams pagal ADA Teisės aktus.

99. Atlikti PDAV reikalaujama šiuo atveju:

99.1. 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,

99.2. Specialių kategorijų asmens duomenų arba duomenų apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas tvarkymas dideliu mastu, arba

99.3. sistemingas viešos vietos stebėjimas dideliu mastu.

100. PDAV turi apimti:

100.1. sistemingą numatytų Duomenų tvarkymo operacijų aprašymą ir Duomenų tvarkymo tikslus, įskaitant, kai taikoma, teisėtus interesus, kurių siekia Bendrovė,

100.2. Duomenų tvarkymo operacijų reikalingumo ir proporcingumo, palyginti su tikslais, vertinimą,

100.3. Duomenų subjektų teisėms ir laisvėms kylančių pavojų vertinimą, ir pavojams pašalinti numatytas priemones, įskaitant apsaugos priemones, saugumo priemones ir mechanizmus, kuriais užtikrinama Asmens duomenų apsauga ir įrodoma, kad laikomasi BDAR, atsižvelgiant į Duomenų subjektų ir kitų susijusių asmenų teises ir teisėtus interesus.

101. Tam tikrais atvejais Bendrovė turi siekti išsiaiškinti Duomenų subjektų ar jų atstovų nuomonę apie numatytą Duomenų tvarkymą, nepažeisdama komercinių ar viešųjų interesų apsaugos arba Duomenų tvarkymo operacijų saugumo reikalavimų.

102. PDAV vykdomas pagal Teisės aktus, kompetentingų institucijų rekomendacijas ir kitus atitinkamus ir naujausius kompetentingų institucijų priimtus dokumentus.

103. Už PDAV atlikimą atsako: Bendrovės struktūrinio padalinio vadovas, dėl kurio vykdomų Duomenų tvarkymo operacijų bus atliekamas PDAV ir (ar) Bendrovės direktoriaus įsakymu paskirtas darbuotojas . Jei Darbuotojai ketina inicijuoti naujas Duomenų tvarkymo operacijas ar keisti esamas taip, kad jos tenkintų šiame Politikos skyriuje nurodytus kriterijus, apie tai privalu nedelsiant informuoti Duomenų apsaugos pareigūną. Viso PDAV atlikimo metu turi dalyvauti ir Duomenų apsaugos pareigūnas, teikti konsultacijas bei pareikšti savo nuomonę raštu.

104. PDAV taip pat privalomai atliekamas šiais atvejais:

104.1. Duomenų tvarkymas mokslinių ar istorinių tyrimų tikslais: (a) kai Specialiųjų kategorijų asmens duomenys tvarkomi be Duomenų subjekto sutikimo arba kai Duomenų tvarkymas atliekamas susiejant ar derinant Duomenų rinkinius, arba (b) tvarkant nepilnamečių Duomenis,

104.2. Duomenų tvarkymas dideliu mastu, kai Duomenys gaunami ne iš Duomenų subjekto bei informacijos, reikalaujamos pagal BDAR, teikimas yra neįmanomas arba pareikalautų neproporcingų pastangų, arba jeigu dėl tokio informacijos pateikimo gali tapti neįmanoma arba jis gali labai sukliudyti pasiekti tvarkymo tikslus,

104.3. Duomenų tvarkymas, kai duomenų gavėjų, kuriems buvo atskleisti Asmens duomenys, informavimas apie Asmens duomenų ištaisymą, ištrynimą arba tvarkymo apribojimą, nėra įmanomas arba pareikalautų neproporcingų pastangų,

104.4. biometrinių duomenų, kuriais siekiama konkrečiai nustatyti fizinio asmens tapatybę, tvarkymas Duomenų subjektų stebėsenos ar kontrolės tikslais arba kai tvarkomi pažeidžiamų Duomenų subjektų Asmens duomenys,

104.5. genetinių duomenų tvarkymas vykdant Duomenų subjekto savybių vertinimą arba balų skyrimą, įskaitant profiliavimą ir prognozavimą,

104.6. asmens vaizdo duomenų tvarkymas, kai vaizdo stebėjimas vykdomas patalpose, kurios nėra Bendrovės valdomos nuosavybės ar kitais teisėtais pagrindais, sveikatos priežiūros, socialinės globos, įkalinimo įstaigose ir kitose įstaigose, kuriose paslaugos yra teikiamos pažeidžiamiems asmenims, arba kartu su garso įrašymu,

104.7. pokalbių telefonu įrašymas,

104.8. Asmens duomenų tvarkymas naudojant inovatyvias technologijas arba egzistuojančias technologijas panaudojant nauju būdu, kai tvarkomi pažeidžiamų Duomenų subjektų Asmens duomenys,

104.9. vaikų Asmens duomenų tvarkymas tiesioginės rinkodaros tikslais, vaikų asmeninių aspektų vertinimas, kuris yra grindžiamas automatizuotu tvarkymu, įskaitant profiliavimą, arba kai vaikams tiesiogiai yra siūlomos informacinės visuomenės paslaugos,

104.10. Darbuotojų Asmens duomenų tvarkymas stebėsenos ar kontrolės tikslais: asmens vaizdo ir (ar) garso duomenų tvarkymas darbo vietoje ir (ar) Bendrovės patalpose ar teritorijose, kuriose dirba jos darbuotojai; Asmens duomenų, susijusių su Darbuotojų, komunikacijos, elgesio, vietos ar judėjimo stebėsena, tvarkymas.

105. Duomenų apsaugos pareigūnas, gavęs Darbuotojo pranešimą, nedelsdamas suteikia raštišką konsultaciją atsakingam (-iems) Darbuotojui (-ams) dėl to, ar atlikti poveikio Duomenų apsaugai vertinimą dėl konkrečių IKT ir (ar) kitų metodų.

106. Gavęs Duomenų apsaugos pareigūno konsultaciją, atsakingas (-i) Darbuotojas (-ai) turi nuspręsti, ar turi būti atliktas poveikio Duomenų apsaugai vertinimas dėl konkrečių IKT ir (ar) kitų metodų, skirtų tvarkyti Duomenis Bendrovėje, bei informuoti Duomenų apsaugos pareigūną apie tokį sprendimą.

107. Duomenų apsaugos pareigūnas, gavęs sprendimą atlikti poveikio Duomenų apsaugai vertinimą, pagal šios Politikos ir Teisės aktų reikalavimus turi:

107.1. nustatyti, ar ir kokia papildoma informacija iš Darbuotojų ir (ar) Paslaugų teikėjų yra reikalinga siekiant atlikti poveikio Duomenų apsaugai vertinimą, ir paprašyti tokią informaciją pateikti;

107.2. nuspręsti, ar Duomenų apsaugos pareigūnas atliks poveikio Duomenų apsaugai vertinimą pats, ar paprašys Paslaugų teikėjo ar kitos kvalifikuotos trečiosios šalies atlikti tokį vertinimą bei paruošti išvadą;

107.3. nustatyti, ar ir kurie Paslaugų teikėjai, išorės Duomenų apsaugos pareigūnai, IT saugumo konsultantai ir (arba) kiti tretieji asmenys turi dalyvauti poveikio Duomenų apsaugai vertinime bei paprašyti šių trečiųjų asmenų įsitraukti į poveikio Duomenų apsaugai vertinimo rengimą;

107.4. per protingą terminą nuo visos reikiamos informacijos gavimo pagal Teisės aktų reikalavimus atlikti poveikio Duomenų apsaugai vertinimą ir parengti raštišką vertinimo ataskaitą; o tais atvejais, kai nusprendžiama poveikio Duomenų apsaugai vertinimą pavesti atlikti Paslaugų teikėjui ar kitai kvalifikuotai trečiajai šaliai, užtikrinti, kad šiuos veiksmus atliktų atitinkamas subjektas;

107.5. pateikti poveikio Duomenų apsaugai vertinimo išvadą atsakingam (-iems) Darbuotojui (-ams), o jei nustatoma, kad kyla didelis pavojus Duomenų subjektų Duomenų apsaugai, patarti jam (-iems) kreiptis į Inspekciją dėl išankstinės konsultacijos;

108. jei Duomenų apsaugai vertinimo išvadoje nustatoma, kad kyla didelis pavojus Duomenų subjektų Duomenų apsaugai, atsakingas (-i) Darbuotojas (-ai) privalo per 3 (tris) darbo dienas nuspręsti, ar kreiptis į Inspekciją dėl išankstinės konsultacijos, ir apie savo sprendimą informuoti Duomenų apsaugos pareigūną;

109. Duomenų apsaugos pareigūnas, gavęs atsakingo (-ų) Darbuotojo (-ų) sprendimą kreiptis į Inspekciją dėl išankstinės konsultacijos, kreipiasi į Inspekciją Bendrovės vardu;

110. Duomenų apsaugos pareigūnas dalyvauja išankstinių konsultacijų procedūroje, bendradarbiauja su Inspekcija, analizuoja ir atsako į Inspekcijos paklausimus, Inspekcijos prašymu renka informaciją, jei reikia prašo Paslaugų teikėjų ir trečiųjų asmenų pagalbos arba kreipiasi į Inspekciją su prašymu gauti raštišką konsultaciją.

XIV SKYRIUS
MOKYMAI IR AUDITAS

111. Bendrovė užtikrina, kad visi Darbuotojai būtų tinkamai apmokyti ir galėtų laikytis Teisės aktų. Bendrovė taip pat turi reguliariai tikrinti savo sistemas ir procesus, kad įvertintų jų atitiktį Teisės aktams.

112. Darbuotojai privalo dalyvauti visuose su Duomenų apsauga susijusiuose Bendrovės organizuojamuose mokymuose.

113. Darbuotojai privalo reguliariai peržiūrėti visas jų valdomas sistemas ir procesus, kad užtikrintų atitiktį šiai Politikai, ir patikrinti, ar yra tinkama valdymo kontrolė ir ištekliai, siekiant užtikrinti tinkamą Duomenų naudojimą ir apsaugą.

114. Bendrovė organizuoja Darbuotojų apmokymą Asmens duomenų apsaugos srityje prieš jiems pradedant darbą ir vėliau reguliariai, bet ne rečiau nei kartą per metus.

XV SKYRIUS
BAIGIAMOSIOS NUOSTATOS

115. Politika peržiūrima ir, reikalui esant, atnaujinama pasikeitus asmens duomenų apsaugą reglamentuojantiems teisės aktams ar jų įgyvendinimo praktikai, taip pat pasikeitus Įstaigos atliekamam asmens duomenų tvarkymui, bet ne rečiau kaip kartą per vienerius metus.

116. Bendrovės darbuotojas, pažeidęs Politikos reikalavimus, atsako Lietuvos Respublikos teisės aktų nustatyta tvarka.

_____

Asmens duomenų apsaugos politikos 1 priedas

DUOMENŲ TVARKYMO SUTARTIS

202_ m. _____ __ d. Nr. SUTARTIES NUMERIS
Vilnius

UAB „GRINDA”, juridinio asmens kodas 120153047, adresas Eigulių g. 32, LT-03150 Vilnius, Lietuva, duomenys kaupiami ir saugomi Lietuvos Respublikos juridinių asmenų registre, atstovaujama direktoriaus _____ (toliau – **Duomenų valdytojas**),

ir

PAVADINIMAS, juridinio asmens kodas KODAS, adresas ADRESAS, atstovaujama direktoriaus VARDAS, PAVARDĖ (toliau – **Duomenų tvarkytojas**),

toliau Duomenų valdytojas ir Duomenų tvarkytojas kartu vadinami **Šalimis**, o kiekvienas iš jų atskirai – **Šalimi**,

ATSIŽVELGDAMOS Į TAI, KAD:

A. Duomenų tvarkytojas teikia PASLAUGŲ RŪŠIS paslaugas Duomenų valdytojui, pagal METAI, MĖNESIS, DIENA d. SUTARTIES PAVADINIMAS sutartį (toliau – **Paslaugų sutartis**);

B. Paslaugų teikimo pagrindu, Duomenų tvarkytojas tvarko Duomenų valdytojo turimus asmens duomenis;

C. Šalys yra suinteresuotos, kad būtų užtikrinta Duomenų valdytojo asmens duomenų apsauga;

Šalys sudaro šią duomenų tvarkymo sutartį ir susitaria (toliau – **Sutartis**):

1. SUTARTIES DALYKAS

1.1. Duomenų tvarkytojas įsipareigoja tvarkyti asmens duomenis laikantis 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 (toliau – **Reglamentas**) ir kitų taikomų teisės aktų, ir Duomenų valdytojo nurodymų.

1.2. Sutartyje vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos Reglamente ir kituose taikomuose asmens duomenų apsaugą reglamentuojančiuose teisės aktuose.

1.3. Aiškumo tikslais Šalys patvirtina, kad ši Sutartis netaikoma tiems asmens duomenims, kuriuos Duomenų tvarkytojas tvarko pats veikdamas kaip Duomenų valdytojas.

2. DUOMENŲ TVARKYMO TIKSLAI, APIMTIS IR TRUKMĖ

2.1. Duomenų valdytojas paveda Duomenų tvarkytojui tvarkyti Duomenų valdytojo asmens duomenis tiek, kiek tai būtina Paslaugų sutarčiai vykdyti.

2.2. Duomenų tvarkymo tikslai, Duomenų subjektų kategorijos ir tvarkomi asmens duomenys, prie kurių Duomenų tvarkytojas turi ar gali turėti prieigą, pateikiami Sutarties priede Nr. 1.

2.3. Duomenų tvarkytojas turi teisę tvarkyti asmens duomenis tol, kol tai yra būtina Duomenų valdytojo nustatytiems tikslams įgyvendinti. Jeigu, Duomenų valdytojo nuomone, duomenų tvarkymo tikslai yra nebeaktualūs ir nebereikalingi, Duomenų tvarkytojas turi iš karto nutraukti asmens duomenų tvarkymo veiksmus.

3. ŠALIŲ ĮSIPAREIGOJIMAI

3.1. Duomenų tvarkytojas, tvarkydamas asmens duomenis Duomenų valdytojo vardu, įsipareigoja:

3.1.1. tvarkyti asmens duomenis tik pagal Duomenų valdytojo pateiktus rašytinius nurodymus, įskaitant nurodymus, išdėstytus šioje Sutartyje ir jos prieduose, išskyrus atvejus, kai taikomi teisės aktai nustato kitaip. Tokiu atveju, prieš pradėdamas tvarkyti asmens duomenis, Duomenų tvarkytojas, kiek tai leidžia teisės aktai, privalo informuoti Duomenų valdytoją apie tokį teisinį reikalavimą. Jei Duomenų tvarkytojas neturi nurodymų, kaip tvarkyti asmens duomenis konkrečioje situacijoje, arba, jei koks nors nurodymas pažeidžia arba galėtų pažeisti taikomą duomenų apsaugos teisės aktą, arba kai Duomenų tvarkytojas kitaip turi tvarkyti duomenis be Duomenų valdytojo rašytinių nurodymų, tačiau teisės aktų reikalavimo pagrindu, Duomenų tvarkytojas privalo nedelsdamas apie tai raštu informuoti Duomenų valdytoją;

3.1.2. tvarkydamas asmens duomenis veikti pagal Reglamentą ir kitų taikytinų asmens duomenų apsaugą reglamentuojančių teisės aktų reikalavimus;

3.1.3. tvarkyti su visų kategorijų su asmens duomenų tvarkymo veikla, vykdoma Duomenų valdytojo vardu, susijusius įrašus;

3.1.4. tvarkyti asmens duomenis tinkamai ir tiksliai, tik tiek, kiek būtina duomenų tvarkymo tikslams pasiekti. Netvarkyti asmens duomenų kitais tikslais, kuriais tvarkyti asmens duomenų neįgaliojo Duomenų valdytojas;

3.1.5. atsižvelgdamas į techninių galimybių išsivystymo lygį, įgyvendinimo sąnaudas bei duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus, taip pat duomenų tvarkymo keliamus įvairios tikimybės ir rimtumo pavojus fizinių asmenų teisėms ir laisvėms, įgyvendinti tinkamas technines ir organizacines priemones, kad būtų užtikrintas pavojų atitinkančio lygio asmens duomenų saugumas. Duomenų tvarkytojas įsipareigoja įgyvendinti visas teisės aktuose bei kompetentingų duomenų apsaugos institucijų nustatytas ar rekomenduojamas technines ir organizacines saugumo priemones, įskaitant ir tas, kurios yra taikomos pagal gerąją praktiką. Duomenų valdytojui paprašius, Duomenų tvarkytojas įsipareigoja pateikti informaciją apie tai, kokias technines ir organizacines saugumo priemones taiko asmens duomenų saugumui užtikrinti, taip pat, jeigu Duomenų valdytojas paprašytų, įgyvendinti Duomenų valdytojo nuomone trūkstamas saugumo priemones;

3.1.6. laikytis šioje Sutartyje nustatytų subtvarkytojo pasitelkimo sąlygų;

3.1.7. sužinojus apie bet kokį atsitiktinį ar neleistiną asmens duomenų atskleidimą, pakeitimą, sunaikinimą, saugojimą, praradimą ar kitokį tvarkymą arba be leidimo gautą prieigą, apie tai informuoti Duomenų valdytoją, nebent tai draustų atlikti teisės aktai, Sutartyje nustatyta tvarka;

3.1.8. netvarkyti asmens duomenų ilgiau negu bus būtina juos tvarkyti, siekiant įgyvendinti Duomenų valdytojo nustatytus duomenų tvarkymo tikslus. Duomenų valdytojo prašymu arba Šalims nutraukus bendradarbiavimą, Duomenų tvarkytojas įsipareigoja tokiu pačiu formatu kaip ir gavo kuo greičiau grąžinti Duomenų valdytojui visus asmens duomenis arba ištrinti esamas jų kopijas Duomenų valdytojo pasirinkimu ir patvirtinti tai raštu;

3.1.9. užtikrinti, kad asmens duomenis tvarkyti įgalioti asmenys būtų įsipareigoję užtikrinti konfidencialumą arba jiems būtų taikoma atitinkama įstatais nustatyta konfidencialumo prievolė. Duomenų tvarkytojas privalo raštu įpareigoti savo darbuotojus, kurie tvarkys asmens duomenis laikyti visus asmens duomenis konfidencialia informacija ir nenaudoti asmens duomenų jokiais kitais tikslais, išskyrus jų tvarkymą Duomenų valdytojo vardu, tiek, kiek tai būtina paslaugai suteikti. Duomenų tvarkytojas įsipareigoja pateikti savo darbuotojams instrukcijas dėl teisės aktuose nustatytų asmens duomenų tvarkymo reikalavimų. Duomenų tvarkytojas įsipareigoja supažindinti savo darbuotojus su instrukcijomis dėl Duomenų valdytojo asmens duomenims taikomų tvarkymo reikalavimų, nustatytų šioje Sutartyje, jos prieduose, pakeitimuose ar bet kokiuose kituose Šalių susitarimuose. Pasikeitus teisės aktuose, šioje Sutartyje, jos prieduose, pakeitimuose ar bet kokiuose kituose Šalių susitarimuose nustatytiems asmens duomenų tvarkymo reikalavimams, Duomenų tvarkytojas įsipareigoja nedelsiant pateikti savo darbuotojams atnaujintas instrukcijas;

3.1.10. imtis priemonių, siekiant užtikrinti, kad bet kuris jam pavaldus fizinis asmuo, galintis susipažinti su asmens duomenimis, jų netvarkytų, išskyrus atvejus, kai duodami nurodymai juos tvarkyti;

3.1.11. pateikti Duomenų valdytojui visą informaciją, būtiną siekiant įrodyti, kad vykdomos šioje Sutartyje nustatytos prievolės, ir sudaryti sąlygas bei padėti Duomenų valdytojui arba kitam Duomenų valdytojo įgaliotam auditoriui atlikti auditą, įskaitant patikrinimus. Duomenų valdytojas arba kitas Duomenų valdytojo įgaliotas auditorius audito arba patikrinimo metu gali, įskaitant, bet neapsiribojant, reikalauti pateikti atsakymus į raštu arba žodžiu pateiktus klausimus, reikalauti pateikti dokumentus ar kitą informaciją, pagrindžiančius atitiktį šioje Sutartyje arba teisės aktuose nustatytiems duomenų apsaugos reikalavimams, apklausti Duomenų tvarkytojo darbuotojus ar kitus asmenis, Duomenų tvarkytojo įgaliotus tvarkyti asmens duomenis;

3.1.12. atsižvelgdamas į asmens duomenų tvarkymo pobūdį, taikydamas tinkamas technines ir organizacines priemones, padėti Duomenų valdytojui įvykdyti Duomenų valdytojo prievolę atsakyti į prašymus pasinaudoti visomis duomenų subjekto teisėmis. Duomenų tvarkytojas, gavęs Duomenų subjekto prašymą pasinaudoti duomenų subjekto teisėmis, privalo nedelsiant perduoti tokį prašymą Duomenų valdytojui. Duomenų tvarkytojas taip pat turi teikti Duomenų valdytojui visą būtiną informaciją ar atlikti kitus su duomenų subjekto prašymu susijusius veiksmus, kai šie veiksmai yra būtini tinkamam prašymo pasinaudoti duomenų subjekto teisėmis įvykdymui;

3.1.13. padėti Duomenų valdytojui užtikrinti su duomenų saugumu, poveikio duomenų apsaugai vertinimu ir išankstinėmis konsultacijomis susijusių prievolių (Reglamento 32-36 straipsniai) laikymąsi, atsižvelgdamas į asmens duomenų tvarkymo pobūdį ir Duomenų tvarkytojo turimą informaciją. Tokia pagalba, be kita ko, apima visos informacijos, būtinos tinkamam su

duomenų saugumu, poveikio duomenų apsaugai vertinimu ir išankstinėmis konsultacijomis susijusių prievolių (Reglamento 32-36 straipsniai) vykdymui pateikimą, bendradarbiavimą mažinant poveikį duomenų apsaugai, priežiūros institucijos rekomendacijų vykdymą ir kitus veiksmus, būtinus užtikrinti su duomenų saugumu, poveikio duomenų apsaugai vertinimu ir išankstinėmis konsultacijomis susijusių prievolių (Reglamento 32-36 straipsniai) laikymąsi.

3.2. Duomenų valdytojas įsipareigoja:

3.2.1. instrukcijas dėl asmens duomenų tvarkymo bendrais atvejais Duomenų tvarkytojui pateikti raštu, nebent situacijos aplinkybės reikalautų kitokios formos. Instrukcijos, duotos kitokia forma nei raštu, bus Duomenų valdytojo patvirtintos raštu, jeigu Duomenų tvarkytojas to paprašys;

3.2.2. teikti tik teisėtus, atitinkančius Reglamento reikalavimus, nurodymus Duomenų tvarkytojui;

3.2.3. bendradarbiauti su Duomenų tvarkytoju ir užtikrinti sklandžią Duomenų tvarkytojo prieigą prie Duomenų valdytojo asmens duomenų;

3.2.4. bendradarbiauti įgyvendinant Duomenų subjektų teises ir operatyviai informuoti Duomenų tvarkytoją, jeigu Duomenų subjektas pateiktų prašymą dėl jo tvarkomų asmens duomenų ištaisymo, duomenų tvarkymo sustabdymo arba duomenų sunaikinimo.

4. DUOMENŲ TVARKYTOJO TEISĖ PASITELKTI DUOMENŲ SUBTVARKYTOJUS

4.1. Duomenų tvarkytojas turi teisę pasitelkti trečiąsias šalis asmens duomenims tvarkyti (subtvarkytojai) tik su išankstiniu rašytiniu Duomenų valdytojo sutikimu kiekvieno atskiro tokio subtvarkytojo pasitelkimo atveju. Duomenų valdytojas suteikia leidimą šios Sutarties priede Nr. 2 nurodytiems duomenų subtvarkytojams. Duomenų tvarkytojas užtikrina, kad su visais pasitelktais duomenų subtvarkytojais būtų sudarytos duomenų tvarkymo sutartys, atitinkančios šioje Sutartyje nustatytus reikalavimus. Duomenų valdytojo prašymu Duomenų tvarkytojas nepagrįstai nedelsdamas ir nemokamai turi pateikti tokių susitarimų kopijas, arba jų išrašus, jeigu tai neprieštarauja Duomenų tvarkytojo konfidencialumo įsipareigojimams, taikomiems Duomenų subtvarkytojo atžvilgiu. Duomenų tvarkytojas prisiima atsakomybę ir užtikrina, kad Duomenų subtvarkytojai laikysis visų šios Sutarties nuostatų. Duomenų tvarkytojui norint pakeisti pasitelktą Duomenų subtvarkytoją kitu, jis turi nedelsdamas pranešti apie tai Duomenų valdytojui.

4.2. Duomenų tvarkytojas visiškai atsako už subtvarkytojų veiksmus ar neveikimą, kaip nurodyta Sutarties 7 skirsnyje.

5. PRANEŠIMAS DUOMENŲ VALDYTOJUI APIE ASMENS DUOMENŲ PAŽEIDIMĄ

5.1. Duomenų tvarkytojas, paaiškėjus galimam asmens duomenų pažeidimui, privalo imtis Sutarties 5.2–5.6 punktuose nustatytų veiksmų.

5.2. Duomenų tvarkytojas nedelsdamas, bet ne vėliau kaip per 24 valandas nuo galimo pažeidimo paaiškėjimo momento, turi apie tai pranešti Duomenų valdytojui, raštu pateikdamas pranešimą, kuriame nurodyta 5.2.1 papunktyje nustatyta informacija, kiek tos informacijos įmanoma pateikti tuo metu, taip pat teikti Duomenų valdytojui 5.2.1 papunktyje nurodytą informaciją, jei ji nebuvo pateikta per šiame punkte nurodytą terminą nedelsiant po jos paaiškėjimo,

bet ne vėliau kaip per 48 valandas nuo galimo pažeidimo paaiškėjimo momento. Pranešime turi būti:

5.2.1. 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;

5.2.2. nurodytas kontaktinio asmens, galinčio suteikti daugiau informacijos, vardas bei pavardė (pavadinimas) ir kontaktiniai duomenys;

5.2.3. aprašytos tikėtinos asmens duomenų saugumo pažeidimo pasekmės;

5.2.4. aprašytos priemonės, kurių ėmėsi arba pasiūlė imtis Duomenų tvarkytojas, kad būtų pašalintas asmens duomenų saugumo pažeidimas, įskaitant, kai tinkama, priemones galimoms neigiamoms jo pasekmėms sumažinti.

5.3. Jei informacijos nėra įmanoma pateikti Duomenų valdytojui Sutarties 5.2 punkte nustatytais terminais, Duomenų tvarkytojas privalo nedelsiant raštu pagrįsti vėlavimo priežastis ir pridėti jas patvirtinančius įrodymus, jei būtina.

5.4. Duomenų tvarkytojas turi kuo greičiau imtis priemonių pašalinti pažeidimus ir (ar) sumažinti ar pašalinti jų pasekmes, siekiant atkurti padėtį, kuri buvo prieš pažeidimą.

5.5. Duomenų tvarkytojas turi išsaugoti esamos situacijos, susijusios su galimu pažeidimu, įrodymus, kad vėliau naudojant technines ir organizacines priemones (pvz., duomenų srauto ir prisijungimų analizės įrankius ar kt.) būtų galima tirti pažeidimą.

5.6. Šalys turi bendradarbiauti tiriant pažeidimą ir teikti informaciją, reikšmingą pažeidimo nustatymui ar (ir) dėl pažeidimo atsiradusių ar gresiančių neigiamų pasekmių sumažinimui ar kelio užkirtimui.

6. ASMENS DUOMENŲ PERDAVIMAS

6.1. Duomenų tvarkytojas, be išankstinio Duomenų valdytojo rašytinio leidimo, negali perduoti asmens duomenų už Europos Ekonominės Erdvės ribų ar tarptautinėms organizacijoms. Duomenų valdytojas suteiks sutikimą konkrečioms valstybėms ir teritorijoms. Duomenų tvarkytojas privalo laikytis visų pagrįstų Duomenų valdytojo nurodymų, susijusių su asmens duomenų tvarkymu tokiose valstybėse ar teritorijose. Jei pagal šią Sutartį asmens duomenys yra perduodami į trečiąsias valstybes, toks perdavimas yra galimas tik jei yra naudojamos standartinės duomenų apsaugos sąlygos, patvirtintos Europos Komisijos (*Standard Contractual Clauses, SCCs*) arba gavėjo atžvilgiu yra priimtas Europos Komisijos sprendimas dėl tinkamumo. Jei asmens duomenys yra perduodami trečiajai valstybei, kurios atžvilgiu nėra priimtas Europos Komisijos sprendimas dėl tinkamumo, Duomenų tvarkytojas, gavęs raštišką Duomenų valdytojo sutikimą dėl tokio duomenų perdavimo, užtikrina tinkamą, proporcingą asmens duomenų apsaugą, kuri būtina pagal Reglamentą.

7. ATSAKOMYBĖ

7.1. Nepaisant Paslaugų sutartyje numatytų atsakomybės apribojimų (jei tokių būtų), įvykus asmens duomenų saugumo pažeidimui, kurį lėmė Duomenų tvarkytojo vykdomas neteisėtas, vykdytas be pagrindo arba aplaidus asmens duomenų tvarkymas, arba Duomenų tvarkytojui kitaip

pažeidus šią Sutartį arba teisės aktus, reglamentuojančius duomenų apsaugą, Duomenų tvarkytojas, Duomenų valdytojui pareikalavus, įsipareigoja atlyginti žalą, padarytą dėl atitinkamo pažeidimo. Duomenų tvarkytojas užtikrina, kad atlygins Duomenų valdytojui bet kokius nuostolius, atsiradusius dėl pateiktų pretenzijų ir (ar) paskirtų baudų, taip pat bet kokius kitus nuostolius, kurie kiltų Duomenų tvarkytojui, jo subtvarkytojams, darbuotojams ar kitiems jo įgaliotiems ar jo vardu veikiantiems asmenims pažeidus šios Sutarties nuostatas arba Reglamento ar kitų taikomų asmens duomenų apsaugą reglamentuojančių teisės aktų reikalavimus.

7.2. Neapribojant Sutarties nuostatų dėl teisės į nuostolių atlyginimą ir atsakomybės taikymo, jeigu Duomenų tvarkytojas pažeidžia Reglamentą nustatydamas tvarkymo tikslus ir priemones, Duomenų tvarkytojas duomenų tvarkymo požiūriu laikytinas duomenų valdytoju ir tokiu būdu prisiima visą atsakomybę už tokį duomenų tvarkymą.

7.3. Už šios Sutarties vykdymą nėra mokamas joks papildomas atlygis Duomenų tvarkytojui. Asmens duomenų tvarkymas yra sudėtinė Paslaugų sutarties paslaugų dalis, o užmokestis už duomenų tvarkymą įeina į Paslaugų sutarties paslaugų kainą.

8. AUDITO ATLIKIMAS

8.1. Su sąlyga, kad Duomenų tvarkytojo nebus reikalaujama pateikti arba leisti susipažinti su informacija apie (i) kitus Duomenų tvarkytojo klientus, (ii) kitas išorines ar vidines neviešas Duomenų tvarkytojo ataskaitas, Duomenų valdytojas ir (arba) Duomenų valdytojo paskirtas nepriklausomas auditorius turi teisę šios Sutarties galiojimo laikotarpiu bet kada atlikti Duomenų tvarkytojo ir jo subtvarkytojų auditą bei patikrinimus, laikantis Sutarties sąlygų ir pranešus apie tai bent prieš 5 darbo dienas. Vis dėlto, šios Sutarties pagrindu atliekami auditai apsiriboja Duomenų tvarkytojo įsipareigojimų pagal šią Sutartį vykdymo vertinimu. Tokį auditą galima atlikti ne dažniau kaip vieną kartą per 12 mėnesių, išskyrus atvejus, kai nustatomas asmens duomenų saugumo pažeidimas.

8.2. Šalys sutinka, kad kompetentinga priežiūros institucija turi teisę atlikti Duomenų tvarkytojo auditą, kuris būtų tokio paties masto ir kuriam būtų taikomos tokios pačios sąlygos kaip ir Duomenų valdytojo auditui, pagal taikytinus duomenų apsaugos teisės aktus.

9. INFORMACIJOS SAUGUMAS IR KONFIDENCIALUMAS

9.1. Duomenų tvarkytojas užtikrina, kad, priklausomai nuo Duomenų tvarkytojo teikiamų paslaugų, ėmėsi tinkamų techninių ir organizacinių priemonių tvarkomiems asmens duomenims apsaugoti ir laikosi visų Duomenų valdytojo nurodytų duomenų saugumo politikų ir instrukcijų bei pateikia Duomenų valdytojui savo IT saugumo politiką arba taikomų saugumo priemonių sąrašą. Priemonės turi užtikrinti tinkamą saugumo lygį, atsižvelgiant į:

9.1.1. esamas technines galimybes;

9.1.2. priemonių sąnaudas;

9.1.3. ypatingą riziką, susijusią su asmens duomenų tvarkymu; ir

9.1.4. specialių kategorijų asmens duomenų tvarkymą.

9.2. Duomenų tvarkytojas taiko šias technines ir organizacines priemones:

9.2.1. fizinės prieigos apsaugą. Neprižiūrimos Duomenų tvarkytojo patalpos, su kompiuterine įranga ir asmenine informacija, turi būti laikomos užrakintos, siekiant apsaugoti asmens duomenis nuo neteisėto naudojimo, poveikio ar vagystės;

9.2.2. duomenų atkūrimo procesą, skirtą nuskaityti asmens duomenis, atkurtus iš atsarginių kopijų;

9.2.3. leidimų kontrolę, pagal kurią prieiga prie asmens duomenų galima per techninę leidimų kontrolės sistemą. Leidimas turi galioti tik tiems asmenims, kuriems asmens duomenys reikalingi tiesioginėms darbo funkcijoms atlikti. Vartotojo vardai ir slaptažodžiai turi būti privatūs ir negali būti perduoti kitiems subjektams. Taip pat turi būti nustatytos leidimų paskirstymo ir panaikinimo procedūros;

9.2.4. galimybę registruoti prisijungimus prie asmens duomenų (angl. logs). Turi būti sudarytos sąlygos retrospektyviai peržiūrėti tokius prisijungimus duomenų bazėse;

9.2.5. saugią komunikaciją, kai išoriniai duomenų perdavimo ryšiai apsaugoti naudojant technines funkcijas; taip pat turinio šifravimą tranzitu perduodamuose duomenų perdavimo kanaluose už Duomenų tvarkytojo kontroliuojamų sistemų;

9.2.6. procesus, skirtus saugiam asmens duomenų naikinimui užtikrinti, kai fiksuotos arba keičiamos laikmenos nebenaudojamos pagal paskirtį;

9.2.7. susitarimų dėl konfidencialumo su paslaugų teikėjais, kurie teikia asmens duomenų saugojimui naudojamos įrangos aptarnavimą ir priežiūrą, sudarymą.

9.3. Be Duomenų valdytojo išankstinio sutikimo, Duomenų tvarkytojas įsipareigoja neatskleisti tvarkomų asmens duomenų jokioms trečioms šalims, išskyrus pasitelktus subtvarkytojus, kaip nurodyta šioje Sutartyje.

10. BAIGIAMOSIOS NUOSTATOS

10.1. Ši Sutartis galioja tol, kol Duomenų valdytojo nurodymu yra atliekami duomenų tvarkymo veiksmai siekiant vykdyti Paslaugų sutartį ir įgyvendinti duomenų tvarkymo tikslus. Nutrūkus Šalių bendradarbiavimui, automatiškai nutrūksta ir ši Sutartis.

10.2. Šalys aiškiai patvirtina, kad šios Sutarties galiojimas yra būtinas tinkamam Paslaugų sutarties vykdymui, todėl nutraukus šią Sutartį ar jai kitaip pasibaigus, automatiškai nutrūksta ir Paslaugų sutartis.

10.3. Jei bet kuri Sutarties nuostata tampa ar pripažįstama visiškai ar iš dalies negaliojančia, tai neturi įtakos kitų Sutarties nuostatų galiojimui. Tokiu atveju Šalys įsipareigoja negaliojančią nuostatą pakeisti galiojančia nuostata taip, kad ji savo teisine ir ekonomine prasme būtų kiek įmanoma artimiausia negaliojančiai nuostatai.

10.4. Visi Sutarties pakeitimai ir papildymai gali būti atliekami tik abiejų Šalių bendru susitarimu raštu. Visi Sutarties pakeitimai ir papildymai įsigalioja nuo jų pasirašymo dienos, jeigu juose nenumatyta vėlesnė įsigaliojimo data.

10.5. Bet kokie nesutarimai ar ginčai, kylantys tarp Šalių dėl Sutarties, sprendžiami Paslaugų sutartyje nustatyta tvarka.

10.6. Sutarčiai ir kitiems Šalių tarpusavio santykiams, neaptartiems Sutartyje, taikoma Lietuvos Respublikos teisė.

10.7. Visi pranešimai, sutikimai ar kita informacija pagal Sutartį teikiami Paslaugų teikimo sutartyje nustatyta tvarka.

10.8. Priedai, sudaryti pagal šią Sutartį, yra neatskiriama šios Sutarties dalis.

10.9. Sutartis sudaryta dviem egzemplioriais, turinčiais vienodą juridinę galią, po vieną egzempliorių kiekvienai Šaliai.

10.10. Ši Sutartis yra sudaryta lietuvių kalba.

11. ŠALIŲ REKVIZITAI

Duomenų valdytojas	Duomenų tvarkytojas
UAB „GRINDA“	[JURIDINIO ASMENS PAVADINIMAS]
Eigulių g. 32, LT-03150 Vilnius Juridinio asmens kodas 120153047	[JURIDINIO ASMENS ADRESAS] Juridinio asmens kodas [KODAS]
Direktorius	
(pareigos)	(pareigos)
(vardas, pavardė)	(vardas, pavardė)
(parašas)	(parašas)

Prie METAI, MĖNUO, DIENA
Duomenų tvarkymo sutarties
Priedas Nr. 1

DUOMENŲ TVARKYMO OPERACIJOS

1. Duomenų tvarkymo tikslai
Nurodykite visus tikslus, kuriais Duomenų tvarkytojas tvarkys asmens duomenis.

Paslaugų pagal Paslaugų teikimo sutartį teikimas: PASLAUGŲ APRAŠYMAS (PVZ., APSKAITA)**.**

2. Asmens duomenų kategorijos
Nurodykite asmens duomenų rūšis, kurios bus tvarkomos kiekvienam numatytam tvarkymo tikslui pasiekti:

2.1. TIKSLAS:

- DUOMENŲ KATEGORIJOS (PVZ., VARDAS, PAVARDĖ).

2.2. TIKSLAS:

- DUOMENŲ KATEGORIJOS (PVZ., VARDAS, PAVARDĖ).

3. Duomenų subjektų kategorijos
Nurodykite duomenų subjektų kategorijas, kurių asmens duomenys bus tvarkomi kiekvienam numatytam tvarkymo tikslui pasiekti.

DUOMENŲ SUBJEKTAI (PVZ., DARBUOTOJAI, KLIENTAI).

4. Tvarkymo operacijos
Nurodykite tvarkymo operacijas, kurias Duomenų tvarkytojas atliks kiekvienam numatytam tvarkymo tikslui pasiekti.

Rūšiavimas, sisteminimas, saugojimas, adaptavimas ar keitimas, išgava, susipažinimas, naudojimas, taip pat sugretinimas ar sujungimas su kitais duomenimis, ištrynimas arba sunaikinimas.

5. Duomenų tvarkymo vieta: PVZ., LIETUVA.

Duomenų valdytojas	Duomenų tvarkytojas
UAB „GRINDA“	[JURIDINIO ASMENS PAVADINIMAS]
Eigulių g. 32, LT-03150 Vilnius Juridinio asmens kodas 120153047	[JURIDINIO ASMENS ADRESAS] Juridinio asmens kodas [KODAS]
Direktorius	
_____	_____
(parašas)	(parašas)

Prie METAI, MĖNUO, DIENA Duomenų tvarkymo sutarties
Priedas Nr. 2

DUOMENŲ TVARKYTOJO SUBTVARKYTOJŲ SĄRAŠAS

Pavadinimas	Registruotas adresas ir veiklos šalis, duomenų tvarkymo vieta	Kontaktiniai duomenys	Teikiamos paslaugos rūšis ir duomenų tvarkymo aprašymas

Duomenų valdytojas

UAB „GRINDA“

Eigulių g. 32, LT-03150 Vilnius
Juridinio asmens kodas 120153047

Direktorius
(pareigos)

(vardas, pavardė)

(parašas)

Duomenų tvarkytojas

[JURIDINIO ASMENS PAVADINIMAS]
[JURIDINIO ASMENS ADRESAS]
Juridinio asmens kodas [KODAS]

(pareigos)

(vardas, pavardė)

(parašas)

Asmens duomenų apsaugos politikos 2 priedas

UAB „GRINDA"
[PAREIGOS]
SPRENDIMAS DĖL INFORMACINIŲ IR RYŠIŲ TECHNOLOGIJŲ TIKRINIMO

[data], Nr. [dokumento numeris]
Vilnius

Vadovaujantis UAB „Grinda" (toliau - Bendrovė) Asmens duomenų apsaugos politika (toliau - Politika), duomenų apsaugą reguliuojančiais teisės aktais, aktualia teismų praktika duomenų apsaugos srityje, kompetentingų institucijų rekomendacijomis bei gairėmis, nusprendžiu patikrinti darbuotojo naudojamas informacines ir komunikacines technologijas (toliau - IKT), kaip nurodyta žemiau:

1. Tikrinimo data:

2. Tikrinamas (-i) darbuotojas (-ai):

3. Tikrinimo tikslas:

4. Konkrečios priežastys, įtarimai ar informacija, dėl kurių būtinas IKT tikrinimas:

5. Trumpas aprašymas, kodėl nepakanka kitų priemonių tikrinimo tikslui pasiekti:

6. Trumpas aprašymas, kaip tikrinimo metu duomenų kiekis bus sumažintas iki būtino minimumo:

7. Trumpas paaiškinimas, kodėl Bendrovės teisėtas interesas pateisina tikrinimą ir yra svarbesnis nei darbuotojo (-ų) interesai, kaip įtvirtinta BDAR 6 str. 1 d. f p.:

8. Darbuotojas, atsakingas už tikrinimą:

9. Darbuotojai, turintys prieigą prie surinktos informacijos:

10. Surinktos informacijos saugojimo terminas:

Įpareigoju atsakingus darbuotojus vykdyti IKT tikrinimą remiantis Politika, duomenų apsaugą reguliuojančiais teisės aktais ir šiuo sprendimu, prireikus konsultuotis su Bendrovės paskirtu Duomenų apsaugos pareigūnu.

_____

Asmens duomenų apsaugos politikos 3 priedas

UAB „GRINDA"
ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ REGISTRO
ĮRAŠAS NR. [..]

1. **Terminai**
   1.1. Pažeidimo pradžios laikas ir data:
   1.2. Pažeidimo pabaigos laikas ir data:
   1.3. Sužinojimo apie pažeidimą laikas ir data:
   1.4. Šio įrašo pildymo užbaigimo / papildymo laikas ir data:
   1.5. Pranešimo apie pažeidimą Valstybinei duomenų apsaugos inspekcijai laikas ir data (jei reikalinga):
   1.6. Paveikto Duomenų subjekto informavimo apie pažeidimą laikas ir data (jei reikalinga):

2. **Faktai apie Asmens duomenų saugumo pažeidimą**
   2.1. Trumpas Asmens duomenų saugumo pažeidimo aprašymas:
   2.2. Asmens duomenų saugumo pažeidimo pobūdis:
   2.3. Asmens duomenų saugumo pažeidimo priežastis:
   2.4. Kas sukėlė Asmens duomenų saugumo pažeidimą?
   2.5. Susiję Paslaugų teikėjai, jei tokie yra:
   2.6. Kaip paaiškėjo Asmens duomenų saugumo pažeidimas?

3. **Pažeidimo paveikti Duomenys**
   3.1. Ar įmanoma nustatyti paveiktus Duomenis?
   3.2. Pažeidimo paveiktų Duomenų subjektų kategorijos:
   3.3. Apytikslis paveiktų Duomenų subjektų skaičius:
   3.4. Paveiktų Duomenų kategorijos:
   3.5. Apytikslis paveiktų Duomenų kategorijų skaičius:
   3.6. Paveiktų Specialių kategorijų asmens duomenų tipai:

4. **Pavojus asmenims**
   4.1. Ar įmanoma nustatyti pažeidimo keliamą pavojų?
   4.2. Trumpas keliamo pavojaus ir blogiausio scenarijaus aprašymas:
   4.3. Kaip vertinate nustatytą pavojų: mažas, vidutinis ar didelis?
   4.4. Trumpa tokio vertinimo argumentacija:

5. Pavojaus mažinimo priemonės

5.1. Ar nustatytas pavojus buvo mažinamos iš anksto?

5.2. Trumpas priemonių, iš anksto mažinančių pavojų, aprašymas:

5.3. Ar nustatytas pavojus buvo sumažintas po pažeidimo?

5.4. Trumpas priemonių, mažinančių pavojų po pažeidimo, aprašymas:

6. Pranešimas Valstybinei duomenų apsaugos inspekcijai

6.1. Ar pranešta Valstybinei duomenų apsaugos inspekcijai apie Asmens duomenų saugumo pažeidimą? Kada?

6.2. Jei ne, trumpai nurodykite priežastis:

6.3. Valstybinės duomenų apsaugos inspekcijos atsakymas į pranešimą apie pažeidimą:

6.4. Kokių veiksmų imtasi gavus Valstybinės duomenų apsaugos inspekcijos atsakymą?

7. Paveiktų Duomenų subjektų informavimas

7.1. Ar apie Asmens duomenų saugumo pažeidimą buvo pranešta paveiktiems Duomenų subjektams? Kada?

7.2. Jei ne, trumpai nurodykite priežastis:

7.3. Jei ne, ar Duomenų subjektai apie pažeidimą buvo informuoti kitu efektyviu būdu (pvz., internete)?

7.4. Jei taip, kokiu būdu Duomenų subjektai buvo informuoti? Kokios rekomendacijos Duomenų subjektams buvo pateiktos?

Asmens duomenų apsaugos politikos 4 priedas

UAB „GRINDA" DUOMENŲ SUBJEKTŲ PRAŠYMŲ REGISTRO ĮRAŠAS NR. [..]

1. **Terminai**

   1.1. Duomenų subjekto prašymo gavimo data:

   1.2. Nuoroda į Prašymą:

   1.3. Atsakymo į Prašymą data:

   1.4. Atsakymo į Prašymą pratęsimo terminas bei apimtis (jei reikia):

   1.5. Termino, skirto atsakyti į Prašymą, pratęsimo priežastys (jei reikia):

   1.6. Ar apie termino pratęsimą bei termino pratęsimo priežastis buvo pranešta Duomenų subjektui? (jei reikia):

   1.7. Šio įrašo užpildymo / papildymo data ir laikas:

2. **Duomenų subjekto tapatybė:**

   2.1. Ar yra pagrįstų abejonių dėl Duomenų subjekto tapatybės?

   2.2. Kokiu būdu buvo nustatyta Duomenų subjekto tapatybė?

   2.3. Ar siekiant patvirtinti Duomenų subjekto tapatybę buvo prašyta papildomos informacijos? (jei reikia)

   2.4. Kokią papildomą informaciją pateikė Duomenų subjektas? (jei reikia)

   2.5. Jei nėra galimybės identifikuoti, nurodykite to priežastis:

3. **Prašymo tipas**

   3.1. Prašymas susipažinti su Bendrovėje tvarkomais asmens duomenimis;

   3.2. Prašymas ištaisyti netikslius Bendrovėje tvarkomus asmens duomenis;

   3.3. Prašymas ištrinti Bendrovėje tvarkomus asmens duomenis;

   3.4. Prašymas apriboti Bendrovėje tvarkomų asmens duomenų naudojimą ar trynimą;

   3.5. Prašymas perkelti asmens duomenis, kuriuos Duomenų subjektas pateikė Bendrovei;

3.6. prieštaravimas dėl asmens duomenų tvarkymo Bendrovėje, kai toks asmens duomenų tvarkymas vykdomas pagal BDAR 6 straipsnio e arba f punktus, įskaitant profiliavimą remiantis tomis nuostatomis bei tiesioginės rinkodaros pranešimų teikimą;

3.7. prieštaravimas dėl bet kokio Duomenų subjekto automatinio vertinimo ir (arba) profiliavimo Bendrovėje;

3.8. bet kuris kitas prašymas ir (arba) skundas dėl bet kurio klausimo, susijusio su duomenų apsauga Bendrovėje. Pateikite paaiškinimą:

4. **Prašymo nevykdymas**

4.1. Ar vykdyti Prašymą buvo visiškai arba iš dalies atsisakyta?

4.2. Jei vykdyti Prašymą buvo visiškai arba iš dalies atsisakyta, paaiškinkite, kurią dalį buvo atsisakyta vykdyti:

4.3. Jei vykdyti Prašymą buvo visiškai arba iš dalies atsisakyta, nurodykite atsisakymo teisinį pagrindą (pagal BDAR 23 str. l d. bei kitas III skirsnio nuostatas ir kitų taikomų įstatymų nuostatas):

4.4. Jei vykdyti Prašymą buvo visiškai arba iš dalies atsisakyta, trumpai apibūdinkite priežastis:

4.5. Jei vykdyti Prašymą buvo atsisakyta dėl to, kad jis yra akivaizdžiai nepagrįstas, pateikite trumpą paaiškinimą:

4.6. Jei vykdyti Prašymą buvo atsisakyta dėl to, kad jis yra akivaizdžiai neproporcingas, pateikite trumpą paaiškinimą:

5. **Atsakymas į Prašymą**

5.1. Atsakymo į Prašymą nuoroda:

5.2. Trumpai apibūdinkite veiksmus, kurių buvo imtasi dėl Prašymo:

5.3. Trumpai apibūdinkite atsakymą į Prašymą:

5.4. Trumpai apibūdinkite, kokiu būdu buvo pateiktas atsakymas į Prašymą:

5.5. Jei tam tikra informacija Duomenų subjektui nebuvo pateikta, pateikite trumpą nepateiktos informacijos apibūdinimą:

5.6. Jei tam tikra informacija Duomenų subjektui nebuvo pateikta, nurodykite informacijos nepateikimo teisinį pagrindą (pagal BDAR 23 str. 1 d. bei kitas III skirsnio nuostatas ir kitų taikomų įstatymų nuostatas) (jei reikia):

5.7. Trumpai apibūdinkite bet kokius tolesnius veiksmus dėl Prašymo (jei reikia):

6. Prašymas dėl duomenų perkeliamumo (jei aktualu)

6.1. Ar prašymas dėl duomenų perkeliamumo yra susijęs su elektroniniais duomenimis?

6.2. Ar prašymas dėl duomenų perkeliamumo susijęs su duomenimis, kurie Bendrovėje naudojami remiantis Duomenų subjekto sutikimu ar sutartimi su Duomenų subjektu?

6.3. Ar prašymas dėl duomenų perkeliamumo susijęs su pateikusio prašymą asmens duomenimis?

6.4. Ar prašymas dėl duomenų perkeliamumo susijęs su duomenimis, kuriuos pateikė pats Duomenų subjektas? Jei taip, pateikite trumpą paaiškinimą:

6.5. Ar duomenys Duomenų subjektui buvo pateikti susistemintu, paprastai naudojamu ir kompiuterio skaitomu formatu? Jei taip, pateikite trumpą paaiškinimą:

6.6. Ar prašymas dėl duomenų perkeliamumo susijęs su duomenimis, kurie gali neigiamai paveikti kitų asmenų? Jei taip, pateikite trumpą paaiškinimą:

6.7. Ar prašymas dėl duomenų perkeliamumo susijęs su duomenų tiesioginiu perdavimu iš Bendrovės kitam juridiniam asmeniui? Jei taip, nurodykite šį juridinį asmenį:

6.8. Ar prašymas dėl duomenų perkeliamumo, kuris yra susijęs su duomenų tiesioginiu perdavimu iš Bendrovės kitam juridiniam asmeniui, yra techniškai įmanomas? Jei ne, pateikite trumpą paaiškinimą:

_____