

ASMENS DUOMENŲ TVARKYMO SUTARTIS

(data)

Vilnius

1. BENDROSIOS NUOSTATOS

- 1.1. AB Vilniaus šilumos tinklai, juridinio asmens kodas 124135580, buveinės adresas Elektrinės g. 2, LT-03150 Vilnius, Lietuva (toliau – Duomenų valdytojas)
ir
TCG Telecom, UAB, juridinio asmens kodas 304120498, buveinės adresas Perkūnkiemio g. 7, LT-12131 Vilnius (toliau – Duomenų tvarkytojas)
toliau kartu ir atskirai vadinamos Šalimi arba Šalimis,
vadovaujantis 2016 m. balandžio 26 d. Europos Parlamento ir Tarybos reglamentu (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (toliau – BDAR), Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu (toliau – ADTAĮ) bei kitų teisės aktų reikalavimais,
įpareigojančiais Duomenų valdytoją pasitelkti tik tuos Duomenų tvarkytojus, kurie garantuoja, kad bus įgyvendintos tinkamos techninės ir organizacinės priemonės bei duomenų tvarkymas atitiks BDAR ir kitų teisės aktų reikalavimus bei bus užtikrinta duomenų subjekto teisių apsauga
sudarė šią Asmens duomenų tvarkymo sutartį (toliau – Sutartis).
- 1.2. Ši Sutartis tampa sudėtine **SMS žinučių siuntimo paslaugų pirkimo sutarties** (toliau – Pagrindinė sutartis) dalimi bei tampa privaloma Duomenų tvarkytojui ir Duomenų valdytojui.
- 1.3. Ši Sutartis pakeičia visus ankstesnius tarp Šalių sudarytus susitarimus dėl asmens duomenų tvarkymo.
- 1.4. Šioje Sutartyje vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos BDAR, ADTAĮ bei kituose teisės aktuose.

2. DUOMENŲ TVARKYMAS

- 2.1. Duomenų tvarkytojas įsipareigoja, tinkamai tvarkyti jam perduotus asmens duomenis, tikslu įvykdyti Pagrindinėje sutartyje ir šioje Sutartyje nustatytus įsipareigojimus.
- 2.2. Duomenų tvarkytojas užtikrina, kad duomenų tvarkymas atitiks BDAR ir kitų teisės aktų reikalavimus bei bus įgyvendintos tinkamos techninės ir organizacinės priemonės nurodytos Sutarties 4 skyriuje, skirtos užtikrinti duomenų subjekto teisių apsaugą.
- 2.3. Duomenų tvarkytojas atsako už tiesioginius nuostolius, kuriuos patiria Duomenų valdytojas dėl to, kad Duomenų tvarkytojas pažeidė taikomus duomenų apsaugos teisės aktus, Sutartį, ar Duomenų valdytojo nurodymus.
- 2.4. Vykdydamos Sutartį Šalys atliks šį asmens duomenų tvarkymą:
 - 2.4.1. asmens duomenų subjektų kategorijos – Duomenų valdytojo klientai (fiziniai asmenys ir/ arba juridinių asmenų atstovai);
 - 2.4.2. asmens duomenų tvarkymo tikslas – šilumos ir/ar karšto vandens pirkimo - pardavimo sutarčių vykdymas (kontaktinių duomenų naudojimas informavimui apie paslaugų teikimą); mokėjimų už paslaugas apskaičiavimas ir administravimas; skolų administravimas ir išieškojimas; klientų informavimas apie Bendrovės veiklą, galinčią turėti įtakos jų interesams;
 - 2.4.3. asmens duomenų tvarkymo pagrindas – BDAR 6 str. 1 d. b) punktas („sutartiniai santykiai su klientu“) ir 6 str. 1 d. f) p. („teisėtas interesas užtikrinti klientų pasitenkinimą“);
 - 2.4.4. asmens duomenų kategorijos –, telefono numeris ir SMS siuntimo/ elektroninių ryšių informacija (data, laikas, statusas).;
 - 2.4.5. asmens duomenų tvarkymo veiksmai – Duomenų tvarkytojui perduodami asmens duomenys Pagrindinės sutarties įgyvendinimui, t. y. duomenys atskleidžiami persiunčiant, įrašomi, saugomi, naudojami, ištrinami pasiekus duomenų tvarkymo tikslus.
 - 2.4.6. asmens duomenų tvarkymo trukmė - asmens duomenys tvarkomi ne ilgiau, nei to reikalauja Sutartyje nurodytas asmens duomenų tvarkymo tikslas, t. y. 6 mėnesius nuo SMS išsiuntimo, išskyrus atvejus, jeigu Pagrindinė sutartis nutraukiama anksčiau, tuomet duomenys ištrinami nepagrįstai nedelsiant
- 2.5. Duomenų tvarkytojas įsipareigoja visus tvarkomus duomenis, kurie nėra perduoti tvarkyti subtvarkytojams, laikyti duomenų saugojimo vietoje, esančioje SMS siuntimo įrankyje (programoje), t. y. Duomenų tvarkytojo IT infrastruktūroje, o būtent <..> .

- 2.6. Duomenų tvarkytojas užtikrina, kad iš Duomenų valdytojo gauti asmens duomenys bus tvarkomi tik teisėtais tikslais ir tik tiek, kiek būtina šiems tikslams įgyvendinti, taip pat užtikrina, kad duomenų subjektų asmens duomenys bus tvarkomi laikantis visų aktualių nacionalinių ar tarptautinių duomenų apsaugos įstatymų ar kitų teisės aktų, taikomų šios Sutarties galiojimo metu priklausomai nuo konkretaus atvejo Duomenų valdytojui arba Duomenų tvarkytojui (toliau – asmens duomenų apsaugos teisės aktai).
- 2.7. Kai asmens duomenų tvarkymas pasibaigia, Duomenų tvarkytojas privalo nedelsiant, bet ne vėliau kaip per Duomenų valdytojo nurodytą terminą, netaikydamas jokio papildomo užmokesčio, Duomenų valdytojo pasirinkimu, išreikštu Duomenų tvarkytojui žemiau šioje Sutartyje nurodytais kontaktais, sunaikinti arba pateikti (grąžinti) Duomenų valdytojui visus asmens duomenis, kurie buvo tvarkomi Duomenų valdytojo pavedimu vykdant Sutartį, taip pat visas turimas šių asmens duomenų kopijas. Kai Asmens duomenys yra sunaikinami, Duomenų tvarkytojas privalo Duomenų valdytojo prašymu nedelsiant raštu patvirtinti šių asmens duomenų ir jų kopijų sunaikinimo faktą.

3. DUOMENŲ KONFIDENCIALUMAS

- 3.1. Duomenų valdytojo perduotus duomenis turi teisę tvarkyti tik tie Duomenų tvarkytojo darbuotojai, kuriems jie yra būtini funkcijų vykdymui, ir tik tada, kai tai yra būtina duomenų tvarkymo tikslams pasiekti, t. y. siekiant tinkamai ir laiku atlikti Pagrindinėje sutartyje ir šioje Sutartyje nurodytus įsipareigojimus.
- 3.2. Duomenų tvarkytojo darbuotojai bei kiti atsakingi asmenys, kuriems yra suteikta teisė susipažinti ir (ar) tvarkyti Duomenų valdytojo perduotus duomenis, laikytųsi konfidencialumo principo reikalavimų ir laikytų paslapytje bet kokią su asmens duomenimis susijusią informaciją, kurią jie sužinojo vykdydami savo pareigas.

4. BENDROSIOS DUOMENŲ VALDYTOJO PAREIGOS

- 4.1. Esant būtinybei ir/ar Duomenų tvarkytojo prašymui, Duomenų valdytojas įsipareigoja pateikti papildomus nurodymus ir instrukcijas dėl asmens duomenų tvarkymo.
- 4.2. Duomenų valdytojas privalo pranešti Duomenų tvarkytojui apie bet kokią asmens duomenų taisyklą ar pakeitimą.
- 4.3. pranešti Duomenų tvarkytojui apie bet kokią duomenų subjekto, kurio asmens duomenys yra perduoti Duomenų tvarkytojui, pateiktą prašymą apriboti asmens duomenų tvarkymą, ištrinti asmens duomenis ir prašymą įgyvendinti kitas duomenų subjekto teises.

5. BENDROSIOS DUOMENŲ TVARKYTOJO PAREIGOS

- 5.1. Duomenų tvarkytojas įsipareigoja asmens duomenis tvarkyti laikydamasis Duomenų valdytojo nurodymų (nurodytų šioje Sutartyje ir kituose Duomenų tvarkytojui pateiktuose rašytiniuose nurodymuose jeigu tokie nurodymai buvo pateikti), BDAR ir kitų privalomų teisės aktų reikalavimų. Duomenų tvarkytojui pažeidus Duomenų valdytojo nurodymus (nurodytus šioje Sutartyje ir kituose Duomenų tvarkytojui pateiktuose rašytiniuose nurodymuose jeigu tokie nurodymai buvo pateikti), BDAR ir kitų privalomų teisės aktų reikalavimus, Duomenų tvarkytojas laikomas atsakingu dėl netinkamo (neteisėto) asmens duomenų tvarkymo.
- 5.2. Duomenų tvarkytojo atliekamas asmens duomenų tvarkymas reglamentuojamas šia Sutartimi ir asmens duomenų apsaugos teisės aktais, kurie yra privalomi Duomenų tvarkytojui Duomenų valdytojo atžvilgiu ir kuriais nustatoma asmens duomenų tvarkymo dalykas ir trukmė, asmens duomenų tvarkymo pobūdis ir tikslas, asmens duomenų rūšis ir asmens duomenų subjektų kategorijos bei Duomenų valdytojo prievolės ir teisės, kaip nurodyta šioje Sutartyje.
- 5.3. Duomenų tvarkytojas, pagal Sutartį tvarkydamas asmens duomenis, turi laikytis visų asmens duomenų apsaugos teisės aktų, Valstybinės duomenų apsaugos inspekcijos ar kitų kompetentingų institucijų rekomendacijų / gairių.
- 5.4. Duomenų tvarkytojas turi padėti Duomenų valdytojui vykdyti pareigas, numatytas asmens duomenų apsaugos teisės aktuose, įskaitant, bet neapsiribojant, Duomenų valdytojo pareigą atsakyti į asmenų prašymus pasinaudoti teise susipažinti su apie juos turima informacija bei prašyti asmens duomenis ištaisyti, ištrinti ar apriboti su asmeniu susijusių duomenų tvarkymą.
- 5.5. Duomenų tvarkytojas negali atlikti jokių veiksmų, dėl kurių Duomenų valdytojas pažeistų asmens duomenų apsaugos teisės aktus.
- 5.6. Duomenų tvarkytojas turi nedelsdamas informuoti Duomenų valdytoją, jei turi klausimų dėl asmens duomenų tvarkymo ar nėra nurodymų dėl asmens duomenų tvarkymo konkrečioje situacijoje, arba jei nurodymai pažeidžia Sutartį arba asmens duomenų apsaugos teisės aktus. Tokiais atvejais Duomenų tvarkytojas privalo prašyti Duomenų valdytojo rašytinių nurodymų, kaip tvarkyti asmens duomenis, ir nepriimti savarankiškų sprendimų dėl asmens duomenų tvarkymo veiksmų be Duomenų valdytojo rašytinių nurodymų ir instrukcijų.

- 5.7. Nesant Duomenų valdytojo išankstinio rašytinio sutikimo, Duomenų tvarkytojas įsipareigoja neatskleisti tvarkomų asmens duomenų jokioms trečiosioms šalims, išskyrus Sutartyje nustatyta tvarka pasitelktus kitus duomenų tvarkytojus.
- 5.8. Jei asmenys, kompetentingos institucijos ar bet kurios kitos trečiosios šalys Duomenų tvarkytojo prašo informacijos apie pagal šią Sutartį tvarkomus asmens duomenis, Duomenų tvarkytojas apie tokį prašymą turi informuoti Duomenų valdytoją. Duomenų tvarkytojas jokių būdu negali veikti Duomenų valdytojo vardu, arba kaip jo atstovas, ir be išankstinių Duomenų valdytojo nurodymų negali perduoti ar bet kuriuo kitu būdu atskleisti asmens duomenų ar kitos informacijos, susijusios su asmens duomenų tvarkymu, trečiosioms šalims. Tais atvejais, kai Duomenų tvarkytojas pagal asmens duomenų apsaugos teisės aktus privalo atskleisti Duomenų valdytojo vardu tvarkomus asmens duomenis, jis turi nedelsdamas informuoti Duomenų valdytoją apie prašymą atskleisti asmens duomenis.
- 5.9. Duomenų tvarkytojas, prieš pradėdamas tvarkyti asmens duomenis, įsipareigoja įgyvendinti tinkamas tvarkomų asmens duomenų pobūdį ir rizikas asmens duomenų saugumui atitinkančias, nuolat ir nepertraukiamai veikiančias technines, organizacines ir teises asmens duomenų apsaugos priemones asmens duomenų saugumui užtikrinti, įskaitant:
- 5.9.1. duomenų šifravimą ir jų anonimiškumo užtikrinimą;
 - 5.9.2. duomenų konfidencialumo, vientisumo, saugumo užtikrinimą viso duomenų tvarkymo proceso metu;
 - 5.9.3. galimybę po techninio sistemos sutrikimo operatyviai atstatyti sklandų naudojimąsi duomenimis;
 - 5.9.4. reguliarių techninių ir organizacinių priemonių atnaujinimą, siekiant garantuoti duomenų tvarkymo proceso saugumą ir efektyvumą.
- 5.10. Paskyrus duomenų apsaugos pareigūną Duomenų tvarkytojas turi nedelsdamas raštu informuoti Duomenų valdytoją apie duomenų apsaugos pareigūno paskyrimą, nurodydamas jo vardą ir pavardę bei kontaktinius duomenis. Taip pat duomenų tvarkytojas privalo informuoti apie duomenų apsaugos pareigūno ar duomenų apsaugos pareigūno kontaktinių duomenų pasikeitimus.
- 5.11. Duomenų tvarkytojas įsipareigoja elektronine forma pildyti jo atliekamos duomenų tvarkymo veiklos įrašus, kurie turi būti prieinami Duomenų valdytojui. Duomenų veiklos tvarkymo įrašuose turi būti nurodoma:
- 5.11.1. Duomenų tvarkytojo ir asmens, atsakingo už asmens duomenų tvarkymą, vardas, pavardė ir kontaktiniai duomenys, Duomenų tvarkytojo paskirto duomenų apsaugos pareigūno vardas, pavardė ir kontaktai,
 - 5.11.2. Duomenų valdytojo vardu atliekamo duomenų tvarkymo kategorijos,
 - 5.11.3. kai taikoma, asmens duomenų perdavimai į trečiąją valstybę arba tarptautinei organizacijai, be kita ko, nurodant tą trečiosios valstybės arba tarptautinės organizacijos identifikavimą ir tinkamų apsaugos priemonių dokumentavimą,
 - 5.11.4. Sutarties 6 skyriuje nustatytų techninių ir organizacinių saugumo priemonių bendras aprašymas,
- 5.12. Duomenų tvarkytojas įsipareigoja padėti Duomenų valdytojui atliekant poveikio duomenų apsaugai vertinimą. Duomenų tvarkytojas įsipareigoja pateikti visą prašomą informaciją, skirtą poveikio duomenų apsaugai vertinimui ne vėliau kaip per 1 darbo dieną.

6. DUOMENŲ TVARKYTOJO TAIKOMOS MINIMALIOS ORGANIZACINĖS IR TECHNINĖS SAUGOS PRIEMONĖS:

- 6.1. Duomenų tvarkytojas įsipareigoja taikyti šias minimalias technines ir organizacines asmens duomenų saugumo priemones ir pateikti jų taikymo įrodymus Duomenų valdytojui (priemonių naudojimą reglamentuojančius vidaus dokumentus, atliktų auditų išvadas ir pan.):

ORGANIZACINĖS ASMENS DUOMENŲ SAUGUMO PRIEMONĖS	
6.1.1. Asmens duomenų saugumo politika ir procedūros	
6.1.1.1.	Duomenų tvarkytojo asmens duomenų ir jų tvarkymo saugumas turi būti dokumentuotas kaip informacijos saugumo politikos dalis;
6.1.1.2.	Duomenų tvarkytojo duomenų saugumo politika turi nustatyti bent: personalo pareigas (funkcijas) ir atsakomybes, pagrindines technines ir organizacines priemones, įdiegtas asmens duomenų saugumui užtikrinti, taip pat duomenų tvarkytojų ar trečiųjų šalių, susijusių su asmens duomenų tvarkymu, sąrašą;
6.1.1.3.	Atsižvelgiant į bendrą saugumo politiką, turi būti sukurtas ir prižiūrimas konkrečių su asmens duomenų saugumu susijusių politikos dokumentų, procedūrų, tvarkų aprašas
6.1.1.4.	Saugumo politika turi būti peržiūrima ir, prireikus, tikslinama kas pusmetį;
6.1.2. Vaidmenys ir atsakomybės	
6.1.2.1.	Su asmens duomenų tvarkymu susiję vaidmenys ir atsakomybės turi būti aiškiai apibrėžti ir paskirstyti pagal saugumo politiką;

6.1.2.2.	Turi būti aiškiai apibrėžtas darbuotojų teisių ir pareigų atšaukimas taikant atitinkamas vaidmenų ir atsakomybių perdavimo ar perleidimo procedūras (Duomenų tvarkytojo pertvarkymo ar darbuotojų atleidimo, funkcijų pasikeitimo metu);
6.1.2.3	Turi būti atliktas aiškus asmenų, atsakingų už konkrečias saugumo užduotis, paskyrimas, įskaitant saugos specialisto (saugos įgaliotinio) paskyrimą;
6.1.2.4.	Saugos specialistas turi būti oficialiai paskirtas (paskyrimą patvirtinant dokumentais). Saugos specialisto uždaviniai ir atsakomybės turi būti aiškiai nustatyti ir dokumentuoti;
6.1.2.5.	Nesuderinamos pareigybės (funkcijos) ir atsakomybių sritys, pavyzdžiui, saugos specialisto pareigybė ir duomenų apsaugos pareigūno pareigybė, turi būti atskirtos, siekiant sumažinti neleistino ar netyčinio asmens duomenų keitimo ar netinkamo naudojimo galimybes;
6.1.3. Prieigos valdymo politika	
6.1.3.1.	Kiekvienam vaidmeniui, susijusiam su asmens duomenų tvarkymu turi būti priskirtos konkrečios prieigos kontrolės teisės, vadovaujantis „būtina žinoti“ (angl. <i>need to know</i>) principu.
6.1.3.2.	Prieigos kontrolės politika turi būti išsami ir dokumentuota. Duomenų tvarkytojas šiame dokumente nustato atitinkamas prieigos kontrolės taisykles, prieigos teises ir apribojimus pagal konkrečias naudotojų pareigas, susijusias su asmens duomenų tvarkymo procesais ir procedūromis;
6.1.3.3.	Prieigos kontrolę užtikrinančių funkcijų atskyrimas (pvz., prieigos užklausų, prieigos leidimų, pačios prieigos administravimas) turi būti aiškiai apibrėžtas ir dokumentuotas;
6.1.3.4.	Tam tikros pareigybės (funkcijos), turinčios dideles prieigos teises, turi būti aiškiai apibrėžtos ir priskirtos tik ribotam darbuotojų skaičiui;
6.1.4. Išteklių ir turto valdymas	
6.1.4.1.	Duomenų tvarkytojas turi turėti IT išteklių (naudojamų asmens duomenimis tvarkyti) registrą (techninės, programinės ir tinklo įrangos sąrašą). IT išteklių registras turi apimti bent tokią informaciją: IT išteklių tipą (pvz., tarnybinę stotį, kompiuterinę darbo vietą), vietą (fizinę ar elektroninę). IT išteklių registro tvarkymas turi būti priskirtas konkrečiam asmeniui, pvz., IT specialistui;
6.1.4.2.	IT išteklių registras turi būti reguliariai, ne rečiau kaip kartą į tris mėnesius, peržiūrimas ir, nustačius poreikį, atnaujinamas;
6.1.4.3.	Visos pareigybės, turinčios prieigą prie IT išteklių, turi būti apibrėžtos ir patvirtintos dokumentais;
6.1.5. Keitimų valdymas	
6.1.5.1.	Duomenų tvarkytojas turi užtikrinti, kad visi esminiai IT sistemų keitimai būtų stebimi ir registruojami konkretaus asmens (pvz., IT arba saugos specialisto);.
6.1.5.2.	Programinės įrangos kūrimas turi būti atliekamas specialioje aplinkoje, kuri nėra prijungta prie IT sistemų, naudojamų tvarkant asmens duomenis. Testuojant sistemas, reikia naudoti testinius duomenis. Tais atvejais, kai tai neįmanoma, turi būti nustatytos specialios testavimo metu naudojamų asmens duomenų apsaugos procedūros;
6.1.5.3.	Turi būti įdiegti išsami ir dokumentais pagrįsta IT keitimų valdymo politika. Keitimų valdymo politika turi apibrėžti: pokyčių įvedimo ir įdiegimo procedūras, pareigybes ir vartotojus, kurių teisės buvo pakeistos, pokyčių įdiegimo laiko terminus. Pokyčių valdymo politika yra reguliariai atnaujinama;
6.1.6. Duomenų tvarkytojai	
6.1.6.1.	Prieš pradėdant asmens duomenų tvarkymo veiklą, duomenų valdytojai turi apibrėžti ir dokumentuoti ir suderinti formalias gaires ir procedūras, taikomas duomenų tvarkytojams (pvz., rangovams ar užsakovų paslaugų tiekėjams) dėl asmens duomenų tvarkymo. Šios gairės ir procedūros turi nustatyti tokį patį (ne žemesnį) asmens duomenų saugumo lygį, koks yra numatytas Duomenų tvarkytojo saugumo politikoje;
6.1.6.2	Duomenų tvarkytojas privalo nedelsdamas pranešti Duomenų valdytojui apie nustatytus asmens duomenų saugumo pažeidimus;
6.1.6.3.	Duomenų tvarkytojas turi pateikti dokumentais pagrįstus įrodymus dėl atitikties jam keliamiems reikalavimams;
6.1.6.4.	Duomenų valdytojas turi reguliariai tikrinti Duomenų tvarkytojo atitiktį nustatytų reikalavimų ir įsipareigojimų lygiui;
6.1.6.5.	Duomenų tvarkytojo darbuotojams, dirbantiems su asmens duomenimis, turi būti taikomi konkretūs dokumentais įtvirtinti informacijos konfidencialumo, neatskleidimo susitarimai;
6.1.7. Asmens duomenų saugumo pažeidimai ir saugumo incidentai	
6.1.7.1.	Turi būti nustatytas reagavimo į saugumo incidentus tvarkos planas, užtikrinantis veiksmingą incidentų, susijusių su asmens duomenų saugumu, valdymą;

6.1.7.2.	Asmens duomenų saugumo pažeidimai turi būti fiksuojami (dokumentuojami). Apie juos turi būti nedelsiant pranešama vadovybei. Turi būti nustatyta pranešimo apie asmens duomenų saugumo pažeidimus kompetentingoms institucijoms ir duomenų subjektams tvarka;
6.1.7.3.	Saugumo incidentų likvidavimo planas turi būti patvirtintas dokumentais, tarp kurių būtų galimų saugumo incidento poveikio mažinimo priemonių sąrašas ir aiškus atskirų funkcijų paskirstymas;
6.1.7.4.	Visi saugumo incidentai, įskaitant ir asmens duomenų saugumo pažeidimus, turi būti fiksuojami kartu su visa susijusia informacija apie įvykį ir vėliau atliktus incidento poveikio mažinimo veiksmus;
6.1.8. Veiklos testinumas	
6.1.8.1.	Duomenų tvarkytojas turi nustatyti pagrindines procedūras, kurių reikia laikytis saugumo incidento ar asmens duomenų saugumo pažeidimo atveju, kad būtų užtikrintas reikiamas asmens duomenų tvarkymo IT sistemomis testinumas ir prieinamumas;
6.1.8.2.	Veiklos testinumo planas turi būti išsamiai apibūdintas ir patvirtintas dokumentais (laikantis bendros saugumo politikos). Jame turi būti pateiktas aiškus veiksmų planas ir funkcijų paskirstymas;
6.1.8.3.	Veiklos testinumo plane turi būti apibrėžtas garantuotos paslaugų kokybės lygis (angl. Service-level agreement (SLA), kuris nustatomas pagrindiniams veiklos procesams, kurie užtikrina asmens duomenų saugumą;
6.1.8.4.	Turi būti paskirti Duomenų tvarkytojo darbuotojai, turintys reikiamą atsakomybę, įgaliojimus ir kompetenciją valdyti veiklos testinumą saugumo incidento, asmens duomenų saugumo pažeidimo atveju;
6.1.8.5.	Turi būti numatyta alternatyvi infrastruktūros priemonė Duomenų tvarkytojo darbui, atsižvelgiant į Duomenų tvarkytoją ir jam priimtina IT sistemų prastovą;
6.1.9. Personalo konfidencialumas	
6.1.9.1.	Duomenų tvarkytojas turi užtikrinti, kad visi darbuotojai suprastų savo atsakomybes ir įsipareigojimus, susijusius su asmens duomenų tvarkymu. Vaidmenys ir atsakomybės turi būti aiškiai išdėstyti darbuotojui prieš pradėdant vykdyti jam paskirtas funkcijas ir darbus;
6.1.9.2.	Darbuotojai, prieš pradėdami eiti savo pareigas, turi būti pasirašytinai supažindinti Duomenų tvarkytojo saugumo politika, taip pat pasirašyti atitinkamus informacijos konfidencialumo ir neatskleidimo susitarimus;
6.1.9.3.	Darbuotojai, atsakingi už aukštos rizikos asmens duomenų tvarkymo operacijas, turi laikytis konkrečių jiems taikomų konfidencialumo sąlygų (pagal jų darbo sutartį ar kitą teisės aktą);
6.1.10. Mokymai	
6.1.10.1.	Duomenų tvarkytojas turi užtikrinti, kad visi darbuotojai būtų tinkamai informuoti apie IT sistemų saugumo reikalavimus, susijusius su darbuotojų kasdieniu darbu. Darbuotojai, susiję su asmens duomenų tvarkymu, turi būti mokomi apie atitinkamus duomenų saugumo reikalavimus ir atsakomybes, rengiant reguliarius mokymus, informavimo renginius ar instruktažus. Siūlomas mokymų periodiškumas – kartą per metus;
6.1.10.2.	Duomenų tvarkytojas turi rengti struktūrinės nuolatinės personalo mokymų programas, tarp kurių būtų ir speciali programa, skirta mokyti naujus darbuotojus (duomenų apsaugos tema);
6.1.10.3.	Kiekvienais metais turi būti parengtas ir įgyvendintas mokymų planas, kuriame būtų nustatyti siektini tikslai ir uždaviniai;
TECHNINĖS ASMENS DUOMENŲ SAUGUMO PRIEMONĖS	
6.1.11. Prieigų kontrolė ir autentifikavimas	
6.1.11.1.	Turi būti įdiegta, įgyvendinta Prieigų kontrolės sistema, kuri taikoma visiems IT sistemos naudotojams. Prieigų kontrolės sistema turi leisti kurti, patvirtinti, peržiūrėti ir panaikinti naudotojų paskyras.
6.1.11.2.	Turi būti vengiama naudoti bendras naudotojų paskyras. Vietose, kur bendra naudotojų paskyra yra būtina, turi būti užtikrinta, kad visi bendros paskyros naudotojai turi tokias pat teises ir pareigas.
6.1.11.3.	Turi būti veikiantis autentifikavimo mechanizmas, leidžiantis prieigą prie IT sistemos (paremtas Prieigų kontrolės politika). Minimalus reikalavimas naudotojui prisijungti prie IT sistemos – naudotojo prisijungimo vardas ir 20 slaptažodis. Slaptažodis sudaromas atsižvelgiant į tam tikrą kompleksiskumo lygį;
6.1.11.4.	Prieigų kontrolės sistema turi turėti galimybę aptikti ir neleisti naudoti slaptažodžių, kurie neatitinka tam tikro kompleksiskumo lygio;
6.1.11.5.	Vartotojo slaptažodžiai turi būti saugomi naudojant kodavimo formą;

6.1.11.6.	Turi būti nustatytos ir dokumentais patvirtintos slaptažodžių naudojimo taisyklės. Taisyklėse turi būti apibrėžtas slaptažodžio ilgis, sudėtingumas, galiojimo laikas, nesėkmingų bandymų įvesti slaptažodį skaičius;
6.1.11.7.	Turi būti naudojamas įrenginio autentifikavimas, garantuojantis, kad 21 asmens duomenys tvarkomi tik naudojant konkrečius tinklo įrenginius (pvz., 802.1X, RADIUS ir kt.);
6.1.12. Techninių žurnalų įrašai ir stebėseną	
6.1.12.1.	Techninių žurnalų įrašai turi būti įgyvendinti kiekvienai IT sistemai, naudojamai asmens duomenims tvarkyti. Techninių žurnalų įrašuose turi būti matoma visa įmanoma prieigų prie asmens duomenų informacija (pvz., data, laikas, peržiūrėjimo, keitimo, panaikinimo veiksmai). Šie įrašai turi būti saugomi ne mažiau kaip 6 mėnesius.
6.1.12.12	Techniniai žurnalų įrašai turi turėti laiko žymas ir būti apsaugoti nuo galimo sugadinimo, suklastojimo ar neautorizuotos prieigos. IT sistemose naudojami laiko apskaitos mechanizmai turi būti sinchronizuoti pagal bendrą laiko atskaitos šaltinį.
6.1.12.13	Visi sistemų administratorių ir operatorių veiksmai (taip pat ir jų atliekamas vartotojo teisių papildymas, panaikinimas, keitimas) turi būti registruojami;
6.1.12.14	Turi būti neįmanoma ištrinti ar pakeisti techninių įrašų turinio. Prieiga prie įrašų taip pat turi būti registruojama, siekiant atlikti neįprastų veiksmų susekimo stebėseną;
6.1.12.15	Stebėsenos sistema turi apdoroti techninius įrašus, ruošti sistemos būklės ataskaitas ir įspėti apie galimus pavojus;
6.1.13. Tarnybinių stočių, duomenų bazių apsauga	
6.1.13.1.	Duomenų bazės ir taikomųjų programų tarnybinės stotys turi būti sukonfigūruotos taip, kad veiktu naudodamos atskiras paskyras su paskirtomis žemiausiomis operacinės sistemos (OS) privilegijomis;
6.1.13.2.	Duomenų bazėse ir taikomųjų programų tarnybinėse stotyse turi būti tvarkomi tik tie asmens duomenys, kurie yra reikalingi darbui, atitinkančiam duomenų tvarkymo tikslus;
6.1.13.3.	Konkrečioms saugomoms byloms ar įrašams apsaugoti turėtų būti naudojamas šifravimas, įdiegiant atitinkamą programinę ar techninę įrangą;
6.1.13.4.	Duomenų bazėse turi būti taikomi pseudonimizavimo metodai, atskiriant tiesioginius identifikatorius nuo esamų sąsajų su kitais duomenimis;
6.1.14. Darbo vietų apsauga	
6.1.14.1.	Naudotojams negalima turėti galimybės išjungti ar apeiti, išvengti IT sistemos saugos nustatymų;
6.1.14.2.	IT sistemos turi turėti nustatytą sesijos laiką, t. y. naudotojui esant neaktyviam sistemoje nustatytą laiką, jo sesija privalo būti nutraukta. Sesijos laikas – ne ilgiau kaip 15 minučių;
6.1.14.3.	Antivirusinės taikomosios programos ir jų informacijos apie virusus duomenų bazės turi būti atnaujinamos ne rečiau kaip kartą per parą;
6.1.14.4.	Kritiniai operacinės sistemos saugos atnaujinimai privalo būti diegiami reguliariai ir nedelsiant;
6.1.14.5.	Naudotojams negalima turėti privilegijų (teisių) diegti, šalinti, administruoti neautorizuotos programinės įrangos;
6.1.14.6.	Kritiniai operacinės sistemos saugos atnaujinimai privalo būti diegiami reguliariai ir nedelsiant;
6.1.14.7.	Turi būti uždrausta perduoti asmens duomenis iš kompiuterinių darbo vietų į išorinius saugojimo įrenginius (pvz., USB raktai, DVD, išorinius standžiuosius diskus ir kt.);
6.1.14.8.	Pageidautina, kad asmens duomenų tvarkymui naudojamos kompiuterinės darbo vietos nebūtų prijungtos prie interneto, nebent būtų imamas saugumo priemonių, kad būtų išvengta neteisėto asmens duomenų tvarkymo, kopijavimo ir perdavimo;
6.1.14.9.	Kompiuterinėse darbo vietose naudojamuose operacinės sistemos diskuose turi būti įgalintas pilnas standžiojo disko šifravimas;
6.1.15. Tinklo ir komunikacijos apsauga	
6.1.15.1.	Kai prieiga prie naudojamų IT sistemų yra vykdoma internetu, privaloma naudoti šifruotą komunikacijos kanalą, t.y. kriptografinius protokolus (pvz., TLS/SSL).
6.1.15.2.	Belaidis ryšys prie IT sistemų turi būti leidžiamas tik tam tikriems vartotojams ir procesams. Belaidžio ryšio potinklis turi būti atskirtas nuo kitų potinkių. Belaidė prieiga turi būti apsaugota patikimais šifravimo mechanizmais;
6.1.15.3.	Reikėtų vengti nuotolinės prieigos prie IT sistemų. Tais atvejais, kai ši prieiga yra išties reikalinga, ji yra galima tik Duomenų tvarkytojo paskirtam darbuotojui (pvz., sistemų administratoriui, saugumo specialistui) kontroliuojant ir stebint jos veikimą per iš anksto nustatytus įrenginius;

6.1.15.4.	Bet koks duomenų judėjimas iš, į IT sistemą turi būti stebimas ir kontroliuojamas naudojant ugniasienes ir įsibrovimo (įsilaužimo) aptikimo ir prevencijos sistemas;
6.1.15.5.	Informacinės sistemos tinklas turi būti atskirtas nuo kitų duomenų valdytojo tinkle;
6.1.15.6.	Prieiga prie IT sistemos turi būti atliekama tik iš patvirtintų įrenginių ir terminalų, naudojant tam skirtas technologijas, pvz., MAC adresų filtravimą arba tinklo prieigos kontrolę;
6.1.16. Atsarginės kopijos	
6.1.16.1.	Atsarginės kopijos ir duomenų atstatymo procedūros privalo būti apibrėžtos, dokumentuotos ir aiškiai susietos su vaidmenimis ir pareigomis;
6.1.16.2.	Atsarginių kopijų laikmenoms privalo būti užtikrintas tinkamas fizinis aplinkos, patalpų saugos lygis, priklausantis nuo saugomų duomenų;
6.1.16.3.	Atsarginių kopijų darymo procesas turi būti stebimas, siekiant užtikrinti užbaigtumą ir išsamumą.;
6.1.16.4.	Pilnos atsarginės duomenų kopijos privalo būti daromos reguliariai. Rekomenduojamas atsarginių kopijų darymo dažnumas: - kasdien – pridedamoji kopija; - kas savaitę – pilna kopija;
6.1.16.5.	Atsarginės kopijos turi būti reguliariai testuojamos, siekiant užtikrinti, kad jos galėtų būti patikimai naudojamos ekstremalioje situacijoje;
6.1.16.6.	Reguliarus atsarginių kopijų kūrimas ar bent reguliarus papildantysis atsarginių kopijų kūrimas turi būti atliekamas bent kartą per parą;
6.1.16.7.	Atsarginės kopijos turi būti saugiai laikomos skirtingose vietose, kurios turi būti geografiškai nutolusios viena nuo kitos;
6.1.16.8.	Atsarginės kopijos turi būti šifruojamos ir saugiai laikomos visiškai atjungus nuo kompiuterinių tinklų;
6.1.17. Mobilieji ir nešiojamieji įrenginiai	
6.1.17.1.	Mobiliųjų ir nešiojamųjų įrenginių administravimo procedūros privalo būti nustatytos ir dokumentuotos, aiškiai aprašant tinkamą tokių įrenginių naudojimą;
6.1.17.2..	Mobilieji ir nešiojamieji įrenginiai, kuriais bus naudojamas darbu su informacinėmis sistemomis, prieš naudojimąsi turi būti užregistruoti ir autorizuoti;
6.1.17.3.	Mobilieji, nešiojamieji įrenginiai turi būti pakankamo prieigos kontrolės procedūrų lygio, kaip ir kita naudojama įranga asmens duomenims tvarkyti;
6.1.17.4.	Mobiliųjų, nešiojamųjų įrenginių valdymo funkcijos ir atsakomybės turi būti aiškiai apibrėžtos;
6.1.17.5.	Duomenų tvarkytojas turi turėti galimybę nuotoliniu būdu ištrinti asmens duomenis mobiliajame, nešiojamame įrenginyje, kurio saugumas buvo sukompromituotas (pvz., pažeistos saugumo nuostatos, prarastas patikimumas);
6.1.17.6.	Nenaudojami mobilieji, nešiojamieji įrenginiai turi būti fiziškai apsaugoti nuo vagystės;
6.1.18. Programinės įrangos sauga	
6.1.18.1.	Specifiniai saugos reikalavimai, susiję su Duomenų tvarkytojo veiklos ypatumais, turi būti apibrėžti pradinuose programinės įrangos kūrimo etapuose;
6.1.18.2.	Turi būti laikomasi duomenų saugą užtikrinančių programavimo standartų ir gerosios praktikos;
6.1.18.3.	Po programinės įrangos kūrimo, testavimo ir verifikacijos, pradedant sistemos įdiegimą ir eksploataciją, jau turi būti laikomasi pagrindinių saugos reikalavimų.
6.1.18.4.	Turi būti atliekami periodiški infrastruktūros atsparumo skverbimuisi testavimai;
6.1.18.5.	Programinės įrangos atnaujinimai turi būti ištestuoti ir įvertinti prieš juos diegiant į darbo aplinką atitinkamomis veiklos sąlygomis;
6.1.19. Duomenų naikinimas ir šalinimas	
6.1.19.1.	Prieš pašalinant bet kokią duomenų laikmeną, turi būti sunaikinti visi joje esantys duomenys, naudojant tam skirtą programinę įrangą, kuri palaiko patikimus duomenų naikinimo algoritmus. Jei to padaryti neįmanoma (pvz., DVD laikmenos), turi būti įvykdytas fizinis duomenų laikmenos sunaikinimas be galimybės atstatyti;
6.1.19.2.	Popierinės ir nešiojamosios duomenų laikmenos (pvz., DVD laikmenos), kuriose buvo saugomi, kaupiami asmens duomenys, turi būti naikintos tam skirtais smulkintuvais arba kitomis mechaninėmis priemonėmis;
6.1.19.3.	Jei saugiams duomenų naikinimo ir šalinimo duomenų laikmenose ar popieriniuose dokumentuose darbams atlikti yra pasitelkiamos trečiosios šalies paslaugos, turi būti sudaryta atitinkama paslaugų sutartis ir atliekamas sunaikintų įrašų protokolavimas;
6.1.19.4.	Po duomenų ištrynimo reikėtų imtis papildomų priemonių, pvz., gali būti atliktas nepageidaujamos magnetinės informacijos pašalinimas (išmagnetinimas). Priklausomai nuo konkretaus atvejo, reikėtų įvertinti fizinio sunaikinimo galimybes;

6.1.19.5.	Jei saugiams įrašų naikinimo ir šalinimo duomenų laikmenose ar popieriniuose dokumentuose darbams atlikti yra pasitelkiamos trečiosios šalies paslaugos, turi būti užtikrinta, kad šis procesas vyktų duomenų valdytojo ir (ar) tvarkytojo patalpose, siekiant išvengti duomenų perdavimo trečiosioms šalims. Atskirais atvejais, kai to neįmanoma atlikti duomenų valdytojo ir (ar) tvarkytojo patalpose, sunaikinimas gali būti atliekamas kitoje fizinėje vietoje, tačiau tik stebint įgaliotam duomenų valdytojo atstovui.
6.1.20. Fizinė sauga	
6.1.20.1.	Turi būti įgyvendinta fizinė aplinkos, patalpų, kuriose yra IT sistemų infrastruktūra, apsauga nuo neautorizuotos prieigos;
6.1.20.2.	Būtina naudoti aiškią visų darbuotojų ir Galimos grėsmės ir pavojai lankytojų identifikavimo sistemą, naudojant tinkamas priemones, pvz., visiems norintiems patekti į Duomenų tvarkytojo patalpas tapatybę patvirtinančius darbo leidimus;
6.1.20.3.	Atitinkamos saugios zonos turėtų būti atskleidimas. apibrėžtos ir apsaugotos tinkamomis patekimo kontrolės priemonėmis. Popierinis ar elektroninis registravimo rinkmenų žurnalas turi būti saugiai laikomas, prižiūrimas ir stebimas;
6.1.20.4.	Įsilaužimo (įsibrovimo) aptikimo sistemos turi būti įdiegtos visose saugumo zonose;
6.1.20.5.	Prireikus turi būti kuriamos fizinės kliūtys, kad būtų užkirstas kelias neteisėtam fiziniam prieinamumui;
6.1.20.6.	Laisvos saugios zonos turi būti fiziškai rakinamos ir periodiškai patikrinamos;
6.1.20.7.	Tarnybinių stočių patalpoje turėtų būti įdiegta automatinė gaisro gesinimo sistema, uždara valdoma oro kondicionavimo sistema ir nepertraukiamo maitinimo šaltinis;
6.1.20.8.	Išorės subjektų personalui, įgyvendinančiam teikiamas palaikymo paslaugas, turi būti suteikta ribota prieiga prie saugių zonų.

7. NAUDOJIMASIS SUBTVARKYTOJŲ PASLAUGOMIS

- 7.1. Duomenų tvarkytojas neturi teisės (perduoti) suteikti prieigos prie asmens duomenų jokiai trečiajam asmeniui ar pasitelkti asmens duomenų subtvarkytojus be raštiško Duomenų valdytojo leidimo. Kai toks leidimas duodamas, Duomenų tvarkytojas privalo iki asmens duomenų perdavimo su atitinkamu subtvarkytoju sudaryti sutartį ir joje įtvirtinti tokius pačius asmens duomenų apsaugos reikalavimus, kaip nustatyti Duomenų tvarkytojui šioje Sutartyje.
- 7.2. Duomenų tvarkytojas privalo užtikrinti, kad Subtvarkytojas įsipareigotų įgyvendinti tinkamas technines ir organizacines priemones, kurios atitiktų Susitarime aprašytam Duomenų tvarkymui taikomų asmens duomenų apsaugą reglamentuojančių teisės aktų reikalavimus.
- 7.3. Duomenų tvarkytojas išlieka visiškai atsakingas Duomenų tvarkytojui už Subtvarkytojo su Duomenų apsauga susijusių prievolių vykdymą tada, jei šis nevykdytų ar netinkamai vykdytų tokias prievoles.
- 7.4. Duomenų tvarkytojas turi ne rečiau kaip kartą per metus tikrinti Subtvarkytojo atliekamo duomenų tvarkymo atitiktį teisės aktų reikalavimams ir pateikti pažymą Duomenų valdytojui, pasirašytą Duomenų tvarkytojo įmonės vadovo ir duomenų apsaugos pareigūno, nurodančią, jog Subtvarkytojo atliekamas duomenų tvarkymas atitinka teisės aktų bei Sutarties reikalavimus.
- 7.5. Duomenų valdytojas be atskiro rašytinio sutikimo nesutinka su Subtvarkytojų pasitelkimu atliekant duomenų tvarkymą.

8. DUOMENŲ APSAUGOS AUDITAS IR POVEIKIO DUOMENŲ APSAUGAI VERTINIMAS

- 8.1. Duomenų tvarkytojas, siekdamas garantuoti, kad įgyvendina tinkamas technines ir organizacines priemones bei duomenų tvarkymas atitinka BDAR ir kitų teisės aktų reikalavimus privalo reguliariai vykdyti asmens duomenų tvarkymo auditus ir apie atlikto audito rezultatus informuoti Duomenų valdytoją.
- 8.2. Duomenų tvarkytojas įsipareigoja asmens duomenų tvarkymo auditus vykdyti ne rečiau kaip kartą per metus
- 8.3. Duomenų valdytojas, norėdamas įsitikinti, kad duomenų tvarkymas atitinka BDAR ir kitų teisės aktų reikalavimus, gali kreiptis į Duomenų tvarkytoją, kuris įsipareigoja Duomenų valdytojui pateikti išsamią ataskaitą apie atliktus veiksmus, susijusius su asmens duomenų tvarkymu.
- 8.4. Duomenų valdytojas gali pavesti kompetentingiems asmenims atlikti Duomenų tvarkytojo veiklos auditą. Audito metu Duomenų tvarkytojas privalo bendradarbiauti ir duomenų auditą atliekančiais asmenimis bei perduoti visą reikalingą informaciją, susijusią su Duomenų valdytojo perduotais duomenimis ir jų tvarkymu.
- 8.5. Duomenų tvarkytojas įsipareigoja pateikti Duomenų valdytojui visą informaciją, būtiną siekiant įrodyti, kaip vykdomos Duomenų valdytojo ir Duomenų tvarkytojo prievolės duomenų apsaugos srityje, bendradarbiauti su

Duomenų valdytoju atliekant poveikio duomenų apsaugai vertinimą, sudaryti tam sąlygas ir suteikti reikiamą prieigą, bendradarbiauti ir neatlygintinai laiku teikti visą reikalaujamą ir reikalingą informaciją ir dokumentus.

9. DUOMENŲ SUBJEKTO TEISĖS

- 9.1. Visi duomenų subjektų prašymai ir pretenzijos, susiję su duomenų tvarkymu turi būti perduoti Duomenų valdytoju įvertinti ir apsvarstyti.
- 9.2. Duomenų tvarkytojas neturi teisės savo nuožiūra priimti sprendimų dėl duomenų subjektų kreipimosi, nepasikonsultavęs su Duomenų valdytoju arba nesilaikydamas Duomenų valdytojo nurodymų.
- 9.3. Duomenų valdytoju gavus duomenų subjekto užklausą, susijusią su Duomenų tvarkytojo tvarkomais duomenimis, Duomenų tvarkytojas įsipareigoja nedelsiant, bet ne vėliau kaip per 1 darbo dieną, pateikti visą reikiamą informaciją ir/ar dokumentus bei pagalbą, būtiną tam, kad Duomenų valdytojas galėtų tinkamai įgyvendinti duomenų subjektų prašymus ir pretenzijas, susijusias su duomenų tvarkymu.
- 9.4. Apie Valstybinės asmens duomenų apsaugos inspekcijos paklausimus ir (ar) prašymus, susijusius su Duomenų tvarkytoju perduotų asmens duomenų tvarkymu, Duomenų tvarkytojas turi nedelsiant pranešti Duomenų valdytoju šioje Sutartyje nurodytais kontaktais pranešimams (šios Sutarties 10 skyrius).

10. APSAUGOS REIKALAVIMŲ PAŽEIDIMAS

- 10.1. Duomenų tvarkytojas įsipareigoja:
 - 10.1.1. informuoti Duomenų valdytoją apie bet kokius techninių, organizacinių ar finansinių sistemų pokyčius, kurie gali turėti poveikį Duomenų tvarkytojo galimybėms ir pasirengimui tvarkyti asmens duomenis, Pagrindinėje sutartyje bei šioje Sutartyje numatytais tikslais;
 - 10.1.2. nedelsiant, bet ne vėliau kaip per 24 valandas nuo sužinojimo momento, informuoti Duomenų valdytoją šioje Sutartyje nurodytais kontaktais pranešimams (šios Sutarties 10 skyrius) apie visus duomenų saugos incidentus ir skubiai pašalinti problemą ir užkirsti kelią tolesnei žalai, taip pat sumažinti tokio saugos incidento padarinius bei bendradarbiauti su Duomenų valdytoju atliekant duomenų saugos pažeidimo tyrimus, teikiant informaciją ir/ar pranešimus apie duomenų saugos pažeidimus Valstybinei duomenų apsaugos inspekcijai ir duomenų subjektams;
 - 10.1.3. nedelsiant informuoti Duomenų valdytoją, jei Duomenų valdytojo duomenims ir/arba duomenų laikmenoms iškyla pavojus dėl turto konfiskavimo ar arešto, nemokumo ar likvidavimo, arba kitų nenumatytų įvykių. Duomenų tvarkytojas tokiais atvejais privalo pranešti visiems atsakingiems asmenims, kad duomenų suverenumas ir nuosavybės teisė į juos priklauso išimtinai Duomenų valdytoju.

11. FORCE MAJEURE

- 11.1. Bet kuri Šalis neatsako už bet kurios iš savo prievolių nevykdymą, jei įrodo, kad toks nevykdymas buvo sąlygotas aplinkybės, kurios Šalis negalėjo kontroliuoti, ir kad nebuvo galima jos numatyti arba išvengti ar įveikti tos aplinkybės ar jos pasekmių.

12. PRANEŠIMAI

- 12.1. Pranešimai ir informacija pagal šią Sutartį turi būti pateikiama raštu:
- 12.2. Duomenų tvarkytojo atstovas: Direktorius
- 12.3. Duomenų valdytojo atstovas: Klientų aptarnavimo centro Klientų aptarnavimo kokybės vadovė

13. BAIGIAMOSIOS NUOSTATOS

- 13.1. Ši Sutartis įsigalioja nuo jos pasirašymo dienos ir galioja iki visų sutartinių įsipareigojimų, kylančių iš šios sutarties, įvykdymo, išskyrus šiuos atvejus:
 - 13.1.1. Susitarimą vienašališkai nenurodant priežasties ir nesikreipiant į teismą galima nutraukti:
 - 13.1.1.1. Duomenų valdytojo iniciatyva įspėjus Duomenų tvarkytoją raštu prieš 30 (trisdešimt) dienų iki Susitarimo nutraukimo;
 - 13.1.1.2. Duomenų tvarkytojo iniciatyva įspėjus Duomenų valdytoją raštu prieš 30 (trisdešimt) dienų iki Susitarimo nutraukimo.
 - 13.1.2. Šalis turi teisę vienašališkai nutraukti Susitarimą, jei kita Šalis pažeidžia Susitarimą ir per nukentėjusios Šalies nurodytą protingą terminą pažeidimo nepanaikina. Duomenų valdytojas turi teisę nedelsdamas nutraukti Susitarimą tada, jei Duomenų tvarkytojas nesilaiko savo įsipareigojimų, nurodytų šiame susitarime.
- 13.2. Visi ginčai, kylantys iš šios sutarties sprendžiami Šalių susitarimu, o Šalims nepavykus per protingą terminą susitarti, gali būti sprendžiami teisinguose Lietuvos Respublikos teismuose pagal Lietuvos Respublikos materialinę teisę.

13.3. Iškilus bet kokiam prieštaravimui dėl duomenų tvarkymo tarp šios Sutarties ir Pagrindinės sutarties, šios Sutarties nuostatomis teikiama pirmenybė.

13.4. Ši Sutartis sudaryta – 2 (dviem) egzemplioriais, po vieną kiekvienai Šaliai.

Duomenų valdytojas:
Klientų komandos vadovas

Duomenų tvarkytojas:
Direktorius
