ASMENS DUOMENŲ TVARKYMO SUTARTIS

20__ mėn. __ Nr. __
(data)

Vilnius
(vieta)

Duomenų valdytojas Akcinė bendrovė Lietuvos oro uostai, pagal Lietuvos Respublikos įstatymus teisėtai įregistruota ir veikianti akcinė bendrovė, juridinio asmens kodas 120864074, PVM mokėtojo kodas LT208640716, registruotos buveinės adresas Švitrigailos g. 19-103, LT-03228, Vilnius, Lietuvos Respublika, duomenys apie kurią kaupiami ir saugomi VĮ Registrų centras, atstovaujamas <...>, veikiančio pagal <...>,
ir
Duomenų tvarkytojas <...>, pagal Lietuvos Respublikos įstatymus teisėtai įregistruota ir veikianti <...>, juridinio asmens kodas <...>, PVM mokėtojo kodas <...>, registruotos buveinės adresas <...>, duomenys apie kurią kaupiami ir saugomi VĮ Registrų centras, atstovaujamas <...>, veikiančio pagal <...>,

kiekvienas atskirai vadinamas „Šalimi“, o kartu „Šalimis“, vadovaudamosi 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamento (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (toliau – Reglamentas (ES) 2016/679), **sudarė šią Asmens duomenų tvarkymo sutartį** (toliau – Sutartis), kurią sudaro Sutartyje nurodyti priedai.

I SKYRIUS
SUTARTIES TIKSLAS

1. Siekiant įgyvendinti Reglamento (ES) 2016/679 28 straipsnio 3 dalį, nustatomos duomenų valdytojo ir duomenų tvarkytojo teisės bei pareigos, duomenų valdytojo vardu tvarkant asmens duomenis. Sutartimi turi būti siekiama apsaugoti duomenų subjektų teises, mažinti konkrečią asmens duomenų apsaugos riziką ir užtikrinti duomenų valdytojo ir duomenų tvarkytojo santykių bei atitinkamų teisių ir pareigų aiškumą.
2. Tiekdamas degalų apskaitos automatizavimo ir stebėsenos sistemą sudarančią aparatinę įrangą bei teikdamas minėtos sistemos palaikymą, turimų kuro kolonėlių sistemų sujungimą su perkamomis arba jau valdomomis informacinėmis sistemomis bei jų integravimą su turima buhalterinės apskaitos programa ar autoparko valdymo sistemos programine ar aparatine įranga, programinės / techninės įrangos sąveikos / apjungimo techninius sprendimus ir šių sprendimų parengimą, pritaikymą naudojimui, įskaitant atitinkamų mokymo sertifikatų suteikimo, apimančias prekes ir paslaugas <...> sutartį Nr. <...> (toliau – Paslaugų teikimo sutartis), duomenų tvarkytojas tvarkys asmens duomenis duomenų valdytojo vardu pagal šią Sutartį. Asmens duomenų tvarkymo sąlygos nustatytos Sutarties 1 priede.

II SKYRIUS
ŠALIŲ ĮSIPAREIGOJIMAI

3. Duomenų valdytojas:

3.1. įsipareigoja užtikrinti, kad asmens duomenys būtų tvarkomi laikantis Reglamento (ES) 2016/679 (žr. Reglamento (ES) 2016/679 24 straipsnį), kitų asmens duomenų apsaugą ir (ar) tvarkymą reglamentuojančių Europos Sąjungos ar jos valstybės narės teisės aktų ir šios Sutarties;
3.2. turi teisę ir pareigą priimti sprendimus dėl asmens duomenų tvarkymo tikslų ir priemonių;
3.3. yra atsakingas, įskaitant, bet neapsiribojant, už tai, kad asmens duomenų tvarkymas, kurį duomenų tvarkytojui pavesta atlikti, turėtų teisinį pagrindą.
4. Duomenų tvarkytojas įsipareigoja:
4.1. tvarkyti asmens duomenis tik pagal duomenų valdytojo pateiktus dokumentais įformintus nurodymus, išskyrus atvejus, kai to reikalaujama pagal Europos Sąjungos ar jos valstybės narės teisės aktus, kurie yra taikomi duomenų tvarkytojui (tokiais atvejais duomenų tvarkytojas informuoja duomenų valdytoją apie šiuos reikalavimus, išskyrus atvejus, kai teisės aktai draudžia minėtą informaciją pateikti dėl svarbaus viešojo intereso). Tokie nurodymai pateikti Sutarties 1 ir 3 prieduose. Duomenų valdytojas taip pat gali pateikti tolesnius nurodymus viso asmens duomenų tvarkymo metu, tačiau tokie su Sutartimi susiję nurodymai visada turi būti pagrįsti dokumentais;
4.2. nedelsiant informuoti duomenų valdytoją, jei duomenų valdytojo nurodymai, duomenų tvarkytojo nuomone, prieštarauja Reglamentui (ES) 2016/679 arba kitiems asmens duomenų apsaugą reglamentuojantiems Europos Sąjungos ar jos valstybių narių teisės aktams;
4.3. tvarkyti su asmens duomenų tvarkymo veikla, vykdoma duomenų valdytojo vardu, susijusius duomenų tvarkymo veiklos įrašus. Ši pareiga taikoma kiekvienam duomenų tvarkytojui ir, kai taikoma, duomenų tvarkytojo atstovui pagal Reglamento (ES) 2016/679 30 straipsnio 2 dalį.
5. Duomenų valdytojas privalo pasirūpinti tuo, kad duomenų tvarkytojui teikiami asmens duomenų tvarkymo nurodymai, nepriklausomai nuo jų formos, būtų teisėti ir neprieštarautų imperatyvioms nacionalinėms ir Europos Sąjungos asmens duomenų apsaugą reglamentuojančioms teisės normoms. Priešingu atveju, duomenų tvarkytojas nedelsdamas privalo informuoti duomenų valdytoją ir savo iniciatyva gali:
5.1. atidėti potencialiai neteisėtų asmens duomenų tvarkymo nurodymų vykdymą protingam laikotarpiui, kuris negali būti ilgesnis nei 14 kalendorinių dienų, jeigu duomenų tvarkytojui kylą pagrįstų abejonių dėl minėtų nurodymų neatitikimo nacionalinei ar tarptautinei teisei;
5.2. atsisakyti vykdyti neteisėtus duomenų valdytojo asmens duomenų tvarkymo nurodymus, pateikdamas motyvuotą atsakymą dėl minėtų nurodymų neatitikimo nacionalinei ar tarptautinei teisei;
5.3. sutikti vykdyti potencialiai neteisėtus arba neteisėtus asmens duomenų tvarkymo nurodymus (kurių neteisėtumas yra nustatytas arba gali būti nustatytas objektyviais įrodymais), prieš tai papildomai informavus duomenų valdytoją ir gavus iš jo atskirą rašytinį patvirtinimą dėl minėtų nurodymų vykdymo. Atsiradus neigiamoms pasekmėms dėl Sutarties 5.3. punkte nurodytų veiksmų, duomenų valdytojas nacionalinių teisės aktu nustatyta tvarka privalo atlyginti dėl jo kaltės atsiradusius tiesioginius duomenų tvarkytojo nuostolius tiek, kiek tai neprieštarauja Reglamento (ES) 2016/679 82 straipsniui ir jame įtvirtintoms Šalių atsakomybių riboms.
6. Ši Sutartis neatleidžia Šalių nuo kitų pareigų, kurios joms taikomos pagal Reglamentą (ES) 2016/679 ar kitus teisės aktus.

III SKYRIUS
KONFIDENCIALUMAS

7. Duomenų tvarkytojas prieigą prie duomenų valdytojo vardu tvarkomų asmens duomenų suteikia tik tiems asmenims, kuriems vadovauja duomenų tvarkytojas, ir kurie yra įpareigoti laikytis

konfidencialumo arba kuriems taikoma teisinė konfidencialumo pareiga, ir tik tuo atveju, jei jiems būtina su jais susipažinti. Šalys užtikrina, kad:
7.1. pasikeitus asmenims, kurie tvarko asmens duomenis, jų prieigos teisės prie duomenų valdytojo asmens duomenų panaikinamos ne vėliau nei paskutinę jo užduočių, dėl kurių jiems būtina prieiga prie duomenų valdytojo asmens duomenų, patikėtų tvarkyti duomenų tvarkytojui, dieną, o tuo atveju jei nutrūksta duomenų tvarkytojo darbuotojo darbo santykiai – ne vėliau nei paskutinę jo darbo dieną.
7.2. asmenų, kuriems suteikta prieiga prie asmens duomenų, sąrašas turi būti periodiškai peržiūrimas ne rečiau kaip kartą kas 6 mėnesius. Vadovaujantis šia peržiūra, tokia prieiga prie asmens duomenų panaikinama, jei tokia prieiga nebereikalinga, todėl asmens duomenys nebegalės būti prieinami tiems asmenims.
8. Duomenų tvarkytojas duomenų valdytojo prašymu įrodo, kad asmenims, kuriems vadovauja duomenų tvarkytojas ir kuriems pavesta tvarkyti asmens duomenis, taikoma Sutarties 7 punkte nurodyta konfidencialumo pareiga.

IV SKYRIUS
DUOMENŲ TVARKYMO SAUGUMAS

9. Vadovaujantis Reglamento (ES) 2016/679 32 straipsniu, duomenų valdytojas ir duomenų tvarkytojas įgyvendina tinkamas technines ir organizacines priemones, kad būtų užtikrintas pavojų atitinkančio lygio saugumas, atsižvelgiant 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.
10. Duomenų valdytojas įvertina fizinių asmenų teisėms ir laisvėms galinčią kilti riziką tvarkant asmens duomenis ir įgyvendina priemones šiai rizikai sumažinti. Priklausomai nuo jų tinkamumo, priemonės gali būti šios:
10.1. asmens duomenų pseudonimizavimas ir (ar) šifravimas;
10.2. galimybė užtikrinti nuolatinį duomenų tvarkymo sistemų ir paslaugų konfidencialumą, vientisumą, prieinamumą ir atsparumą;
10.3. galimybė laiku atkurti prieinamumą ir prieigą prie asmens duomenų, įvykus fiziniam ar techniniam incidentui;
10.4. techninių ir organizacinių priemonių, užtikrinančių duomenų tvarkymo saugumą, reguliaraus testavimo, tikrinimo ir įvertinimo procesas.
11. Pagal Reglamento (ES) 2016/679 32 straipsnį duomenų tvarkytojas, nepriklausomai nuo duomenų valdytojo, taip pat įvertina duomenų tvarkymo riziką, susijusią su asmens duomenų tvarkymo veikla, kuriai atlikti duomenų valdytojas pasitelkė duomenų tvarkytoją, galinčią kilti fizinių asmenų teisėms ir laisvėms, ir įgyvendina priemones šiai rizikai sumažinti. Šiuo tikslu duomenų valdytojas duomenų tvarkytojui pateikia visą informaciją, reikalingą tokiai rizikai nustatyti ir įvertinti.
12. Be to, duomenų tvarkytojas padeda duomenų valdytojui užtikrinti duomenų valdytojo pareigų pagal Reglamento (ES) 2016/679 32 straipsnį vykdymą, teikdamas *inter alia* duomenų valdytojui informaciją apie technines ir organizacines priemones, kurias duomenų tvarkytojas jau įgyvendino pagal Reglamento (ES) 2016/679 32 straipsnį kartu su visa kita informacija, reikalinga duomenų valdytojui įvykdyti duomenų valdytojo pareigas pagal Reglamento (ES) 2016/679 32 straipsnį.
13. Jei, atsižvelgiant į duomenų valdytojo atliktą vertinimą, nustatytai rizikai sumažinti duomenų tvarkytojas turi įgyvendinti papildomas priemones, duomenų valdytojas šias priemones nurodo

Sutarties 3 priede, o duomenų tvarkytojas turi įgyvendinti papildomas priemones ir tas, kurias jau įgyvendino pagal Reglamento (ES) 2016/679 32 straipsnį. Duomenų tvarkytojas turi duomenų valdytojui suteikti visą informaciją, kuri būtina siekiant įrodyti Sutarties X skyriuje nustatytų duomenų tvarkytojo pareigų vykdymą.

V SKYRIUS
KITŲ DUOMENŲ TVARKYTOJŲ PASITELKIMAS

14. Duomenų tvarkytojas turi laikytis Reglamento (ES) 2016/679 28 straipsnio 2 ir 4 dalyse nurodytų reikalavimų, kad galėtų pasitelkti kitą duomenų tvarkytoją (toliau – pagalbinis duomenų tvarkytojas).
15. Duomenų valdytojo sąlygos, kuriomis vadovaujantis duomenų tvarkytojas galės pasitelkti pagalbinius duomenų tvarkytojus, ir duomenų valdytojo įgaliotų pagalbinių duomenų tvarkytojų sąrašas pateikiamos Sąlygų 2 priede.
16. Duomenų tvarkytojas turi bendrąjį rašytinį duomenų valdytojo leidimą, kad jis galėtų pasitelkti pagalbinius duomenų tvarkytojus. Duomenų tvarkytojas raštu informuoja duomenų valdytoją apie bet kokius numatomus pakeitimus, susijusius su pagalbinių duomenų tvarkytojų pasitelkimu ar pakeitimu bent jau prieš 14 kalendorinių dienų, tokiu būdu duomenų valdytojui suteikiant galimybę prieštarauti tokiems pakeitimams iki atitinkamo (-ų) pagalbinio (-ų) duomenų tvarkytojo(-ų) pasitelkimo. Ilgesni išankstinio pranešimo apie specialias papildomo tvarkymo paslaugas laikotarpiai gali būti pateikti Sutarties 2 priede.
17. Kai duomenų tvarkytojas konkrečiai duomenų tvarkymo veiklai duomenų valdytojo vardu atlikti pasitelkia pagalbinį duomenų tvarkytoją, sutartimi ar kitu teisės aktu pagal Sąjungos ar valstybės narės teisę, tam pagalbiniam duomenų tvarkytojui nustatomos tos pačios duomenų apsaugos prievolės, kaip ir prievolės, nustatytos Sutartyje, tarptautiniame ir/ar nacionaliniame teisės akte, visų pirma prievolė pakankamai užtikrinti, kad tinkamos techninės ir organizacinės priemonės bus įgyvendintos tokiu būdu, kad duomenų tvarkymas atitiktų Sutarties ir Reglamento (ES) 2016/679 reikalavimus. Prieš pradėdamas tvarkyti asmens duomenis, duomenų tvarkytojas informuoja pagalbinį duomenų tvarkytoją apie tai, kurio duomenų valdytojo asmens duomenų tvarkymui jis yra pasitelkiamas, nurodydamas duomenų valdytojo tapatybę ir kontaktinius duomenis.
18. Sutarties su pagalbiniu duomenų tvarkytoju kopija ir jos vėlesni pakeitimai, duomenų valdytojo prašymu, pateikiami duomenų valdytojui, tokiu būdu suteikiant duomenų valdytojui galimybę užtikrinti, kad pagalbiniam duomenų tvarkytojui taikomos tos pačios duomenų apsaugos prievolės, kaip yra nustatyta Sutartyje. Duomenų tvarkytojas turi informuoti duomenų valdytoją apie visus netinkamo pagalbinio duomenų tvarkytojo pareigų, nustatytų tokia sutartimi ar kitu teisės aktu, atvejus. Duomenų valdytojui nėra privaloma pateikti asmens duomenų tvarkymo sutarties dėl su verslu susijusių nuostatų, kurios nedaro įtakos su pagalbiniu duomenų tvarkytoju sudarytos sutarties teisinėms asmens duomenų apsaugos sąlygoms.
19. Duomenų tvarkytojas turi susitarti su pagalbiniu duomenų tvarkytoju, jei toks pasitelkiamas, kad pirminio duomenų tvarkytojo bankroto atveju, duomenų valdytojas turi teisę tęsti duomenų tvarkymo santykius su pirminio duomenų tvarkytojo pasitelktu pagalbiniu duomenų tvarkytoju tiesiogiai ir (arba) teikti tiesioginius nurodymus dėl duomenų tvarkymo, pavyzdžiui, nurodyti pagalbiniam duomenų valdytojui ištrinti arba grąžinti asmens duomenis.
20. Duomenų tvarkytojas yra atsakingas už reikalavimą, kad pagalbinis duomenų tvarkytojas laikytųsi bent tų pareigų, kurios duomenų tvarkytojui taikomos pagal Sutartį ir Reglamentą (ES)

2016/679. Jei pagalbinis duomenų tvarkytojas nevykdo asmens duomenų apsaugos prievolių, pirminis duomenų tvarkytojas, su kuriuo sudaryta asmens duomenų tvarkymo sutartis, išlieka visiškai atsakingas duomenų valdytojui už pagalbinio duomenų tvarkytojo prievolių vykdymą. Tai nedaro įtakos duomenų subjektų teisėms pagal Reglamentą (ES) 2016/679, ypač Reglamento (ES) 2016/679 79 ir 82 straipsniuose numatytoms teisėms, duomenų valdytojo ir duomenų tvarkytojo, įskaitant pagalbinius duomenų tvarkytojus, atžvilgiu.

VI SKYRIUS
DUOMENŲ PERDAVIMAS Į TREČIĄSIAS VALSTYBES ARBA TARPTAUTINĖMS ORGANIZACIJOMS

21. Duomenų tvarkytojas asmens duomenis gali perduoti į trečiąsias valstybes ar tarptautinėms organizacijoms tik gavęs duomenų valdytojo dokumentais įformintus nurodymus ir laikantis Reglamento (ES) 2016/679 V skyriaus reikalavimų.
22. Jei asmens duomenis trečiosioms valstybėms ar tarptautinėms organizacijoms reikia perduoti pagal Europos Sąjungos ar jos valstybės narės teisės aktus, kurių turi laikytis duomenų tvarkytojas, nors duomenų valdytojas nedavė nurodymų duomenų tvarkytojui tai atlikti, duomenų tvarkytojas informuoja duomenų valdytoją apie šį teisinį reikalavimą prieš duomenų perdavimą, nebent tas teisės aktas draudžia perduoti tokią informaciją.
23. Duomenų tvarkytojas be duomenų valdytojo dokumentais įformintų nurodymų arba be konkretaus reikalavimo pagal Europos Sąjungos ar jos valstybės narės teisės aktus negali pagal šias Sąlygas:
23.1. perduoti asmens duomenis duomenų valdytojui ar duomenų tvarkytojui trečiojoje valstybėje ar tarptautinėje organizacijoje;
23.2. perduoti asmens duomenų tvarkymą pagalbiniam duomenų tvarkytojui trečiojoje valstybėje;
23.3. leisti, kad asmens duomenis tvarkytų duomenų tvarkytojas trečiojoje valstybėje.
24. Duomenų valdytojo nurodymai ar leidimai dėl asmens duomenų perdavimo į trečiąją valstybę, įskaitant, jei taikoma, asmens duomenų perdavimo į trečiąsias valstybes Reglamento (ES) 2016/679 V skyriuje nustatytus pagrindai, kuriais duomenų valdytojo nurodymai yra grindžiami, pateikiami Sutarties 3 priede.
25. Šios Sutarties sąlygos nėra standartinės duomenų apsaugos sąlygos, apibrėžtos Reglamento (ES) 2016/679 46 straipsnio 2 dalies c ir d punktuose, ir šalys negali remtis šia Sutartimi kaip asmens duomenų perdavimo į trečiąsias valstybes ar tarptautinėms organizacijoms pagrindu pagal Reglamento (ES) 2016/679 V skyrių.

VII SKYRIUS
PAGALBA DUOMENŲ VALDYTOJUI

26. Atsižvelgdamas į duomenų tvarkymo pobūdį, duomenų tvarkytojas, kiek tai įmanoma, padeda duomenų valdytojui tinkamomis techninėmis ir organizacinėmis priemonėmis įvykdyti duomenų valdytojo prievoles atsakyti į prašymus naudotis duomenų subjekto teisėmis, nustatytomis Reglamento (ES) 2016/679 III skyriuje. Tai reiškia, kad duomenų tvarkytojas, kiek tai įmanoma, padeda duomenų valdytojui, kad duomenų valdytojas įgyvendintų:
26.1. teisę būti informuotam renkant asmens duomenis iš duomenų subjekto;
26.2. teisę būti informuotam, kai asmens duomenys yra gauti ne iš duomenų subjekto;
26.3. teisę susipažinti su duomenimis;

26.4. teisę reikalauti ištaisyti duomenis;
26.5. teisę reikalauti ištrinti duomenis („teisę būti pamirštam“);
26.6. teisę apriboti duomenų tvarkymą;
26.7. prievolę pranešti apie asmens duomenų ištaisymą ar ištrynimą arba duomenų tvarkymo apribojimą;
26.8. teisę į duomenų perkeliamumą;
26.9. teisę nesutikti su duomenų tvarkymu;
26.10. teisę, kad nebūtų taikomi sprendimai, pagrįsti vien automatiniu tvarkymu, įskaitant profiliavimą.
27. Be duomenų tvarkytojo prievolės padėti duomenų valdytojui pagal Sutarties 12 punktą, duomenų tvarkytojas, atsižvelgdamas į tvarkymo pobūdį ir duomenų tvarkytojui prieinamą informaciją, taip pat padeda duomenų valdytojui užtikrinti:
27.1. duomenų valdytojo pareigą nedelsiant ir, jei įmanoma, ne vėliau kaip per 72 valandas po to, kai apie tai sužinojo, pranešti apie asmens duomenų saugumo pažeidimą kompetentingai priežiūros institucijai – Valstybinei duomenų apsaugos inspekcijai, nebent asmens duomenų saugumo pažeidimas neturėtų kelti pavojaus fizinių asmenų teisėms ir laisvėms;
27.2. duomenų valdytojo pareigą nepagrįstai nedelsiant pranešti duomenų subjektui apie asmens duomenų pažeidimą, kai asmens duomenų saugumo pažeidimas gali sukelti didelę riziką fizinių asmenų teisėms ir laisvėms;
27.3. duomenų valdytojo pareigą atlikti numatytų asmens duomenų tvarkymo operacijų poveikio duomenų apsaugai vertinimą, kai asmens duomenų tvarkymo būdas gali sukelti didelę riziką fizinių asmenų teisėms ir laisvėms;
27.4. duomenų valdytojo pareigą konsultuotis su kompetentinga priežiūros institucija Valstybine duomenų apsaugos inspekcija prieš pradedant duomenų tvarkymą, jei poveikio duomenų apsaugos vertinimas rodo, kad duomenų tvarkymas sukeltų didelę riziką, jei duomenų valdytojas nesiimtų priemonių tai rizikai sumažinti.
28. Šalys Sutarties 3 priede nustato tinkamas technines ir organizacines priemones, kurias turi taikyti duomenų tvarkytojas siekiant padėti duomenų valdytojui įgyvendinti duomenų subjekto teises ir vykdyti Reglamento (ES) 2016/679 33–36 straipsniuose įtvirtintas pareigas. Tai taikoma prievolėms, nurodytoms Sutarties 27 punkte.

VIII SKYRIUS
PRANEŠIMAS APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ

29. Duomenų tvarkytojas, sužinojęs apie asmens duomenų saugumo pažeidimą, nepagrįstai nedelsdamas apie tai praneša duomenų valdytojui. Duomenų tvarkytojas praneša duomenų valdytojui ne vėliau kaip per 24 valandas po to, kai duomenų tvarkytojas sužinojo apie asmens duomenų saugumo pažeidimą, kad duomenų valdytojas galėtų įvykdyti duomenų valdytojo pareigą pranešti apie asmens duomenų saugumo pažeidimą kompetentingai priežiūros institucijai, pagal Reglamento (ES) 2016/679 33 straipsnį.
30. Sutarties 27.1 papunktyje nurodyta duomenų tvarkytojo pareiga padėti duomenų valdytojui pranešti kompetentingai priežiūros institucijai apie asmens duomenų pažeidimą reiškia, kad duomenų tvarkytojas privalo duomenų valdytojui padėti gauti toliau išvardytą informaciją, kuri, remiantis Reglamento (ES) 2016/679 33 straipsnio 3 dalimi, turi būti nurodyta duomenų valdytojo pranešime kompetentingai priežiūros institucijai:

30.1. asmens duomenų pobūdis, įskaitant, jei įmanoma, atitinkamų duomenų subjektų kategorijos ir apytikslis jų skaičius bei atitinkamų asmens duomenų kategorijos ir apytikslis skaičius;
30.2. tikėtinos asmens duomenų pažeidimo pasekmės;
30.3. priemonės, kurių ėmėsi ar siūlo imtis duomenų valdytojas dėl asmens duomenų pažeidimo, įskaitant, jei reikia, priemones, skirtas sušvelninti galimą neigiamą pažeidimo poveikį;
30.4. bet kokia kita reikšminga informacija, kuri yra ar gali būti reikalinga duomenų valdytojui rengiant pranešimą arba atsakant į papildomus su asmens duomenų saugumo pažeidimu susijusius kompetentingos priežiūros institucijos raštus.
31. Sutarties 3 priede nustatomi visi elementai, kuriuos turi pateikti duomenų tvarkytojas, padėdamas duomenų valdytojui pranešti kompetentingai priežiūros institucijai apie asmens duomenų saugumo pažeidimą. Jei duomenų tvarkytojas duomenų valdytojui pateikia ne visą informaciją apie asmens duomenų saugumo pažeidimą arba vėliau paaiškėja papildoma informacija, duomenų tvarkytojas privalo nepagrįstai nedelsdamas, bet ne vėliau kaip per 12 valandų pateikti papildomą pranešimą duomenų valdytojui, nurodydamas visą trūkstamą informaciją.
32. Duomenų tvarkytojas duomenų valdytojo prašymu, papildomai prie Sutarties 31 punkte nurodytos informacijos, pateikia dokumentų, pagrindžiančių atliktus veiksmus, taikytas priemones ar atliktus vidinius patikrinimus ir jų išvadų, kopijas.

IX SKYRIUS
DUOMENŲ TRYNIMAS IR GRĄŽINIMAS

33. Pasibaigus asmens duomenų tvarkymo paslaugų teikimui, duomenų tvarkytojas privalo duomenų valdytojo pasirinkimu ištrinti visus asmens duomenis, tvarkomus duomenų valdytojo vardu, ir įrodyti duomenų valdytojui, kad tai padarė ir (arba) grąžinti visus asmens duomenis duomenų valdytojui ir ištrinti esamas kopijas, nebent asmens duomenis reikia saugoti pagal Europos Sąjungos ar jos valstybės narės teisės aktus.

X SKYRIUS
DUOMENŲ TVARKYTOJO AUDITAS IR TIKRINIMAS

34. Duomenų tvarkytojas duomenų valdytojui suteikia visą informaciją, reikalingą įrodyti, kad laikomasi Reglamento (ES) 2016/679 28 straipsnyje ir Sutartyje nustatytų pareigų, ir sudaro sąlygas ir padeda duomenų valdytojui ar kitam duomenų valdytojo įgaliotam auditoriui atlikti auditą, įskaitant patikrinimus vietoje.
35. Duomenų valdytojo atliekamam duomenų tvarkytojo ir pagalbinių duomenų tvarkytojų auditui, įskaitant patikrinimus, taikoma Sutarties 3 Priedo 6 punkte nurodyta procedūra.
36. Duomenų tvarkytojas turi suteikti priežiūros institucijoms, kurios pagal galiojančius teisės aktus turi prieigą prie duomenų valdytojo ir duomenų tvarkytojo įrenginių, arba atstovams, veikiantiems tokių priežiūros institucijų vardu, prieigą prie duomenų tvarkytojo fizinių priemonių ar atlikti kitus priežiūros institucijų nurodytus veiksmus auditui ar kitam patikrinimui atlikti. Šalys turi kompetentingų priežiūros institucijų prašymu pateikti šioje Sutartyje nurodytą informaciją, įskaitant auditų rezultatus.

XI SKYRIUS

BAIGIAMOSIOS NUOSTATOS

37. Ši Sutartis įsigalioja nuo jos pasirašymo dienos.
38. Asmens duomenų tvarkymo paslaugų teikimo laikotarpiu Sutartis negali būti nutraukta, jei šalys nėra susitarusios dėl kitos Sutarties, reglamentuojančios asmens duomenų tvarkymo paslaugų teikimą.
39. Jei asmens duomenų tvarkymo paslaugų teikimas yra nutraukiamas, o asmens duomenys ištrinami arba grąžinami duomenų valdytojui pagal Sutarties 33 punktą ir Sutarties 3 Priedo 4 punktą, Sutartis gali būti nutraukiama bet kuriai Šaliai pateikus rašytinį pranešimą.
40. Nedarant poveikio jokioms Reglamento (ES) 2016/679 nuostatoms, duomenų tvarkytojui pažeidus pareigas pagal šią Sutartį, duomenų valdytojas gali nurodyti duomenų tvarkytojui laikinai sustabdyti asmens duomenų tvarkymą, kol pastarasis laikysis šios Sutarties arba Sutartis bus nutraukta. Duomenų tvarkytojas nedelsdamas informuoja duomenų valdytoją, jei dėl kokios nors priežasties jis negali vykdyti Sutarties.
41. Duomenų valdytojas turi teisę nutraukti Sutartį, jeigu:
41.1. duomenų tvarkytojas iš esmės arba nuolat pažeidžia Sutartį arba savo įsipareigojimus pagal Reglamentą (ES) 2016/679;
41.2. duomenų tvarkytojas nesilaiko privalomo teismo arba priežiūros institucijos sprendimo dėl savo įsipareigojimų pagal Sutartį arba Reglamentą (ES) 2016/679;
41.3. duomenų valdytojas sustabdė duomenų tvarkytojo atliekamą asmens duomenų tvarkymą pagal Sutarties 41.1 ir (ar) 41.2 papunkčius ir atitiktis šiai Sutarčiai nėra atkurta per 30 kalendorinių dienų.
42. Sutartis turi pirmenybę prieš bet kokias panašias su asmens duomenų tvarkymu susijusias nuostatas kituose Šalių susitarimuose.
43. Kiekviena Šalis paskiria asmenį, atsakingą už Sutarties vykdymą.

XII SKYRIUS
ŠALIŲ REKVIZITAI, PARAŠAI

Duomenų valdytojo vardu:	Duomenų tvarkytojo vardu:
(parašas)	(parašas)

Sutarties priedai:
1 priedas. Informacija apie asmens duomenų tvarkymą.
2 priedas. Informacija apie pagalbinius duomenų tvarkytojus.
3 priedas. Nurodymai, kaip tvarkyti asmens duomenis

Asmens duomenų tvarkymo sutarties
1 priedas

INFORMACIJA APIE ASMENS DUOMENŲ TVARKYMĄ

1. Informacija apie asmens duomenų tvarkymą:

Detalus duomenų tvarkytojo teikiamų paslaugų aprašymas pateiktas Techninėje specifikacijoje (Paslaugų teikimo sutarties Priedas Nr. 1).

1.1. Duomenų tvarkytojo atliekamo asmens duomenų tvarkymo tikslas yra:

Tinkamai organizuoti degalų apskaitos automatizavimo ir stebėsenos sistemos ir šią sistemą sudarančių elementų, įskaitant informacinių sistemų, programinės ar aparatinės įrangos, informacinių sistemų integracijos / sąveikos techninių sprendimų, diegimą, tinkamą veikimą bei ilgalaikį palaikymą.

1.2. Duomenų tvarkytojo asmens duomenų tvarkymas daugiausia susijęs su (tvarkymo pobūdžiu):

Tarnybinės transporto priemonės ir jos vairuotojo, judėjimo, buvimo vietos ar kitų telemetrinių duomenų perdavimu degalų apskaitos automatizavimo ir stebėsenos sistemai, vaizdo stebėjimu transporto priemonėje ir už jos ribų, sistemos vartotojų / naudotojų paskyrų suformavimu, vartotojų identifikavimo / prieigos kontrolės funkcionalumo diegimu, sistemos vartotojų / naudotojų veiksmų fiksavimu (pvz. operacijų įrašų įrašymas) / analizavimu, telemetrinės įrangos gaunamų duomenų rinkimu / stebėjimu / saugojimu, transporto priemonės ataskaitų formavimu, asmens duomenų apsaugos nustatymų sistemoje pritaikymu pagal duomenų valdytojo nurodymus ar teisės aktus, ataskaitų eksportavimu įvairiais formatais, automatinių pranešimų formavimu / siuntimu, duomenų apsikeitimui su trečiųjų šalių programine įranga reikalingų sąsajų / integracijų diegimu, mokymų organizavimu ir mokymų sertifikatų teikimu.

1.3. Duomenų tvarkymas apima šiuos asmens duomenis:

Darbuotojų identifikaciniai ir kontaktiniai duomenys (vardas, pavardė, pareigos, el. paštas, telefono numeris, vairuotojo kortelės numeris); judėjimo, buvimo vietos ar kiti telemetriniai duomenys; su vairavimo elgsena susiję duomenys; sistemų naudotojo / vartotojo autentifikacijos, prisijungimo ir veiklos sistemose duomenys; vaizdo stebėjimo transporto priemonėje ir už jos ribų duomenys.

1.4. Duomenų tvarkymas apima šias duomenų subjektų kategorijas:

Duomenų valdytojo darbuotojai, naudojantys tarnybines transporto priemones, kurios yra pritaikytos prie degalų apskaitos automatizavimo ir stebėjimo sistemos, bei darbuotojai, kurie atlieka šios sistemos administratoriaus funkcijas. Viešojo saugumo tarnybos pareigūnai, naudojantys duomenų valdytojo transporto priemones. Atskirais atvejais, kai duomenų tvarkytojas atliks transporto priemonių išorinio vaizdo stebėjimo įrangos montavimą, pritaikymą ar šios sistemos priežiūrą, gali būti tvarkomi ir kitų asmenų, patenkančių į vaizdo stebėjimo lauką, duomenys.

1.5. Duomenų tvarkytojas gali tvarkyti asmens duomenis duomenų valdytojo vardu, kai įsigalioja Sutartis. Duomenų tvarkymo trukmė:

Duomenų tvarkytojas pasitelkiamas tvarkyti asmens duomenis kol galioja pagrindinė paslaugų teikimo sutartis.
Duomenų tvarkytojas užtikrina, kad asmens duomenys, įgyvendinus aukščiau apibūdintus mokymus ir įteikus mokymų dalyviams mokymų baigimo sertifikatus bus saugomi tik tiek, kiek tai yra reikalinga paslaugų sutarties įgyvendinimui. Šis reikalavimas nėra taikomas tais atvejais, kai asmens duomenis yra privaloma saugoti pagal galiojančius teisės aktus ir, duomenų valdytojui paprašius, yra gaunamas duomenų tvarkytojo atskiras patvirtinimas apie tai raštu.

Asmens duomenų tvarkymo sutarties
2 priedas

INFORMACIJA APIE PAGALBINIUS DUOMENŲ TVARKYTOJUS

1. Įgalioti pagalbiniai duomenų tvarkytojai:

Įsigaliojus Sutarčiai, duomenų valdytojas leidžia pasitelkti šiuos pagalbinius duomenų tvarkytojus:

Pavadinimas, vardas, pavardė	Įmonės kodas / individualios veiklos pažymėjimo numeris arba verslo liudijimo numeris	Buveinės adresas / gyvenamosios vietos adresas	Asmens duomenų tvarkymo aprašymas

Įsigaliojus Duomenų tvarkymo sutarčiai, Duomenų valdytojas leidžia Duomenų tvarkytojui pasitelkti šiame priede nurodytus subtvarkytojus Duomenų tvarkymo sutartyje nurodytais tikslais. Siekiant pasitelkti minėtus subtvarkytojus asmens duomenų tvarkymui kitais tikslais, būtinas rašytinis Duomenų valdytojo leidimas.

2. Išankstinis pranešimas dėl leidimo suteikimo pagalbiniams duomenų tvarkytojams

Duomenų valdytojas suteikia išankstinį bendrąjį rašytinį leidimą duomenų tvarkytojui pasitelkti pagalbinius duomenų tvarkytojus užtikrinant, kad duomenų tvarkytojas raštu ne vėliau nei prieš 14 dienų informuos duomenų valdytoją apie planuojamą pasitelkti pagalbinį duomenų tvarkytoją ar bet kokį kitą numatomą pakeitimą ir pateiks duomenų valdytojui visą būtiną informaciją, tam, kad duomenų valdytojas galėtų įvertinti ir pareikšti prieštaravimą iki atitinkamo pagalbinio duomenų tvarkytojo pasitelkimo.

Asmens duomenų tvarkymo sutarties
3 priedas

NURODYMAI, KAIP TVARKYTI ASMENS DUOMENIS

1. Duomenų tvarkymo nurodymas

Duomenų tvarkytojas duomenų valdytojo vardu asmens duomenų tvarkymo metu atlieka šiuos veiksmus:

- Duomenų surinkimą;
- Duomenų įrašymą;
- Duomenų peržiūrą;
- Duomenų rūšiavimą;
- Duomenų sugretinimą ar apjungimą su kitais duomenimis (formuojant ataskaitas);
- Duomenų saugojimą;
- Duomenų naudojimą;
- Susipažinimą su duomenimis;
- Duomenų perdavimo integracijų kūrimą;
- Duomenų analizavimą.

2. Duomenų tvarkymo saugumas

Asmens duomenų apsaugos lygis nustatomas atsižvelgiant į įvairius išorinius ir vidinius duomenų saugumą įtakojančius faktorius. Šios duomenų tvarkymo sutarties atžvilgiu ypač svarbu yra tai, kad duomenų tvarkymas yra susijęs su ganėtinai plačia asmens duomenų tvarkymo veikla. Asmens duomenų tvarkymo tikslai bei apimtys yra ganėtinai ženklios, o asmens duomenų tvarkymo pobūdis, kontekstas ir aplinkybės yra susijusios su potencialiai didelį pavojų duomenų subjektų teisėms ir laisvėms keliančia veikla. Nepaisant to asmens duomenų tvarkymo metu nebus tvarkomi specialiųjų kategorijų ar kiti jautresni asmens duomenys, o visi iš duomenų valdytojo arba jo darbuotojų gauti bendrieji asmens duomenys bus tvarkomi duomenų valdytojo ar duomenų tvarkytojo valdomoje infrastruktūroje, prie kurios priėjimą turi tik ribotas asmenų ratas. Remiantis pateiktais apibendrinimais, asmens duomenų tvarkymo veiklai nustatomas **„aukštas“** apsaugos lygis.

Duomenų tvarkytojas turi teisę ir privalo priimti sprendimus dėl techninių ir organizacinių saugumo priemonių naudojimo užtikrinti reikiamą (ir suderintą) duomenų saugumo lygį.

Tačiau duomenų tvarkytojas užtikrina ir įsipareigoja:

1. Organizacinės saugumo priemonės	
1.1. Saugumo valdymas	
1.1.1. Saugumo politika ir asmens	Organizacija turėtų nustatyti savo politiką, kuri, kaip informacijos saugumo politikos dalis, būtų taikoma asmens duomenų tvarkymui.

	duomenų apsaugos procedūros	Organizacijos 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.
		Atsižvelgiant į bendrą saugumo politiką, turi būti sukurtas ir prižiūrimas konkrečių su asmens duomenų saugumu susijusių politikos dokumentų, procedūrų, tvarkų aprašas.
		Saugumo politika turėtų būti peržiūrima kas pusmetį ir, esant būtinybei, pakoreguojama.
1.1.2.	**Vaidmenys ir atsakomybės sritys**	Su asmens duomenų tvarkymu susiję vaidmenys ir atsakomybės turėtų būti aiškiai apibrėžti ir paskirstyti vadovaujantis saugumo politika.
		Vidinių reorganizacijų ar darbo santykių nutraukimo ar pasikeitimo atvejais, turėtų būti aiškiai nustatyta teisių ir atsakomybių atšaukimo bei perdavimo tvarka.
		Reikėtų atlikti aiškų asmenų, atsakingų už konkrečias saugumo užduotis, paskyrimą, įskaitant saugos specialisto arba jam prilyginto asmens paskyrimą.
		Saugos specialistas turi būti oficialiai paskirtas (paskyrimą patvirtinant dokumentais). Saugos specialisto uždaviniai ir atsakomybės turi būti aiškiai nustatyti ir dokumentuoti.
		Saugos specialisto pareigybė ir duomenų apsaugos pareigūno pareigybė, turi būti atskirtos, siekiant sumažinti neleistino ar netyčinio asmens duomenų keitimo ar netinkamo naudojimo galimybes.
1.1.3.	**Prieigos kontrolės politika**	Prieiga prie asmens duomenų suteikiama pagal patvirtintą procedūrą tik duomenų tvarkytojo darbuotojams, kuriems yra reikalinga darbo funkcijoms vykdyti suteikiant minimalią, darbo funkcijoms ar užduotims atlikti būtiną informaciją ir prieigą vadovaujantis „būtina žinoti“ principu.
		Prieigos kontrolės politika turėtų būti išsami ir įforminta dokumentais. Šiame dokumente Organizacija turėtų nustatyti atitinkamas prieigos kontrolės taisykles, prieigos teises ir apribojimus konkretaus vartotojo atliekamiems vaidmenims, susijusiems su asmens duomenų atžvilgiu vykdomais procesais ir procedūromis.
		Prieigos kontrolės vaidmenų atskyrimas (pvz. prašymas naudotis prieiga, prieigos suteikimas, prieigos administravimas) turėtų būti aiškiai apibrėžtas ir įformintas dokumentais.
		Privilegijuotoji prieiga turi būti apribota ir leidžiama tik tiems duomenų tvarkytojo darbuotojams, kuriems to reikia dėl duomenų valdytojui teikiamų paslaugų ir kuriems duomenų valdytojas priskyrė/suteikė administratoriaus teises.
		Tam tikros pareigybės, turinčios dideles prieigos teises, turi būti aiškiai apibrėžtos ir priskirtos tik ribotam darbuotojų skaičiui.
1.1.4.	**Išteklių/turto valdymas**	Organizacija turi turėti IT išteklių (kompiuterinės įrangos, programinės įrangos ir tinklo), naudojamų asmens duomenų tvarkymui, registrą. Registre turėtų būti nurodyta bent jau ši informacija: IT ištekliai, tipas (pvz. serveris,

	darbo stotis), vieta (fizinė ar elektroninė). Registro tvarkymo ir atnaujinimo funkcija turėtų būti priskirta konkrečiam asmeniui (pvz. IT specialistui).
	Turėtų būti apibrėžti ir dokumentais įforminti prie tam tikrų išteklių prieigą turinčių asmenų vaidmenys.
	Visos pareigybės, turinčios prieigą prie IT išteklių, turi būti apibrėžtos ir patvirtintos dokumentais.
1.1.5. Pakeitimų valdymas	Turėtų būti patvirtinta išsami pakeitimų valdymų politika, kurioje turėtų būti numatytas: pakeitimų įdiegimo procesas, vaidmenys/vartotojai, kurie turi teisę atlikti pakeitimus, pakeitimų įdiegimo terminai. Pakeitimų politika turėtų būti reguliariai atnaujinama.
	Organizacija turėtų užtikrinti, kad visi IT sistemos pakeitimai būtų užregistruoti ir stebimi konkretaus asmens (pvz. IT ar saugumo pareigūno).
	Turi būti įdiegta išsami ir dokumentais pagrįsta IT pakeitimų valdymo politika. Keitimų valdymo politiką turi apibrėžti: pokyčių įvedimo ir įdiegimo procedūras, pareigybes ir vartotojus, kurių teisės buvo pakeistos, pokyčių įdiegimo laiko terminus.
1.2. Reagavimas į incidentus ir veiklos tęstinumas	
1.2.1. Incidentų valdymas/asmens duomenų saugumo pažeidimai	Asmens duomenų saugumo pažeidimai turi būti valdomi pagal patvirtintą procedūrą. Turėtų būti parengtas reagavimo į incidentus planas, nustatantis išsamias procedūras, siekiant užtikrinti efektyvų ir tinkamą reagavimą į su asmens duomenų saugumu susijusius incidentus.
	Apie visus saugumo incidentus ir pažeidimus, susijusius su teikiamomis paslaugomis ar tvarkomais asmens duomenimis, privalo būti pranešta duomenų valdytojui duomenų tvarkymo sutartyje nustatyta tvarka ir terminais ir toliau asmens duomenų saugumo pažeidimai turi būti valdomi atsižvelgiant į patvirtintas procedūras ir duomenų valdytojo nurodymus ar prašymus.
	Visi incidentai, susiję su tvarkomais asmens duomenimis privalo būti registruojami ir dokumentuojami bei valdomi pagal patvirtintą procedūrą.
	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.
1.2.2. Veiklos tęstinumas	Organizacija turėtų nustatyti pagrindines procedūras ir kontrolės mechanizmus, kurie turėtų būti taikomi, siekiant užtikrinti asmens duomenis tvarkančios informacinės sistemos tęstinumo ir prieinamumo reikalaujamą lygį (incidentų/asmens duomenų saugumo pažeidimo atvejais).
	Veiklos tęstinumo politika arba veiklos tęstinumo planas (toliau – **VTP**) turėtų būti išsamūs, įforminti atskiru dokumentu arba įtraukti į bendrąją asmens duomenų saugumo politiką, kaip sudėtinė jos dalis. VTP turėtų būti numatyti aiškūs veiksmai ir vaidmenų pasiskirstymas palaikant veiklos tęstinumą.
	Veiklos tęstinumo plane turi būti apibrėžtas garantuojamas paslaugų kokybės lygis (angl. Service-level agreement), kuris nustatomas pagrindiniams veiklos procesams, kurie užtikrina asmens duomenų saugumą.

	Organizacijoje turi būti paskirti darbuotojai, turintys reikiamą atsakomybę, įgaliojimus ir kompetenciją valdyti veiklos tęstinumą saugumo incidento, asmens duomenų saugumo pažeidimo atvejais.
	Turi būti numatyta alternatyvi infrastruktūros priemonė organizacijos darbui, atsižvelgiant į organizaciją ir jai priimtiną IT sistemų prastovą.
1.3. Žmogiškieji ištekliai	
1.3.1. Personalui taikomi konfidencialumo įsipareigojimai	Organizacija turėtų užtikrinti, kad visi darbuotojai suprastų su asmens duomenų tvarkymu susijusias savo atsakomybes ir įsipareigojimus. Vaidmenys ir atsakomybės turėtų būti aiškiai išdėstyti prieš priimant į darbą ir (arba) įdarbinimo metu.
	Darbuotojai, kuriems yra suteiktos prieigos teisės prie asmens duomenų, prieš pradedant vykdyti savo pareigas, turi būti supažindinti su asmens duomenų ir informacijos saugumo dokumentais bei informuoti apie asmens duomenų pobūdį, asmens duomenų apsaugą reglamentuojančių teisės aktų reikalavimus bei įsipareigoję saugoti asmens duomenų, kuriuos sužinojo vykdydami savo funkcijas, paslaptį tiek darbo metu, tiek ir nutraukus darbo santykius.
	Darbuotojai, atsakingi už aukštos rizikos asmens duomenų tvarkymo operacijas (specialiųjų kategorijų asmens duomenys arba duomenys susiję su apkaltinamaisiais nuosprendžiais ar nusikalstama veika), turi laikytis konkrečių jiems taikomų konfidencialumo sąlygų (pagal jų darbo sutartį ar kitą teisės aktą).
1.3.2. Mokymai	Reguliariai turi būti vykdomi darbuotojų informacijos ir asmens duomenų saugumo mokymai, darbuotojai turi būti nuolat informuojami apie informacijos ir asmens duomenų saugumo politikų bei procedūrų, susijusių su jų darbu, teisės aktų pokyčius. Neapsiribojant nurodytomis priemonėmis, darbuotojai turėtų būti supažindinami su naujomis praktinėmis grėsmėmis asmens duomenų apsaugai.
	Organizacija turi rengti struktūrines nuolatines personalo mokymų programas, tarp kurių būtų ir speciali programa, skirta mokyti naujus darbuotojus (duomenų apsaugos tema).
	Kiekvienais metais turi būti parengtas ir įgyvendintas mokymų planas, kuriame būtų nustatyti siektini tikslai ir uždaviniai.
2. Techninės saugumo priemonės	
2.1. Prieigos kontrolė ir autentifikavimas	Turėtų būti įdiegta prieigos kontrolės sistema, taikoma visiems IT sistema besinaudojantiems vartotojams. Sistema turėtų leisti sukurti, patvirtinti, peržiūrėti ir ištrinti vartotojų paskyras.
	Prieigos kontrolės politikos ir sistemos pagrindu turėtų būti nustatytas autentifikavimo mechanizmas, leidžiantis prisijungti prie IT sistemos. Turėtų būti naudojama bent jau vartotojo vardo/slaptažodžio kombinacija.
	Turi būti užtikrinama naudotojų prieigos kontrolė naudojant mažiausiai 8 ženklų ilgio stiprų slaptažodį (privilegijuotiems naudotojams – mažiausiai 12 ženklų ilgio slaptažodis bei papildomai, esant galimybėms, naudojami kelių faktorių autentifikavimo sprendimai (MFA), slaptažodžiai turi būti keičiami periodiškai ne rečiau kaip kartą per 2 mėn.

	Vartotojo slaptažodžiai privalo būti saugomi „hash“ (šifruotų slaptažodžių) forma.
	Turi būti nustatytos ir dokumentais patvirtintos slaptažodžių naudojimo taisyklės (galiojimo laikas, nesėkmingų bandymų įvesti slaptažodį skaičius, slaptažodžio/paskyros blokavimas).
	Prieigos kontrolės sistema turėtų sugebėti aptikti ir neleisti naudoti slaptažodžių, kurie neatitinka nustatyto sudėtingumo lygio.
	Privilegijuotiems vartotojams (pvz., sistemų administratoriams) prisijungimui prie asmens duomenų tvarkymo sistemų turi būti taikomas dviejų veiksnių autentifikavimas. Visais atvejais, kai į tokias sistemas jungiamasi ne iš vidinio kompiuterių tinklo, turi būti naudojamas dviejų veiksnių autentifikavimas. Autentifikavimo veiksniais gali būti slaptažodžiai, saugumo žetonai, USB raktai su slapta žyma, biometriniai duomenys ir kt.
	Turi būti naudojamas įrenginio autentifikavimas, garantuojantis, kad 21 asmens duomenys tvarkomi tik naudojant konkrečius tinklo įrenginius (pvz., 802.1X, RADIUS ir kt.).
2.2. Operacijų įrašų registravimas ir stebėsena	Turėtų būti aktyvuojami kiekvienos sistemos/programos, naudojamos asmens duomenų tvarkymui, atliktų operacijų įrašai (log files). Juose turėtų matytis visos prieigos prie duomenų (peržiūra, keitimas, ištrynimas ir t.t.).
	Turėtų būti registruojami sistemos administratorių ir sistemos operatorių veiksmai, įskaitant papildomų teisių vartotojui suteikimą/ištrynimą/pakeitimą.
	Neturėtų būti numatyta galimybė ištrinti ar pakeisti operacijų įrašų (log files) turinį. Prisijungimai prie operacijų įrašų (log files) taip pat turėtų būti registruojami kartu su neįprastų veiksmų stebėsena.
	Visi sistemų administratorių ir operatorių veiksmai (taip pat ir jų atliekamas vartotojo teisių papildymas, panaikinimas, keitimas) turi būti registruojami.
	Stebėsenos sistema turi apdoroti techninius įrašus, ruošti sistemos būklės ataskaitas ir įspėti apie galimus pavojus.
2.2.1. Darbo stoties saugumas	Vartotojams neturėtų būti sudaryta galimybė deaktyvuoti ar apeiti saugumo nustatymus.
	Vartotojai neturėtų galėti įdiegti ar išjungti nesankcionuotų programinių įrangų.
	Duomenų bazių ir programų serveriai turėtų tvarkyti tik tuos asmens duomenis, kurių reikia siekiant tikslų, dėl kurių jie buvo surinkti.
	Konkrečioms saugomoms byloms ar įrašams apsaugoti turėtų būti naudojamas šifravimas, įdiegiant atitinkamą programinę ar techninę įrangą.
	Duomenų bazėse turi būti taikomi pseudonimizavimo metodai, atskiriant tiesioginius identifikatorius nuo esamų sąsajų su kitais duomenimis.
	Neturėtų būti leidžiama atsisiųsti asmens duomenų iš darbo vietos į išorines atminties rinkmenas (pvz. USB, DVD, išorinius kietuosius diskus).

	Duomenų bazėje turi būti taikomi autorizuotų užklausų, šifruotos paieškos ir kiti privatumo užtikrinimo metodai.
2.3. Tinklo/ryšio saugumas	Kai jungiamasi per internetą, ryšys turėtų būti perduodamas užšifruotu pavidalu naudojant kriptografinius protokolus (TLS/SSL).
	Duomenų bazių ir programų serveriai turėtų tvarkyti tik tuos asmens duomenis, kurių reikia siekiant tikslų, dėl kurių jie buvo surinkti.
	Duomenų srautas į ir iš informacinės sistemos turėtų būti stebimas ir kontroliuojamas naudojant ugniasienes ir įsilaužimų aptikimo sistemas.
	Belaidis ryšys prie IT sistemų turi būti leidžiamas tik tam tikriems vartotojams ir procesams. Belaidžio ryšio potinklis turi būti atskirtas nuo kitų potinklių. Belaidė prieiga turi būti apsaugota patikimais šifravimo mechanizmais.
	Informacijos sistemos tinklas turėtų būti atskirtas nuo kitų duomenų valdytojo tinklų.
	Prieiga prie IT sistemų turėtų būti atliekama tik iš leistinų darbo vietų ir (arba) įrenginių (pvz., naudojant MAC filtravimą ar leisti prisijungti tik iš konkrečių leistinų IP adresų).
	Duomenų bazės, kuriose yra asmens duomenys turi būti anonimizuojamos (šifravimo būdu arba suteikiant pseudonimus).
	Turėtų būti pritaikyti pasirinktini privatumo išsaugojimo metodai duomenų bazių lygyje, tokie kaip autorizuoti paklausimai, privatumą išsaugojantis duomenų bazių paieškų vykdymas, užšifruotas ieškojimas ir kt.
	Tarnybinėms stotims ir jose esančiai programinei įrangai, kuri yra naudojama asmens duomenims tvarkyti, prisijungimas prie interneto neturi būti leidžiamas.
	Informacinės sistemos tinklas turi būti atskirtas nuo kitų duomenų valdytojo/tvarkytojo tinklų.
	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.
2.4. Duomenų atsarginės kopijos	Turėtų būti apibrėžtos, dokumentais įformintos ir aiškiai su vaidmenimis ir atsakomybėmis susiję atsarginių kopijų ir duomenų atkūrimo procedūros.
	Atsarginėms kopijoms turėtų būti taikomas atitinkamas fizinės ir aplinkos apsaugos lygis, atitinkantis duomenų, kurių kopijos yra daromos, apsaugos standartus.
	Turėtų būti reguliariai daromos pilnos atsarginės kopijos.
	Atsarginės kopijos turi būti reguliariai testuojamos, siekiant užtikrinti, kad jos galėtų būti patikimai naudojamos ekstremalioje situacijoje.
	Planuotos prieauginės atsarginės kopijos (angl. *incremental backups*) turėtų būti daromos periodiškai.
	Reguliarus atsarginių kopijų kūrimas ar bent reguliarus papildantysis (angl. incremental) atsarginių kopijų kūrimas turi būti atliekamas bent kartą per parą.

	Atsarginės kopijos turėtų būti saugiai laikomos skirtingose vietose arba šlaitiniuose (laikmenose).
	Atsarginės kopijos turi būti šifruojamos ir saugiai laikomos visiškai atjungus (angl. offline) nuo kompiuterinių tinklų.
2.5. Duomenų ištrynimas, sunaikinimas	Popieriniai dokumentai, kuriose buvo laiko, saugomi, renkami asmens duomenys, turi būti supjaustomi/sunaikinami, kai jie nebėra yra reikalingi užsibrėžtų asmens duomenų tvarkymo tikslų įgyvendinimui.
	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.
	Prieš šalinant asmens duomenis iš laikmenų, turi būti atlikti visų šalinamų laikmenų daugybiniai programinės įrangos perrašymai (angl. Multiple passes of software-based overwriting).
	Jei saugiems 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.
	Jei saugiems 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.
	Po duomenų ištrynimo reikėtų imtis papildomų priemonių, pvz., gali būti atliktas nepageidaujamos magnetinės informacijos pašalinimas (išmagnetinimas). Priklausomai nuo konkretaus atvejo, reikėtų papildomai įvertinti fizinio sunaikinimo galimybes.
2.6. Fizinis saugumas	IT sistemos infrastruktūros fizinis perimetras turėtų būti neprieinamas leidimo neturintiems darbuotojams.
	Turėtų būti nustatytos saugumo zonos ir patekimo į jas kontrolė. Turėtų būti naudojamas ir stebimas fizinis registracijos žurnalas ar elektroninė kontrolės sistema, fiksuojanti patekimą į saugumo zonas.
	Visose saugumo zonose turėtų būti įdiegtos įsilaužimo aptikimo sistemos.
	Nenaudojamos saugumo zonos turėtų būti fiziškai užrakintos ir reguliariai tikrinamos.
	Serverinėje turi būti įdiegta automatinė gaisro apsaugos sistema, tikslios kontrolės oro kondicionavimo sistema ir nenutrūkstamas elektros energijos tiekimas (UPS).
	Palaikymo paslaugas iš išorės teikiantiems asmenims turėtų būti nustatytas ribotas patekimas į saugumo zonas.

	Laisvos saugios zonos turi būti fiziškai rakinamos ir periodiškai patikrinamos

3. Pagalba duomenų valdytojui

Duomenų tvarkytojas, kiek tai įmanoma ir atsižvelgiant į toliau nurodytą pagalbos sritį bei apimtį, padeda duomenų valdytojui pagal Sutarties 25–27 punktus įgyvendinti šias technines bei organizacines priemones:

- Duomenų subjektų prašymai turi būti nepagrįstai nedelsiant, bet ne vėliau nei per 2 darbo dienas nuo prašymo gavimo, persiųsti duomenų valdytojui el. paštu: dap@ltou.lt;
- Esant duomenų valdytojo prašymui, duomenų tvarkytojas parengia atsakymus duomenų subjektams pagal duomenų valdytojo nurodymus;
- Įvykus asmens duomenų saugumo pažeidimui, duomenų tvarkytojas informuoja duomenų valdytoją, ne vėliau kaip per 24 val. nuo to momento, kai sužinojo apie pažeidimą momento pateikdamas informaciją el. paštu: dap@ltou.lt;
- Laikytis ir taikyti kitas priemones, kurios gali būti pateiktos duomenų valdytojo raštišku nurodymu.

4. Duomenų saugojimo laikotarpis/duomenų trynimo procedūros

Asmens duomenys saugomi Paslaugos teikimo sutarties galiojimo laikotarpį, kuriam pasibaigus, Duomenų tvarkytojas rankiniu arba automatiniu būdu, kuris neleistų duomenų nesankcionuotai atkurti, ištrina asmens duomenis iš savo valdomų, naudojamų arba administruojamų informacinių sistemų ir kitų šaltinių, arba grąžina asmens duomenis, atsižvelgiant į Sutarties 32 punkto reikalavimus, nebent pasirašęs Sutartį duomenų valdytojas pakeičia pirminį duomenų tvarkytojo pasirinkimą. Atsižvelgiant į Sutartį, tokie pakeitimai turi būti pagrįsti dokumentais.

5. Duomenų tvarkymo vieta

Atsižvelgiant į Sutartį, be išankstinio rašytinio duomenų valdytojo leidimo asmens duomenys negali būti tvarkomi kitose vietose, išskyrus šias:

- Duomenų tvarkytojo vidinėje informacinėje sistemoje arba duomenų tvarkytojo valdomuose asmens duomenų tvarkymo ištekliuose ar infrastruktūroje;
- Duomenų tvarkytojo už Sutarties vykdymą ir paslaugų teikimą atsakingų darbuotojų darbo vietoje įrengtuose elektroniniuose prietaisuose ir jų fizinėse laikmenose;
- Duomenų valdytojo degalų apskaitos sistemoje arba duomenų tvarkytojo valdomuose asmens duomenų tvarkymo ištekliuose ar infrastruktūroje.

Asmens duomenų tvarkymo veiksmai ir operacijos bus atliekamos neperžengiant Europos Sąjungos/EEE teritorijos ir jurisdikcijos ribų.

6. Procedūros, skirtos duomenų valdytojo atliekamiems duomenų tvarkytojo asmens duomenų tvarkymo auditams, įskaitant patikrinimams vietoje

Duomenų valdytojas arba duomenų valdytojo atstovas, Sutarties galiojimo laikotarpiu, gali pasinaudoti savo Reglamento (ES) 2016/679 28 str. 3 d. h p. nustatyta teise fiziškai patikrinti tas vietas, kuriose duomenų tvarkytojas tvarko asmens duomenis, įskaitant fizines priemones, taip pat informacines sistemas, naudojamas ir susijusias su duomenų tvarkymu, siekiant įsitikinti, ar duomenų tvarkytojas ir jo nurodyti pagalbiniai duomenų tvarkytojai laikosi Reglamento (ES) 2016/679 ir LR asmens duomenų teisinės apsaugos įstatymo Nr. I-1374 reikalavimų asmens duomenų apsaugos srityje.

Duomenų valdytojas arba jo atstovas apie savo norą, atlikti informacinių technologijų infrastruktūros patikrinimą, turi pranešti duomenų tvarkytojui raštu prieš 7 darbo dienas. Šios pranešimo tvarkos duomenų valdytojas arba jo atstovas gali nesilaikyti tais atvejais, kai jam kyla pagrįstų abejonių dėl duomenų tvarkytojo vykdomų asmens duomenų tvarkymo veiksmų ir operacijų, kurios gali turėti neigiamą poveikį asmens duomenų saugumui.