SUSITARIMAS NR. 6PS-21-199
DĖL 2021-06-22 SUTARTIES NR. 6PS-21-144 IR 2019-04-15 SUTARTIES NR. 6PS-19-113 KEITIMO

Valstybės įmonė Lietuvos oro uostai, buveinės adresas Rodūnios kelias 10A, Vilnius, juridinio asmens kodas 120864074, atstovaujama generalinio direktoriaus Mariaus Gelžinio, veikiančio pagal įmonės įstatus (toliau – **Klientas**),
ir
Uždaroji akcinė bendrovė „Archyvita“, buveinės adresas Draugystės g. 19, Kaunas, juridinio asmens kodas 135761379, atstovaujama Direktorės Sigitos Varneckienės, veikiančio (-s) pagal įmonės įstatus (toliau –**Paslaugų teikėjas**),

toliau kartu vadinami **Šalimis**, atsižvelgdami į tai, kad:

1. Šalys:
   1.1. 2021 m. birželio 22 d. sudarė dokumentų tvarkymo paslaugų (toliau – **Paslaugos**) pirkimo-pardavimo sutartį Nr. 6PS-21-144 (toliau – **Sutartis**), kuria Paslaugų teikėjas įsipareigojo per Sutartyje nurodytą Paslaugų teikimo terminą suteikti Techninėje specifikacijoje nurodytas Paslaugas kaip numatyta Sutartyje ir pašalinti Paslaugų trūkumus (jei tokių būtų), o Klientas įsipareigojo Sutartyje numatyta tvarka priimti tinkamai suteiktas Paslaugas bei sumokėti Paslaugų teikėjui Sutartyje numatytą kainą.
   1.2. 2019 m. balandžio 15 d. sudarė dokumentų saugojimo privačiame archyve paslaugų (toliau – **Paslaugos**) pirkimo-pardavimo sutartį Nr. 6PS-19-113 (toliau – **Sutartis**), kuria Paslaugų teikėjas įsipareigojo per Sutartyje nurodytą Paslaugų teikimo terminą suteikti Techninėje specifikacijoje nurodytas Paslaugas kaip numatyta Sutartyje ir pašalinti Paslaugų trūkumus (jei tokių būtų), o Klientas įsipareigojo Sutartyje numatyta tvarka priimti tinkamai suteiktas Paslaugas bei sumokėti Paslaugų teikėjui Sutartyje numatytą kainą.
2. Sutarties vykdymui yra būtinas asmens duomenų tvarkymas, todėl, atsižvelgiant į 2018 m. gegužės 25 d. įsigaliojusio Bendrojo duomenų apsaugos reglamento nuostatas, atsirado poreikis pakeisti Sutartį papildant ją nuostatomis dėl asmens duomenų tvarkymo. Sutartis keičiama Šalims pasirašant asmens duomenų tvarkymą Sutarties apimtyje reglamentuojantį susitarimą (Priedas Nr. 1).
3. Pirkimo sutartis jos galiojimo laikotarpiu keičiama neatliekant naujos pirkimo procedūros, nes pakeitimas, neatsižvelgiant į jo vertę, nėra esminis, pakeitimu nenustatoma tokia nauja sąlyga, kurią įtraukus į pradinį pirkimą būtų buvę galima priimti kitų kandidatų paraiškų, dalyvių pasiūlymų ar pirkimas būtų sudominęs daugiau tiekėjų; dėl pakeitimo ekonominė pirkimo sutarties ar preliminariosios sutarties pusiausvyra nepasikeičia tiekėjo, su kuriuo sudaryta ši sutartis, naudai taip, kaip nebuvo aptarta pradinėje sutartyje; pakeitimu nepadidėja pirkimo sutarties ar preliminariosios sutarties apimtis; tiekėjo, su kuriuo sudaryta pirkimo sutartis ar preliminarioji sutartis, nepakeičia naujas tiekėjas, kaip tai numatyta Lietuvos Respublikos pirkimų, atliekamų vandentvarkos, energetikos, transporto ar pašto paslaugų srities perkančiųjų subjektų, įstatymo (toliau – **PĮ**) 97 str. 1 d. 5 p.

Šalys, vadovaudamosi PĮ 97 str. 1 d. 5 p. bei aukščiau minėtomis aplinkybėmis sudarė šį susitarimą (toliau – **Susitarimas**) ir susitarė:

1. Pakeisti Sutartis pasirašant asmens duomenų tvarkymą Sutarties apimtyje reglamentuojantį susitarimą (Priedas Nr. 1).
2. Kitos Sutarčių sąlygos, nepaminėtos šiame Susitarime, lieka nepakitusios ir Šalys patvirtina iš jų kylančias prievoles.
3. Susitarimas įsigalioja Šalims jį pasirašius. Susitarimo pasirašymo diena yra laikoma diena, kurią Susitarimą pasirašė abi Šalys. Tuo atveju, jeigu Šalys Susitarimą pasirašė skirtingomis dienomis, Susitarimo pasirašymo diena yra laikoma ta diena, kurią Susitarimą pasirašė paskutinė iš Šalių. Jeigu Susitarimo pasirašymo datą nurodė tik viena iš Šalių, laikoma, kad abi Šalys pasirašė tą pačią dieną.
4. Susitarimas yra neatskiriama Sutarties dalis.
5. Susitarimas sudarytas dviem vienodą juridinę galią turinčiais egzemplioriais, po vieną kiekvienai Šaliai.

PRIDEDAMA. Susitarimas dėl asmens duomenų tvarkymo, 20 lapų.

KLIENTAS	**PASLAUGŲ TEIKĖJAS**
Valstybės įmonė Lietuvos oro uostai	**Uždaroji akcinė bendrovė „Archyvita“**
Generalinis direktorius	Direktorė
Marius Gelžinis	Sigita Varneckienė
_____	_____
(parašas, pasirašymo data)	*(parašas, pasirašymo data)*

SUSITARIMAS DĖL ASMENS DUOMENŲ TVARKYMO Nr. 6PS-21-

2021 m. rugsėjo d.

Vilnius

Valstybės įmonė Lietuvos oro uostai, juridinio asmens kodas 120864074, registruotos buveinės adresas Rodūnios kelias 10A, LT-02189, Vilnius (toliau – **Duomenų valdytojas**), atstovaujamas generalinio direktoriaus Mariaus Gelžinio, veikiančio pagal įstatus,

ir

UAB „Archyvita“, juridinio asmens kodas 135761379, registruotos buveinės adresas Draugystės g. 19, Kaunas (toliau – **Duomenų tvarkytojas, Organizacija**), atstovaujamas direktorės Sigitos Varneckienės, veikiančio pagal įstatus,

toliau Duomenų valdytojas ir Duomenų tvarkytojas kartu vadinami Šalimis, o kiekvienas atskirai – Šalimi;

ATSIŽVELGDAMOS Į TAI, KAD:

(A) Pagal paslaugų teikimo sutartis Nr. 6PS-21-144 ir Nr. 6PS-19-113 (toliau – **Sutartys**) Duomenų tvarkytojas įsipareigoja teikti dokumentų tvarkymo bei dokumentų saugojimo privačiame archyve paslaugas Duomenų valdytojui, kurių metu Duomenų tvarkytojas turi prieigą prie Duomenų valdytojo tvarkomų Asmens duomenų ir Duomenų valdytojo vardu tvarko Asmens duomenis;

(B) Sutarčių paslaugų teikimui yra būtinas Duomenų valdytojo tvarkomų Asmens duomenų ir kitos informacijos tvarkymas;

(C) Šalys, atsižvelgdamos į tai, kad 2018 m. gegužės 25 d. įsigaliojo Bendrasis duomenų apsaugos reglamentas (toliau – **Reglamentas**);

(D) Reglamentas reikalauja, kad duomenų valdytojai pasitelktų tik tuos duomenų tvarkytojus, kurie pakankamai užtikrina, kad tinkamos techninės ir organizacinės priemonės bus įgyvendintos tokiu būdu, kad duomenų tvarkymas atitiktų Reglamento reikalavimus ir būtų užtikrinta duomenų subjekto teisių apsauga;

(E) Reglamentas taip pat reikalauja, kad duomenų tvarkytojo atliekamas Asmens duomenų tvarkymas būtų reglamentuojamas susitarimu, kuriame būtų Reglamente aprašyti privalomi įpareigojimai duomenų tvarkytojui;

(F) Duomenų valdytojas yra pasitelkęs Duomenų tvarkytoją pagal Sutartis tam tikroms Asmens duomenų tvarkymo veikloms atlikti Duomenų valdytojo vardu pagal Duomenų valdytojo nurodymus, Šalys, siekdamos tinkamai įgyvendinti Reglamento reikalavimus sudarė šį Susitarimą dėl asmens duomenų tvarkymo (toliau – **Susitarimas**).

1. Sąvokos

1.1. Jei Susitarimo kontekstas nereikalauja kitos reikšmės, šiame Susitarime, įskaitant jo preambulę, ir jo priedus pateiktos sąvokos turi šias reikšmes:

Asmens duomenys	bet kokia informacija apie fizinį asmenį, kurio tapatybė nustatyta arba kurio tapatybę galima nustatyti; fizinis asmuo, kurio tapatybę galima nustatyti, yra asmuo, kurio tapatybę tiesiogiai arba netiesiogiai galima nustatyti, 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;
Asmens duomenų saugumo pažeidimas	saugumo pažeidimas, dėl kurio tyčia arba neteisėtai sunaikinami, prarandami pakeičiami, be leidimo atskleidžiami persiųsti, saugomi arba kitaip tvarkomi asmens duomenys arba prie jų be leidimo gaunama prieiga;
Pagalbinis tvarkytojas	bet kuris pagal šio Susitarimo sąlygas Duomenų tvarkytojo pasitelktas duomenų tvarkytojas, tvarkantis Duomenų valdytojo pateiktus asmens duomenis;
Taikomi teisės aktai	reiškia Reglamentą, taip pat galiojančius Lietuvos Respublikos įstatymus, įskaitant, tačiau neapsiribojant, Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymą, Lietuvos Respublikos elektroninių ryšių įstatymą, taip pat Valstybinės duomenų apsaugos inspekcijos (toliau – **Priežiūros institucija**) rekomendacijas bei gaires ir kitus galiojančius Europos Sąjungos, Lietuvos Respublikos teisės aktus, valstybinės valdžios ir valdymo bei savivaldos organų sprendimus, nutarimus, įsakymus, nurodymus, potvarkius, leidimus, licencijas, taip pat kitus poįstatyminius aktus;
Asmens duomenų tvarkymas	bet kokia automatizuotomis arba neautomatizuotomis priemonėmis su asmens duomenimis ar asmens duomenų rinkiniais atliekama operacija ar operacijų seka, kaip 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.

1.2. Šiame Susitarime, jei kontekstas nereikalauja kitaip, žodžiai vienaskaitoje apima ir daugiskaitą, ir atvirkščiai.

1.3. Šiame Susitarime, jei kontekstas nereikalauja kitaip, nuoroda į straipsnį, punktą ar priedą reiškia nuorodą į tą konkretų šio Susitarimo straipsnį, punktą ar priedą.

1.4. Susitarimo pavadinimas ar straipsnių pavadinimai naudojami tik dėl patogumo ir neturi įtakos jokios Susitarimo nuostatos interpretavimui.

2. Susitarimo dalykas

2.1. Teikdamas paslaugas pagal Sutartį Duomenų tvarkytojas, tvarkys Asmens duomenis Duomenų valdytojo vardu. Šalys, siekdamos užtikrinti, kad Asmens duomenys būtų tvarkomi, laikantis Taikomų teisės aktų reikalavimų, sudarė šį Susitarimą.

2.2. Esant prieštaravimams tarp Susitarimo ir Sutarties nuostatų dėl Asmens duomenų tvarkymo, vadovaujamasi Susitarimo nuostatomis, išskyrus, kai Susitarime nustatyta kitaip.

2.3. Kai Susitarime minimas Duomenų tvarkytojas, atitinkamos Susitarimo nuostatos taikytinos ir bet kuriam Duomenų tvarkytojo pasitelktam Pagalbiniam tvarkytojui.

3. Duomenų tvarkytojo įsipareigojimai

3.1. Duomenų tvarkytojas įsipareigoja tvarkyti Asmens duomenis tik laikydamasis Taikomų teisės aktų reikalavimų, Sutarties, Susitarimo nuostatų ir Susitarimo 1 priede išdėstytų Duomenų valdytojo nurodymų dėl Asmens duomenų tvarkymo. Šalys laikosi Taikomuose teisės aktuose nustatytų įpareigojimų. Jeigu Duomenų tvarkytojas nėra gavęs dokumentais įformintų nurodymų (instrukcijų) dėl Asmens duomenų tvarkymo, kurie reikalingi jo įsipareigojimams pagal Susitarimą vykdyti, jis nedelsdamas informuoja apie tai Duomenų valdytoją ir veikia taip, kad kuo geriausiai apsaugotų Duomenų valdytojo interesus, kol minėti nurodymai bus pateikti.

3.2. Duomenų tvarkytojas neturi teisės:

3.2.1. rinkti arba paskelbti, perduoti Asmens duomenų jokiems tretiesiems asmenims (išskyrus tuos, kurie nurodyti Susitarime);

3.2.2. keisti Asmens duomenų tvarkymo pobūdžio;

3.2.3. tvarkyti Asmens duomenis bet kokiu kitu nei Sutartyje ir Susitarime nurodytu būdu ir tikslu;

3.2.4. teikti Asmens duomenis į trečiąsias valstybes be rašytinio Duomenų valdytojo sutikimo.

3.3. Duomenų tvarkytojas turi paskirti už šio Susitarimo vykdymą atsakingą asmenį ir nurodyti jo kontaktinius duomenis Susitarimo priede Nr.1.

3.4. Duomenų tvarkytojas turi tvarkyti visų Duomenų valdytojo vardu vykdomos Asmens duomenų tvarkymo veiklos kategorijų įrašus (taip pat, kai taikytina, tokią pareigą turi ir Duomenų tvarkytojo pasitelktas Pagalbinis tvarkytojas); tokiame įraše turi būti nurodyta ši informacija:

3.4.1. Duomenų tvarkytojo, Duomenų valdytojo ir, kai taikytina, Pagalbinio tvarkytojo duomenų apsaugos pareigūno arba asmens, atsakingo už duomenų apsaugą vardas, pavardė ir kontaktiniai duomenys;

3.4.2. informacija apie visas Duomenų valdytojo vardu atliekamo Asmens duomenų tvarkymo kategorijas;

3.4.3. kai taikytina, informacija apie Asmens duomenų perdavimą į trečiąją šalį, įskaitant tokios trečiosios šalies pavadinimą, ir, kai taikytina, tinkamų apsaugos priemonių dokumentai;

3.4.4. kai įmanoma, bendras techninių ir organizacinių saugumo priemonių apibūdinimas.

3.5. Duomenų tvarkytojas Duomenų valdytojui parašius nedelsiant pateikia Duomenų tvarkytojo pagal Susitarimą tvarkomus Asmens duomenų tvarkymo veiklos įrašus, tačiau bet kokiu atveju ne vėliau nei per 10 (dešimt) kalendorinių dienų nuo atitinkamo Duomenų valdytojo prašymo gavimo.

3.6. Duomenų tvarkytojas įsipareigoja užtikrinti, kad Asmens duomenų tvarkymą atliekantys Duomenų tvarkytojo darbuotojai yra informuoti apie Susitarime numatytus Duomenų tvarkytojo įsipareigojimus ir jų laikysis.

3.7. Duomenų tvarkytojas įsipareigoja užtikrinti, kad Asmens duomenų tvarkymą atliekantys Duomenų tvarkytojo darbuotojai būtų saistomi konfidencialumo įsipareigojimo Asmens duomenų atžvilgiu.

4. Techninės ir organizacinės saugumo priemonės

4.1. Atsižvelgdamas į techninių galimybių išsivystymo lygį, įgyvendinimo sąnaudas bei Asmens duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus, taip pat Asmens duomenų tvarkymo keliamus įvairios tikimybės ir rimtumo pavojus fizinių asmenų laisvėms ir teisėms, Duomenų tvarkytojas įgyvendina tinkamas technines ir organizacines priemones, kad būtų užtikrintas pavojų atitinkančio lygio saugumas, įskaitant Susitarimo priede Nr. 2 nurodytas minimalias priemones.

4.2. Duomenų valdytojui paprašius, nepagrįstai nedelsiant, Duomenų tvarkytojas turi pateikti Duomenų valdytojui dokumentus, kuriuose aprašomos Duomenų tvarkytojo įgyvendintos techninės ir organizacinės saugumo priemonės.

5. Poveikio duomenų apsaugai vertinimas

5.1. Tais atvejais, kai dėl Asmens duomenų tvarkymo rūšies, visų pirma, kai naudojamos naujos technologijos, ir atsižvelgiant į Asmens duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus, fizinių asmenų teisėms bei laisvėms gali kilti didelis pavojus, prieš pradėdamas tvarkyti Asmens duomenis, Duomenų tvarkytojas teikia pagalbą Duomenų valdytojui atliekant numatytų Asmens duomenų tvarkymo operacijų poveikio Asmens duomenų apsaugai vertinimą įskaitant, bet neapsiribojant: informacijos teikimą apie Duomenų tvarkytojo taikomas technines ir organizacines saugumo priemones, informacines sistemas, Pagalbinius tvarkytojus, pagalbą vertinant Asmens duomenų tvarkymo veiklos mąstą, poveikį Duomenų subjektams ir riziką, bei savo kompetencijos ribose teikiant siūlymus dėl esamos rizikos mažinimo priemonių.

5.2. Duomenų tvarkytojui yra žinoma, kad, kai Priežiūros institucijos manymu dėl aukščiau 5.1 punkte nurodytos planuojamos Asmens duomenų tvarkymo veiklos gali būti pažeisti Taikomi teisės aktai, Priežiūros institucija gali Duomenų tvarkytojui raštu pateikti rekomendacijas bei pasinaudoti bet kuriais iš Taikomuose teisės aktuose numatytais įgaliojimais.

6. Teisė atlikti auditą

6.1. Duomenų valdytojas turi teisę bet kuriuo metu, iš anksto pranešęs prieš protingą terminą, pats arba pasitelkdamas nepriklausomą trečiąją šalį – auditorių, atlikti Duomenų tvarkytojo veiklos atitikties Susitarimo reikalavimams auditą. Šiuo tikslu Duomenų tvarkytojas įsipareigoja

užtikrinti galimybę Duomenų valdytojui ar jo auditoriui patekti į Duomenų tvarkytojo patalpas, prieigą prie kompiuterinės, programinės įrangos, reikalingų dokumentų, kitos informacijos, kiek to reikia auditui atlikti. Šie įsipareigojimai neapima informacijos apie kitus Duomenų tvarkytojo klientus. Šalies prašymu kita Šalis ir (arba) auditorius turi įsipareigoti laikyti visą su auditu susijusią informaciją konfidencialia, tačiau toks įsipareigojimas neapriboja Duomenų valdytojo ir (arba) auditoriaus teisės imtis veiksmų dėl audito metu pagrįstai padarytų išvadų.

7. Pranešimas apie Asmens duomenų saugumo pažeidimą

7.1. Duomenų tvarkytojas, įtardamas, kad yra padarytas Asmens duomenų saugumo pažeidimas arba yra tokio pažeidimo grėsmė, turi nepagrįstai nedelsdamas, ne vėliau nei per 24 (dvidešimt keturias) valandas pranešti apie tai Duomenų valdytojui.

7.2. Pranešime apie Asmens duomenų saugumo pažeidimą turi būti bent:

7.2.1. aprašytas įvykusio ar galinčio įvykti Asmens duomenų saugumo pažeidimo pobūdis, įskaitant, jeigu įmanoma, atitinkamų duomenų subjektų kategorijos ir apytikslis skaičius, taip pat atitinkamų Asmens duomenų įrašų kategorijos ir apytikslis skaičius;

7.2.2. nurodyta duomenų apsaugos pareigūno arba kito kontaktinio asmens, galinčio suteikti daugiau informacijos, vardas ir pavardė (juridinio asmens pavadinimas) ir kontaktiniai duomenys;

7.2.3. aprašytos tikėtinos Asmens duomenų saugumo pažeidimo pasekmės;

7.2.4. aprašytos priemonės, kurių ėmėsi arba siūlo imtis Duomenų tvarkytojas, kad būtų pašalintas Asmens duomenų saugumo pažeidimas, įskaitant, priemones galimoms neigiamoms pasekmėms sumažinti;

7.2.5. pateikta bet kokia kita Duomenų tvarkytojo turima informacija, kurios Duomenų valdytojui reikia, kad galėtų pritaikyti atitinkamas saugumo priemones ir įvykdyti įpareigojimus pranešti apie Asmens duomenų saugumo pažeidimą priežiūros institucijai ir, kai reikalinga, nukentėjusiems duomenų subjektams.

7.3. Duomenų tvarkytojas dokumentuoja visus Asmens duomenų saugumo pažeidimus, galimus kilti incidentus ir su Asmens duomenų saugumo pažeidimais susijusius faktus, poveikį ir taisomuosius veiksmus, kurių buvo imtasi.

7.4. Kai Duomenų valdytojo nuomone Asmens duomenų saugumo pažeidimas yra esminis, Duomenų valdytojas turi teisę nedelsiant sustabdyti Asmens duomenų perdavimą Duomenų tvarkytojui ir (arba) nedelsiant nutraukti Sutartį bei šį Susitarimą, nemokėdamas Duomenų tvarkytojui jokių kompensacijų.

8. Pagalba Duomenų valdytojui ir informacijos duomenų subjektams bei Priežiūros institucijai pateikimas

8.1. Duomenų subjektui, Priežiūros institucijai ar trečiajai šaliai, vadovaujantis Taikomais teisės aktais, paprašius Duomenų tvarkytojo suteikti informacijos apie tvarkomus Asmens duomenis, Duomenų tvarkytojas nepagrįstai nedelsdamas, bet ne vėliau kaip per 1 (vieną) darbo dieną persiunčia tokį prašymą Duomenų valdytojui.

8.2. Visais atvejais į duomenų subjekto prašymus įgyvendinti duomenų subjekto teises atsakymą pateikia Duomenų valdytojas.

8.3. Duomenų tvarkytojas įsipareigoja padėti Duomenų valdytojui įvykdyti įsipareigojimus susijusius su duomenų subjekto teisių įgyvendinimu (įskaitant, bet neapsiribojant, teise reikalauti ištaisyti ir ištrinti Asmens duomenis, teise į Asmens duomenų perkeliamumą, teise nesutikti bei apriboti Asmens duomenų tvarkymą), tokia apimtimi, kokia duomenis tvarko pats Duomenų tvarkytojas. Duomenų tvarkytojas yra atsakingas už tai, kad Duomenų tvarkytojo pasitelkti Pagalbiniai tvarkytojai įvykdytų įsipareigojimus susijusius su duomenų subjektų teisių įgyvendinimu.

8.4. Duomenų tvarkytojas įsipareigoja padėti Duomenų valdytojui užtikrinti BDAR 32-36 straipsniuose nustatytų įsipareigojimų įgyvendinimą.

8.5. Duomenų tvarkytojas įsipareigoja padėti Duomenų valdytojui tiek, kiek reikės, atsakyti į aukščiau neaptartus duomenų subjektų, Priežiūros institucijos ir trečiųjų asmenų prašymus, įgyvendinant Asmens duomenų apsaugos reikalavimus.

8.6. Duomenų tvarkytojas užtikrina, kad jo turima informacija būtų pateikta nepagrįstai nedelsiant, bet ne vėliau kaip per 10 (dešimt) darbo dienų nuo informacijos iš Duomenų valdytojo gavimo dienos.

9. Pagalbiniai tvarkytojai

9.1. Duomenų tvarkytojas Asmens duomenų tvarkymo operacijoms, kurias atlieka Duomenų valdytojo vardu, gali pasitelkti Pagalbinį tvarkytoją tik su išankstiniu rašytiniu Duomenų valdytojo sutikimu kiekvieno atskiro tokio Pagalbinio tvarkytojo pasitelkimo atveju. Jeigu gavęs išankstinį Duomenų valdytojo rašytinį sutikimą Duomenų tvarkytojas atlieka Asmens duomenų tvarkymo operacijas pasitelkdamas Pagalbinį tvarkytoją, jis privalo su šiuo Pagalbiniu tvarkytoju prieš perduodant jam Duomenų valdytojo pateiktus Asmens duomenis sudaryti rašytinį susitarimą, pagal kurį Pagalbinis tvarkytojas būtų įpareigotas laikytis visų šiame Susitarime išdėstytų reikalavimų.

9.2. Duomenų valdytojo prašymu Duomenų tvarkytojas nepagrįstai nedelsdamas ir nemokamai turi pateikti tokių susitarimų kopijas. Duomenų tvarkytojas taip pat turi turėti aktualią informaciją apie visų jo pasitelktų Pagalbinių tvarkytojų tapatybę ir jų veiklos vietą, kuri būtų prieinama Duomenų valdytojui bei Priežiūros institucijai. Duomenų tvarkytojas prisiima atsakomybę ir užtikrina, kad Pagalbiniai tvarkytojai laikysis visų šio Susitarimo nuostatų. Duomenų tvarkytojas, pageidaujantis pakeisti pasitelktą Pagalbinį tvarkytoją kitu, privalo nedelsiant apie tai raštu pranešti Duomenų valdytojui.

9.3. Duomenų tvarkytojo pasitelkti Pagalbiniai tvarkytojai yra nurodyti Susitarimo priede Nr. 3.

9.4. Jei Duomenų valdytojas prieštarauja dėl Asmens duomenų perdavimo Pagalbiniam tvarkytojui, Duomenų tvarkytojas privalo toliau vykdyti savo įsipareigojimus pagal šį Susitarimą.

10. Asmens duomenų perdavimas į ES/ EEE nepriklausančias šalis

10.1. Duomenų tvarkytojas užtikrina, kad jokiu būdu netvarkys, neperduos ir jokiu kitu būdu nesuteiks prieigos ar galimybės naudotis Asmens duomenimis iš šalies ar šalyje, kuri nepriklauso ES arba EEE. Siekiant išvengti abejonių, šis draudimas apima ir yra taikomas techninei pagalbai, priežiūros, palaikymo ir panašių paslaugų teikimui.

10.2. Tuo atveju, kai Duomenų valdytojas nebuvo davęs leidimo raštu Duomenų tvarkytojui, bet Asmens duomenų perdavimas į trečiąją valstybę arba tarptautinei organizacijai yra privalomas pagal Europos Sąjungos arba Lietuvos Respublikos teisės aktus, Duomenų tvarkytojas prieš perduodamas Asmens duomenis privalo informuoti Duomenų valdytoją elektroniniu paštu apie tokį teisinį reikalavimą, nebent teisės aktai draudžia apie tai informuoti dėl svarbių viešojo intereso priežasčių.

11. Nuostolių atlyginimas ir atsakomybė

11.1. Šalių nuostolių atlyginimą bei atsakomybę pagal šį Susitarimą ir Sutartį reglamentuoja Sutartis.

12. Konfidencialumas

12.1. Nuostatos, kuriomis įtvirtintas konfidencialumo įsipareigojimas pagal šį Susitarimą ir Sutartį yra pateiktos Sutartyje.

13. Asmens duomenų grąžinimas ir sunaikinimas

13.1. Pasibaigus Asmens duomenų tvarkymui (pasibaigus Sutarties galiojimui arba anksčiau, jei to pareikalauja Duomenų valdytojas), Duomenų tvarkytojas Duomenų valdytojo nurodymu grąžina visus Asmens duomenis Duomenų valdytojui ir (arba) juos ištrina, sunaikina ir patvirtina apie tai raštu (išskyrus, kai įstatymuose numatyta kitaip). Jeigu Duomenų valdytojas pareikalauja, kad Asmens duomenys būtų saugomi tam tikrą laiką, tai turi būti daroma, remiantis Duomenų valdytojo dokumentais įformintais nurodymais.

14. Susitarimo galiojimas ir pakeitimai

14.1. Šis Susitarimas įsigalioja, kai ją pasirašo Šalių įgalioti atstovai, ir galioja, kol Duomenų tvarkytojas tvarko Asmens duomenis Duomenų valdytojo vardu.

14.2. Bet koks Susitarime numatytų Duomenų tvarkytojo įsipareigojimų pažeidimas laikomas esminiu ir suteikia Duomenų valdytojui teisę nutraukti Susitarimą ir Sutartį raštu informuojant Duomenų tvarkytoją apie nutraukimą, kuris įsigalioja nedelsiant arba nuo kitos pranešime nurodytos datos.

15. Taikytina teisė ir ginčų sprendimas

15.1. Šiam Susitarimui yra taikoma ir jis parengtas pagal Lietuvos Respublikos teisę.

15.2. Visi ginčai, kylantys iš Susitarimo arba susiję su šiuo Susitarimu sprendžiami Sutartyje nustatytais būdais.

16. Susitarimo priedai

16.1.1. 1 priedas – Duomenų valdytojo nurodymai dėl Asmens duomenų tvarkymo;

16.1.2. 2 priedas – Organizacinių ir techninių priemonių sąrašas;

Duomenų valdytojas:

Valstybės įmonė Lietuvos oro uostai

Adresas: Rodūnios kelias 10A, LT 02189, Vilnius,
Juridinio asmens kodas: 120864074
PVM mokėtojo kodas: LT208640716
Tel: +370 527 39326
El. paštas: info@ltou.lt

_____

Duomenų tvarkytojas:

UAB „Archyvita“

Adresas: Draugystės g. 19, Kaunas
Juridinio asmens kodas: 135761379
PVM mokėtojo kodas: LT100001185115
Bankas: AB SEB bankas
A/S Nr.: LT217044060003507240
Tel: 8 614 75075
El. paštas: archyvita@archyvita.lt

_____

Priedas Nr. 1 prie Susitarimo dėl asmens duomenų tvarkymo Nr. 6PS-21-

NURODYMAI DĖL ASMENS DUOMENŲ TVARKYMO

1. Bendros pastabos

Duomenų tvarkytojas įsipareigoja tvarkyti Asmens duomenis pagal Duomenų valdytojo dokumentais įformintus nurodymus dėl Asmens duomenų tvarkymo, išdėstytus šiame priede ir Susitarime.

2. Duomenų tvarkymo tikslas/-ai:

Duomenų tvarkytojas tvarko Asmens duomenis, Duomenų valdytojo tikslais:

Asmens duomenų tvarkymo tikslas yra archyvavimo paslaugų, detalizuotų pagrindinės sutarties specifikacijoje, vykdymas.

3. Duomenų tvarkymo pobūdis

Duomenų tvarkytojas atlieka tik šias Asmens duomenų tvarkymo operacijas:

- Saugo Asmens duomenis griežtai Susitarime aptartais terminais ir sąlygomis bei sunaikina Asmens duomenis, kai pasiekiami nustatyti tikslai arba yra gaunamas Duomenų valdytojo nurodymas;
- Užtikrina duomenų saugumą, prieinamumą, konfidencialumą ir vientisumą.

4. Prieigos kontrolė ir personalas

Duomenų tvarkytojas privalo užtikrinti, kad darbuotojai, dirbantys su Asmens duomenimis, būtų informuoti, apmokyti ir susipažintų su šiame Susitarime pateiktais nurodymais Duomenų tvarkytojui ir techninėmis bei organizacinėmis priemonėmis.

- Duomenų valdytojas pateiks Duomenų tvarkytojo atsakingam už Susitarimo vykdymą asmeniui arba jo nurodytam darbuotojui Asmens duomenis naudojantis elektroninį paštą/ kitą Asmens duomenų perdavimo kanalą edita@archyvita.lt ;
- Darbuotojai negali dalintis savo prieigos duomenimis su kitais darbuotojais;
- Darbuotojai negali dalintis jiems suteiktais Asmens duomenimis su kitais darbuotojais, kurie nėra atsakingi už Sutarties bei Susitarimo vykdymą;
- Pasikeitus darbuotojo rolei, darbuotojui netekus darbo funkcijų vartotojo paskyra turi būti blokuojama. Naujam darbuotojui turi būti sukurta nauja paskyra;
- Pasikeitus darbuotojo rolei, jam netekus darbo funkcijų, darbuotojui turi būti panaikinta galimybė prieiti prie pateiktų duomenų.

5. Asmens duomenų rūšys

- Vardas;
- Pavardė;
- Asmens kodas;

- Gimimo data;
- Telefono numeris;
- Gyvenamasis adresas;
- El. paštas;
- Banko sąskaitos numeris;
- Pardavimų – mokėjimų ataskaita;
- Sąskaita faktūra;
- Pareigos;

6. Duomenų subjektų kategorijos

- Darbuotojai;
- Klientai;
- Keleiviai;
- Tiekėjų atstovai;
- Renginių dalyviai;
- Lankytojai;

7. Duomenų perdavimas

Duomenų tvarkytojas, perduodamas Asmens duomenis Duomenų valdytojui ir atvirkščiai, turi juos perduoti tik saugiu būdu, naudojant duomenis šifruojančią programinę įrangą. Duomenų dešifravimo slaptažodis turi būti perduodamas atskiru duomenų perdavimo kanalu, nei perduodami duomenys.

8. Duomenų tvarkymo vieta

- Asmens duomenys tvarkomi Duomenų tvarkytojo, Asmens duomenis jam perdavus elektroniniu paštu/ kitu perdavimo kanalu.

9. Duomenų tvarkymo trukmė/ Saugojimo laikotarpis

Duomenų tvarkytojas turi užtikrinti perduotų Asmens duomenų rezervinį kopijavimą, užtikrinant Asmens duomenų vientisumą, prieinamumą ir atstatomumą.

- Pasibaigus Sutarties ir Susitarimo galiojimo terminui Duomenų tvarkytojo tvarkomi Asmens duomenys turi būti grąžinti Duomenų valdytojui;
- Pasibaigus Sutarties ir Susitarimo galiojimo terminui Duomenų tvarkytojas turi sunaikinti be galimybės atstatyti ir to rašytiniai įrodymai pateikiami Duomenų valdytojui.

10. Už Susitarimo vykdymą atsakingi asmenys

Valstybės įmonė Lietuvos oro uostai	UAB „Archyvita“
_____	

Duomenų valdytojas:

Valstybės įmonė Lietuvos oro uostai

Adresas: Rodūnios kelias 10a, LT-02189, Vilnius
Juridinio asmens kodas: 120864074
PVM mokėtojo kodas: LT208640716
Tel: +370 5 2739326
El. paštas: info@ltou.lt

_____

Duomenų tvarkytojas:

UAB „Archyvita“

Adresas: Draugystės g. 19, Kaunas
Juridinio asmens kodas: 135761379
PVM mokėtojo kodas: LT100001185115
Bankas: AB SEB bankas
A/S Nr.: LT217044060003507240
Tel: 8 614 75075
El. paštas:archyvita@archyvita.lt

_____

Priedas Nr. 2 prie Susitarimo dėl asmens duomenų tvarkymo Nr. 6PS-21-

ORGANIZACINIŲ IR TECHNINIŲ PRIEMONIŲ SĄRAŠAS

1. Organizacinės saugumo priemonės	
1.1. Saugumo valdymas	
1.1.1. Saugumo politika ir asmens duomenų apsaugos procedūros	Organizacija turėtų nustatyti savo politiką, kuri, kaip informacijos saugumo politikos dalis, būtų taikoma asmens duomenų tvarkymui.
	Saugumo politika turėtų būti peržiūrima kasmet 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.
	Turėtų būti nustatyta aiški asmenų, atsakingų už konkrečių saugumo užtikrinimo užduočių vykdymą, įskaitant saugumo pareigūną, paskyrimo tvarka.
	Turėtų būti oficialiai paskirtas (paskyrimą įforminant dokumentais) saugumo pareigūnas. Saugumo pareigūno uždaviniai ir atsakomybės taip pat turėtų būti aiškiai nustatyti ir įforminti dokumentais.
1.1.3. Prieigos kontrolės politika	Kiekvienam vaidmeniui (susijusiam su asmens duomenų tvarkymu) turėtų būti priskirtos konkrečios prieigos kontrolės teisės 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.

	Vaidmenys, kuriems suteikiamos pernelyg didelės teisės, turi būti aiškiai apibrėžti ir priskirti tik ribotam konkrečių 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).
	IT išteklius reikėtų reguliariai peržiūrėti ir atnaujinti.
	Turėtų būti apibrėžti ir dokumentais įforminti prie tam tikrų išteklių prieigą turinčių asmenų vaidmenys.
1.1.5. Pakeitimų valdymas	Organizacija turėtų užtikrinti, kad visi IT sistemos pakeitimai būtų užregistruoti ir stebimi konkretaus asmens (pvz. IT ar saugumo pareigūno). Šis procesas turėtų būti stebimas reguliariai.
	Programinė įranga turėtų būti kuriama specialioje aplinkoje, kuri nėra sujungta su asmens duomenų tvarkymui naudojama IT sistema. Jei reikalingi bandymai, turėtų būti naudojami fiktyvūs, o ne tikri duomenys. Jei to padaryti neįmanoma, turėtų būti įdiegtos specialios procedūros, skirtos bandymams naudojamų asmens duomenų apsaugai užtikrinti.
	Turėtų būti įdiegta išsami ir dokumentais įforminta pakeitimų politika. Joje turėtų būti numatytas: pakeitimų įdiegimo procesas, vaidmenys/vartotojai, kurie turi teisę atlikti pakeitimus, pakeitimų įdiegimo terminai. Pakeitimų politika turėtų būti reguliariai atnaujinama.
1.2. Reagavimas į incidentus ir veiklos tęstinumas	
1.2.1. Incidentų valdymas / asmens duomenų saugumo pažeidimai	Turėtų būti parengtas reagavimo į incidentus planas, nustatantis išsamias procedūras, siekiant užtikrinti efektyvų ir tinkamą reagavimą į su asmens duomenų saugumu susijusius incidentus.
	Apie asmens duomenų saugumo pažeidimus turėtų būti nedelsiant pranešta vadovybei. Pranešimų, susijusių su pažeidimais, pateikimo kompetentingoms institucijoms ir duomenų subjektams tvarka turi būti parengta vadovaujantis teisės aktų nuostatomis.
	Reagavimo į incidentus planas turėtų būti įformintas dokumentu, įskaitant veiksmų, kurių reiktų imtis, siekiant sušvelninti padarytą žalą, sąrašą ir aiškų vaidmenų pasiskirstymą.

1.2.2. Veiklos tęstinumas	Organizacija turėtų nustatyti pagrindines procedūras ir kontrolės mechanizmus, kurie turėtų būti taikomi, siekiant užtikrinti asmens duomenis tvarkančios IT sistemos tęstinumo ir prieinamumo reikalaujamą lygį (incidentų/asmens duomenų saugumo pažeidimo atvejais).
	Veiklos tęstinumo politika (toliau – **VTP**) turėtų būti išsami ir įforminta dokumentu (remiantis bendrąja saugumo politika). Joje turėtų būti numatyti aiškūs veiksmai ir vaidmenų pasiskirstymas.
	VTP turėtų būti apibrėžtas garantuotas paslaugos kokybės lygis pagrindiniams veiklos procesams, kurie užtikrina asmens duomenų saugumą.
	Turėtų būti apsvarstyta alternatyvi priemonė, priklausomai nuo Organizacijos ir IT sistemos prastovos priimtinumo.
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.
	Prieš pradedant vykdyti pareigas, darbuotojų turėtų būti paprašyta susipažinti su Organizacijos saugumo politika bei pasirašyti atitinkamus konfidencialumo ir įsipareigojimo neatskleisti konfidencialios informacijos susitarimus.
	Darbuotojams, dirbantiems su asmens duomenimis, kurių tvarkymas kelia didelę riziką, turėtų būti taikomi specialūs konfidencialumo įsipareigojimai (numatyti jų darbo sutartyje ar kitame teisiniame dokumente).
1.3.2. Mokymai	Organizacija turėtų reguliariai organizuoti mokymus darbuotojams, įskaitant specialius mokymus naujiems darbuotojams, asmens duomenų apsaugos klausimais.
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.
	Turėtų būti vengiama naudoti bendrąsias vartotojų paskyras. Tai atvejais, kai tai yra būtina, turėtų būti užtikrinta, kad visi bendrosios paskyros vartotojai turėtų vienodus vaidmenis ir atsakomybes.
	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.
	Slaptažodžiai turi būti sudaryti ne mažiau kaip iš 8 (aštuonių) simbolių, tarp kurių privalo būti trys iš nurodytų keturių simbolių tipų: didžiosios ir mažosios raidės, skaitmenys, specialieji (skyrybos) ženklai. Šie slaptažodžiai turi būti keičiami ne rečiau kaip kartą per 60 dienų ir turi skirtis nuo 10 anksčiau naudotų slaptažodžių.
	Prieigos kontrolės sistema turėtų sugebėti aptikti ir neleisti naudoti slaptažodžių, kurie neatitinka nustatyto sudėtingumo lygio.
	Turėtų būti apibrėžta ir dokumentais įtvirtinta konkreti slaptažodžių politika. Šioje politikoje turėtų būti bent jau nustatytas slaptažodžio ilgis, sudėtingumas, galiojimo terminas bei priimtinas nesėkmingų bandymų prisijungti skaičius.
	Vartotojo slaptažodžiai privalo būti saugomi „hash“ (šifruotų slaptažodžių) forma.
	Rekomenduotina naudoti dviejų faktorių autentifikavimo apsaugą prieigos sistemoms, kurios tvarko asmens duomenis. Dviejų faktorių apsauga galėtų būti slaptažodžiai, saugumo raktai, USB su slaptu raktu, biometriniai duomenys ir pan.
	Įrenginio autentifikavimas turėtų būtu naudojamas siekiant užtikrinti, kad asmens duomenų tvarkymas būtų vykdomas tik per konkrečius tinklo šaltinius.
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).
	Atliktų operacijų įrašai (log files) turėtų turėti laiko žymą ir būti tinkamai apsaugoti nuo mėginimų klastoti ir neteisėtos prieigos. Laikrodžiai turėtų būti sinchronizuoti su vienu orientaciniu laiko šaltiniu.
	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.

	Stebėsenos sistema turėtų tvarkyti operacijų įrašus (log files) ir teikti ataskaitas apie sistemos būklę bei pranešti apie potencialius perspėjimus.
2.2.1. Serveris/Duomenų bazės saugumas	Duomenų bazių ir aplikacijų serveriai turėtų būti sukonfigūruoti taip, kad veiktų naudojantis skirtingomis paskyromis, naudojant minimalias OS teises, užtikrinančias pakankamą veikimą.
	Duomenų bazių ir programų serveriai turėtų tvarkyti tik tuos asmens duomenis, kurių reikia siekiant tikslų, dėl kurių jie buvo surinkti.
	Duomenų bazės, kuriose yra asmens duomenys turi būti šifruojamos.
	Atminties laikmenos turėtų būti šifruojamos.
	Pseudonimų suteikimo metodai turėtų būti taikytini per duomenų atskyrimą nuo tiesioginių identifikatorių, siekiant išvengti duomenų subjekto susiejimo be papildomos informacijos.
	Turėtų būti pritaikyti pasirinktini privatumo išsaugojimo metodai duomenų bazių lygyje, tokie kaip autorizuoti paklausimai, privatumą išsaugojantis duomenų bazių paieškų vykdymas, užšifruotas ieškojimas ir kt.
2.2.2. Darbo stoties saugumas	Vartotojams neturėtų būti sudaryta galimybė deaktyvuoti ar apeiti saugumo nustatymus.
	Vartotojai neturėtų galėti įdiegti ar išjungti nesankcionuotų programinių įrangų.
	Sistema turėtų įsijungti į naudojimosi pertraukos režimą, kuomet vartotojas tam tikrą laiko tarpą neatlieka jokių veiksmų.
	Svarbiausi apsaugos atnaujinimai, išleisti operacinės sistemos kūrėjo, turėtų būti įdiegti reguliariai.
	Antivirusinės ir parašu paremtos įsilaužimo prevencijos programos turėtų būti konfigūruojamos kiekvieną dieną.
	Neturėtų būti leidžiama atsisiųsti asmens duomenų iš darbo vietos į išorines atminties rinkmenas (pvz. USB, DVD, išorinius kietuosius diskus).
	Darbo vietos, kuriose yra tvarkomi asmens duomenys neturėtų būti prisijungusios prie interneto, nebent apsaugos priemonės yra pakankamos apsisaugoti nuo nesankcionuoto asmens duomenų tvarkymo, kopijavimo ir perleidimo į rinkmenas.
	Pilnas disko programinės įrangos užšifravimas turėtų būti leidžiamas darbo vietos operacinėse sistemose.

2.3.	**Tinklo /ryšio saugumas**	Kai jungiamasi per internetą, ryšys turėtų būti perduodamas užšifruotu pavidalu naudojant kriptografinius protokolus (TLS/SSL).
		Belaidė prieiga prie IT sistemos turėtų būti suteikta tiktai konkretiems vartotojams ir procesams. Prieigai apsaugoti turėtų būti naudojami šifravimo mechanizmai.
		Turėtų būti vengiama nuotolinės prieigos prie IT sistemos. Tais atvejais, kai tai yra tikrai būtina, tokios prieigos procesą naudojant iš anksto numatytus įrenginius turėtų kontroliuoti ir stebėti konkretus asmuo iš Organizacijos (pvz. IT administratorius/saugumo pareigūnas).
		Duomenų srautas į ir iš IT sistemos turėtų būti stebimas ir kontroliuojamas naudojant ugniasienes ir įsilaužimų aptikimo sistemas.
		Informacijos sistemos tinklas turėtų būti atskirtas nuo kitų duomenų valdytojo tinklų.
		Prieiga prie IT sistemų turėtų būti atliekama tik iš anksto sankcionuotų prietaisų ir terminalų, naudojant, tokias priemones, kaip MAC filtravimas arba Tinklo prieigos kontrolė (NAC).
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.
		Atsarginių kopijų darymo procesas turėtų būti stebimas, siekiant užtikrinti užbaigtumą.
		Turėtų būti reguliariai daromos pilnos atsarginės kopijos.
		Atsarginės kopijos turėtų būti reguliariai testuojamos, siekiant užtikrinti, kad nutikus nenumatytiems atvejams būtų galima jomis pasikliauti.
		Planuotos prieauginės atsarginės kopijos (angl. *incremental backups*) turėtų būti daromos bent jau kartą per dieną.
		Atsarginės kopijos turėtų būti saugiai laikomos skirtingose vietose.
		Tais atvejais, kai atsarginių kopijų saugojimo tikslais yra naudojamasi trečiųjų šalių paslaugomis, kopijos turėtų būti užšifruotos prieš jas perduodant duomenų valdytojui.

	Atsarginės kopijos turėtų būti užšifruotos ir taip pat saugiai laikomos ir išorės šaltiniuose (angl. off-line).
2.5. Mobiliojo ryšio / nešiojami įrenginiai	Turėtų būti apibrėžtos ir dokumentais įformintos mobiliojo ryšio ir nešiojamųjų įrenginių valdymo procedūros, nustatančios naudojimosi tokiais įrenginiais taisykles.
	Mobiliojo ryšio įrenginiai, kurie turi prieigą prie informacinės sistemos turėtų būti iš anksto registruoti ir iš anksto sankcionuoti.
	Mobiliojo ryšio įrenginiams turėtų būti taikomi tie patys prieigos kontrolės procedūrų lygiai kaip ir galiniams įrenginiams.
	Turėtų būti aiškiai apibrėžti konkretūs vaidmenys ir atsakomybės, susiję su mobiliojo ryšio ir nešiojamųjų įrenginių valdymu.
	Organizacija turėtų turėti galimybę ištrinti asmens duomenis nuotoliniu būdu (kas liečia jų tvarkymo veiklą) iš mobiliojo ryšio įrenginio, kuris buvo pamestas, pavogtas ar kitaip sugadintas.
	Mobiliojo ryšio įrenginiai turėtų suteikti galimybę per saugios programinės įrangos suteiktas talpyklas atskirti naudojimą privatiems tikslams ir darbo santykių metu.
	Mobiliojo ryšio įrenginiai turėtų būti fiziškai apsaugoti nuo vagysčių, kai jie nenaudojami.
	Prieiga prie mobiliojo ryšio įrenginių turėtų turėti dviejų faktorių autentifikaciją.
	Asmens duomenys patalpinti mobiliojo ryšio įrenginyje (kaip dalis Organizacijos duomenų tvarkymo operacijų) turėtų būti užšifruoti.
2.6. Aplikacijos saugumas	Kūrimo ciklo metu turėtų būti naudojama geriausia praktika, pažangiausi metodai ir visuotinai pripažinta saugaus kūrimo praktika, struktūra bei standartai.
	Specifiniai saugumo reikalavimai turėtų būti nustatyti ankstyvojoje kūrimo ciklo fazėje.
	Specifinės technologijos ir metodai sukurti apsaugoti privatumą ir asmens duomenis (taip pat žinomi, kaip *Privacy Enchancing Technologies (PETs)*) turėtų būti taikomi kartu su saugumo reikalavimais.
	Turėtų būti naudojami Saugaus kodavimo standartai ir praktika.
	Kūrimo metu turėtų būti atliekamas testavimas ir patvirtinama, ar būtinieji saugumo reikalavimai buvo įgyvendinti.

	Pažeidžiamumo vertinimas, programų ir infrastruktūros skverbties bandymas turėtų būti atliekamas patikimos trečiosios šalies dar prieš patvirtinant operacijas. Programa neturi būti patvirtinta iki kol nebus pasiektas reikiamas saugumo lygis.
	Skverbties bandymas turėtų būti atliekamas reguliariai.
	Turėtų būti gauta informacija apie techninį informacinių sistemų pažeidžiamumą.
	Programinės įrangos pakritimai turėtų būti išbandyti ir įvertinti prieš įdiegiant ją į operacinę erdvę.
2.7. Duomenų ištrynimas, sunaikinimas	Popierius ir nešiojamosios laikmenos, kuriose buvo laikomi asmens duomenys turi būti supjaustomi/sunaikinami.
	Jei yra naudojamasi trečiųjų šalių paslaugomis saugiai pašalinti medijų ir popierinius įrašus, turėtų būti tinkamai sudaryta paslaugų sutartis ir atliekami įrašai apie įrašų sunaikinimą.
	Po programinės įrangos ištrynimo, turėtų būti atliekamos papildomos techninės priemonės, tokios kaip išmagnetinimas. Atsižvelgiant į konkrečią situaciją, fizinis sunaikinimas taip turėtų būti apsvarstytas.
	Jei yra naudojamasi trečiąja šalimi, kuri yra duomenų tvarkytojas, siekiant sunaikinti medijų ir popierines bylas, turėtų būti apsvarstyta galimybė šį procesą atlikti duomenų valdytojo patalpose (siekiant išvengti asmens duomenų perdavimo į išorę).
2.8. Fizinis saugumas	IT sistemos infrastruktūros fizinis perimetras turėtų būti neprieinamas leidimo neturintiems darbuotojams.
	Turėtų būti aiškiai nustatyta Organizacijos visų darbuotojų ar patalpų lankytojų identifikavimo tvarka naudojant atitinkamas priemones, pvz. tapatybę nustatančias korteles.
	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.
	Turėtų būti pastatyti fiziniai barjerai, jei įmanoma, užtikrinantys neteisėtą fizinį patekimą.
	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.

Duomenų valdytojas:

Valstybės įmonė Lietuvos oro uostai

Adresas: Rodūnios kelias 10A, LT 02189, Vilnius
Juridinio asmens kodas: 120864074
PVM mokėtojo kodas: LT208640716
Tel: +370 527 39326
El. paštas: info@ltou.lt

_____

Duomenų tvarkytojas:

UAB „Archyvita“

Adresas: Draugystės g. 19, Kaunas
Juridinio asmens kodas: 135761379
PVM mokėtojo kodas: LT100001185115
Bankas: AB SEB bankas
A/S Nr.: LT217044060003507240
Tel: 8 614 75075
El. paštas:archyvita@archyvita.lt

_____