SUSITARIMAS
DĖL ASMENS DUOMENŲ TVARKYMO

2024 m. d. Nr.
Vilnius

Valstybės įmonė Valstybinių miškų urėdija (toliau – Duomenų valdytojas, Pirkėjas), įmonės kodas 132340880, atstovaujama generalinio direktoriaus Valdo Kaubrės, veikiančio pagal įmonės įstatus, ir **UAB „Heksimus“** įmonės kodas 300580894 (toliau – Duomenų tvarkytojas, Tiekėjas), atstovaujama direktorės Giedrės Ruginytės-Čepienės, veikiančios pagal įmonės įstatus,

atsižvelgdamos į 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentą (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (toliau – Reglamentas (ES) 2016/679),

vadovaudamosios tarpusavyje 2024-12-03 sudarytos Viešojo pirkimo – pardavimo sutarties (toliau – Sutartis) Nr. 77-VP-8653-2024 Bendrųjų sąlygų 14.2 papunkčio nuostata, numatančia Paslaugų teikėjo pareigą pasirašyti su Užsakovu visus reikiamus susitarimus dėl asmens duomenų tvarkymo, vadovaujantis Reglamentu (ES) 2016/679 (Sutartyje – BDAR) ir kitais asmens duomenų tvarkymą ir jų apsaugą reglamentuojančiais teisės aktais, Šalys įsipareigoja sudaryti atskirą susitarimą dėl asmens duomenų tvarkymo, kuriuo nustato asmens duomenų tvarkymo dalyką ir trukmę, asmens duomenų tvarkymo pobūdį ir tikslą, asmens duomenų rūšis ir duomenų subjektų kategorijas bei duomenų valdytojo ir duomenų tvarkytojo prievoles ir teises,

sudarė šį susitarimą (toliau – Susitarimas), kuriame Pirkėjas ir Tiekėjas kartu vadinami Šalimis, o kiekvienas atskirai − Šalimi, ir susitarė:

I. ASMENS DUOMENŲ TVARKYMO DALYKAS, POBŪDIS IR TIKSLAI

1.1. Asmens duomenų tvarkymo dalykas yra Duomenų tvarkytojo atliekamas Antivirusinės programinės įrangos licencijų pirkimo paslaugų (toliau – paslaugos) teikimas, kuris apima asmens duomenų tvarkymą, kaip tai numatyta Susitarimo 1.3 papunktyje.

1.2. Duomenų valdytojas įgalioja Duomenų tvarkytoją jo vardu tvarkyti Susitarimo 2.2 papunktyje nurodytus asmens duomenis paslaugų teikimo tikslu pagal Sutartį.

1.3. Duomenų tvarkytojas teikdamas paslaugas prieina prie elektroninių pranešimų ir juose esančių priedų, kurie siunčiami į smėliadėžę debesyje.

II. DUOMENŲ SUBJEKTŲ KATEGORIJOS IR ASMENS DUOMENŲ RŪŠYS

2.1.1. Duomenų subjektų, kurių asmens duomenys tvarkomi vadovaujantis šiuo Susitarimu, kategorijos yra: Duomenų valdytojo darbuotojai, dirbantys pagal darbo sutartį (toliau – darbuotojai), kaip elektroninio pašto pranešimo gavėjai, elektroninio pašto pranešimo siuntėjai.

2.2. Pagal šį Susitarimą tvarkomi:

2.2.1. Darbuotojų asmens duomenys: vardas (vardai) ir pavardė (pavardės), pareigos, elektroninio pašto adresas, elektroninio pašto turinys ir kt. elektroninio pašto pranešime nurodyta informacija;

2.2.2. Elektroninio pašto pranešimo siuntėjo asmens duomenys: vardas (vardai) ir pavardė (pavardės), elektroninio pašto adresas ir kt. elektroninio pašto pranešime nurodyta informacija.

III. DUOMENŲ VALDYTOJO TEISĖS IR ĮSIPAREIGOJIMAI

3.1. Duomenų valdytojas įsipareigoja:

3.1. Visą asmens duomenų, numatytų Susitarimo 2.2 papunktyje (toliau – Duomenys), tvarkymo laikotarpį duoti Duomenų tvarkytojui nurodymus dėl asmens duomenų tvarkymo, įskaitant juos tvarkyti tik Duomenų valdytojo vardu, raštu (įskaitant elektroniniu paštu) ir kurie neprieštarautų teisės aktams, išskyrus atvejus, kai tai daryti reikalaujama pagal Europos Sąjungos arba Lietuvos Respublikos teisės aktus, kurie yra taikomi Duomenų tvarkytojui.

3.2. Užtikrinti, kad vadovaujantis Reglamento (ES) 2016/679 24 straipsniu, Duomenys būtų tvarkomi laikantis Reglamento (ES) 2016/679, kitų asmens duomenų apsaugą reglamentuojančių Europos Sąjungos ar Lietuvos Respublikos teisės aktų ir šio Susitarimo.

3.3. Priimti sprendimus dėl Duomenų tvarkymo tikslų ir priemonių.

3.4. Duomenų valdytojas turi teisę reikalauti Duomenų tvarkytojo, o Duomenų tvarkytojas įsipareigoja pateikti informaciją ir (ar) dokumentus, kurių reikia norint įsitikinti, kad Duomenų tvarkytojas tinkamai vykdo Susitarime ir teisės aktuose nustatytus asmens duomenų apsaugos reikalavimus. Duomenų tvarkytojas privalo Duomenų valdytojui pateikti šią informaciją ir (ar) dokumentus per Duomenų valdytojo nurodytą protingą terminą.

3.5. Tuo atveju, jei nustatoma grėsmė ar kyla pagrįstų įtarimų dėl grėsmės tvarkomų Duomenų vientisumui, konfidencialumui, ar saugumui ir (arba) jei Duomenų tvarkytojas netinkamai užtikrina tvarkomų Duomenų vientisumą, konfidencialumą ar saugumą ir (arba) jei Duomenų tvarkytojas netinkamai vykdo Susitarime ir teisės aktuose nustatytus asmens duomenų apsaugos reikalavimus, Duomenų valdytojas apie tai raštu arba elektroninių ryšių priemonėmis informuoja Duomenų tvarkytoją ir turi teisę reikalauti nedelsiant apriboti Duomenų tvarkymą ne vėliau kaip per 1 (vieną) darbo dieną nuo tokio reikalavimo gavimo. Gavęs tokį reikalavimą, Duomenų tvarkytojas pašalina nustatytas grėsmes ir apie tai ne vėliau kaip per 1 (vieną) darbo dieną raštu arba elektroninių ryšių priemonėmis informuoja Duomenų valdytoją apie pasirengimą tinkamai vykdyti Susitarime ir teisės aktuose nustatytus asmens duomenų apsaugos reikalavimus. Duomenų valdytojas, įvertinęs iš Duomenų tvarkytojo gautą informaciją, gali duoti sutikimą atnaujinti Duomenų tvarkymą. Jei Duomenų tvarkytojas neinformuoja Duomenų valdytojo apie pasirengimą tinkamai vykdyti Susitarime ir teisės aktuose nustatytus asmens duomenų apsaugos reikalavimus per 5 (penkias) darbo dienas nuo reikalavimo gavimo, Duomenų valdytojas turi teisę vienašališkai nutraukti Sutartį joje numatyta tvarka Sutarties Bendrųjų sąlygų 22.2.2.12 papunktyje nurodytu atveju (pagrindu).

IV. DUOMENŲ TVARKYTOJO ĮSIPAREIGOJIMAI

4.1. Duomenų tvarkytojas, teikdamas paslaugas, įsipareigoja:

4.1.1. Tvarkyti Duomenis tik Duomenų valdytojo vardu, Susitarimo 1.2 papunktyje nustatytu tikslu ir pagal jo rašytinius nurodymus, išskyrus atvejus, kai to reikalaujama pagal Europos Sąjungos arba Lietuvos Respublikos teisės aktus, taikomus Duomenų tvarkytojui, bei Susitarime nustatytus įsipareigojimus. Tokiu atveju, prieš pradėdamas tvarkyti Duomenis, Duomenų tvarkytojas praneša Duomenų valdytojui apie tokį teisinį reikalavimą, išskyrus atvejus, kai toks pranešimas yra draudžiamas dėl svarbių viešojo intereso priežasčių. Duomenų valdytojas taip pat gali pateikti tolesnius nurodymus viso Duomenų tvarkymo metu, tačiau tokie su Susitarimu susiję nurodymai visada turi būti pagrįsti dokumentais. Jeigu Duomenų tvarkytojas dėl bet kokių priežasčių negali užtikrinti atitikties ilgesnį negu 1 (vieno) mėnesio laikotarpį, Duomenų tvarkytojas nedelsiant praneša Duomenų valdytojui apie tai, kad jis negali užtikrinti atitikties, ir tokiu atveju Duomenų valdytojas turi teisę apriboti Duomenų tvarkymą ir (arba) nutraukti Sutartį joje numatyta tvarka Sutarties Bendrųjų sąlygų 22.2.2.12 papunktyje nurodytu atveju (pagrindu).

4.1.2. Nenaudoti Duomenų savo ar kitų asmenų, išskyrus Duomenų valdytoją, interesais bei neatlikti jokių kitų Susitarime neatitinkančių ar neteisėtų Duomenų tvarkymo veiksmų.

4.1.3. Be atskiro Duomenų valdytojo sutikimo neatskleisti, neperduoti ar kitu būdu nesudaryti galimybių jokiomis priemonėmis naudotis / susipažinti su tvarkomais Duomenimis jokioms trečiosioms šalims, jei kitaip nenustato Susitarimas ar Lietuvos Respublikos įstatymai ir kiti teisės aktai (šis punktas netaikomas Duomenų perdavimui kitam duomenų tvarkytojui (toliau – subtvarkytojas)).

4.1.4. Nustatyti tinkamo Duomenų saugumo lygį, atsižvelgiant į Duomenų tvarkymo keliamus įvairios tikimybės ir rimtumo pavojus fizinių asmenų teisėms ir laisvėms, ir savo lėšomis, tinkamomis techninėmis ir organizacinėmis priemonėmis užtikrinti Susitarimo vykdymo tikslais ir pagal Duomenų valdytojo nurodymus tvarkomų Duomenų apsaugą, vadovaujantis Reglamentu (ES) 2016/679 ir kitais teisės aktais. Duomenų valdytojo nurodomų techninių ir organizacinių priemonių sąrašas pateikiamas šio Susitarimo 2 priede „Techninės ir organizacinės priemonės“. Duomenų valdytojo prašymu ir per Duomenų valdytojo nurodytą protingą terminą Duomenų tvarkytojas įsipareigoja pateikti Duomenų valdytojui šių priemonių taikymo, Duomenų tvarkytojui tvarkant Duomenų valdytojo pavestus Duomenis, įrodymus.

4.1.5. Pagal Reglamento (ES) 2016/679 32 straipsnį, Duomenų tvarkytojas nepriklausomai nuo Duomenų valdytojo, įsipareigoja įvertinti Duomenų tvarkymo riziką, susijusią su Duomenų tvarkymo veikla, galinčią kilti fizinių asmenų teisėms ir laisvėms, ir įgyvendinti technines ir organizacines priemones, kurios galėtų sumažinti šiuos pavojus.

4.1.6. Jei kyla grėsmė Duomenų saugumui ir reikia įgyvendinti kitas ar papildomas priemones, negu jau yra įgyvendinęs Duomenų tvarkytojas pagal Reglamento (ES) 2016/679 32 straipsnį, Duomenų valdytojas Susitarimo 2 priede nurodo, kokias technines ir (arba) organizacines priemones turi įgyvendinti Duomenų tvarkytojas. Duomenų tvarkytojas įsipareigoja pateikti Duomenų valdytojui šių priemonių taikymo, Duomenų tvarkytojui tvarkant Duomenų valdytojo pavestus Duomenis, įrodymus.

4.1.7. Padėti Duomenų valdytojui užtikrinti Duomenų valdytojo pareigų pagal Reglamento (ES) 2016/679 32 straipsnį vykdymą, inter alia, teikdamas Duomenų valdytojui informaciją apie technines ir organizacines priemones, kurias Duomenų tvarkytojas jau įgyvendina pagal Reglamento (ES) 2016/679 32 straipsnį, kartu su visa kita informacija, būtina Duomenų valdytojui įvykdyti duomenų valdytojo pareigas pagal Reglamento (ES) 2016/679 32 straipsnį.

4.1.8. Užtikrinti, kad Duomenų tvarkytojo darbuotojai ar kiti asmenys, įgalioti tvarkyti Duomenis pagal Susitarimą, būtų pasirašytinai įpareigoti saugoti asmens duomenų paslaptį. Duomenų valdytojo prašymu ir per Duomenų valdytojo nurodytą protingą terminą Duomenų tvarkytojas įsipareigoja pateikti tai patvirtinančius įrodymus.

4.1.9. Duomenis laikyti paslaptyje ir pasibaigus Susitarimo galiojimui.

4.1.10. Duomenų tvarkytojas nedelsdamas, bet ne vėliau kaip per 3 (tris) darbo dienas, raštu informuoja Duomenų valdytoją, jei, jo nuomone, Duomenų valdytojo nurodymas prieštarauja šiam Susitarimui, Reglamentui (ES) 2016/679, kitiems Europos Sąjungos ir Lietuvos Respublikos asmens duomenų apsaugą reglamentuojantiems teisės aktams. Duomenų tvarkytojas turės teisę nevykdyti tokio Duomenų valdytojo nurodymo ir dėl to nepažeis šio Susitarimo ir neprisiims kitokios atsakomybės Duomenų valdytojo atžvilgiu dėl tokio nurodymo nevykdymo.

4.1.11. Pasitelkiant subtvarkytoją, iš anksto informuoti Duomenų valdytoją ir gauti jo išankstinį konkretų leidimą.

4.1.12. Subtvarkytojo (-ų) teikiamos tvarkymo paslaugos bus vykdomos pagal šio Susitarimo 6 punktą.

V. PRANEŠIMAS APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ

5.1. Duomenų tvarkytojas nedelsdamas, bet ne vėliau kaip per 8 (aštuonias) darbo valandas, nuo tada, kai jis sužinojo apie asmens duomenų saugumo pažeidimą, susijusį su Duomenimis tvarkomais pagal Susitarimą, nepriklausomai nuo to, ar asmens duomenų saugumo pažeidimas gali kelti pavojų fizinių asmenų teisėms ir laisvėms, pateikia elektroniniu paštu duomenuapsauga@vmu.lt Duomenų valdytojui pranešimą, kuriame būtų pateikiama bent tokia informacija:

5.1.1. data ir laikas, kada asmens duomenų saugumo pažeidimas įvyko ar buvo nustatytas, aprašytas asmens duomenų saugumo pažeidimo pobūdis, įskaitant, jei įmanoma, atitinkamų duomenų subjektų kategorijas ir apytikslį skaičių, atitinkamų asmens duomenų kategorijas ir apytikslį skaičių;

5.1.2. nurodyta kontaktinio asmens, galinčio suteikti daugiau informacijos, vardas, pavardė ir kontaktiniai duomenys;

5.1.3. aprašytos tikėtinos asmens duomenų saugumo pažeidimo pasekmės;

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

5.2. Jeigu visos informacijos apie asmens duomenų saugumo pažeidimą neįmanoma pateikti tuo pačiu metu ir (arba) atsiranda poreikis Duomenų valdytojui pateikti papildomą informaciją, Duomenų tvarkytojas privalo nedelsdamas, tačiau ne vėliau nei per 5 (penkias) darbo valandas nuo naujos informacijos sužinojimo momento, pateikti papildomą pranešimą Duomenų valdytojui, nurodydamas visą trūkstamą informaciją.

5.3. Duomenų tvarkytojas, atsižvelgiant į tvarkomų Duomenų pobūdį ir turimą informaciją, įsipareigoja pateikti Duomenų valdytojui turimą informaciją apie asmens duomenų saugumo pažeidimą ir jo tyrimą, per Duomenų valdytojo nurodytą protingą terminą.

5.4. Duomenų tvarkytojas, atsižvelgiant į tvarkomų Duomenų pobūdį ir turimą informaciją, įsipareigoja suteikti Duomenų valdytojui pagalbą, kurios reikia, kad būtų tinkamai pranešta apie asmens duomenų saugumo pažeidimą kompetentingai priežiūros institucijai ir (ar) duomenų subjektui (-ams).

5.5. Duomenų tvarkytojas įsipareigoja dokumentuoti visus asmens duomenų saugumo pažeidimus, susijusius su šio Susitarimo vykdymu, įskaitant su asmens duomenų saugumo pažeidimu susijusius faktus, jo poveikį ir taisomuosius veiksmus, kurių buvo imtasi. Duomenų valdytojui pareikalavus, Duomenų tvarkytojas turi pateikti šiuos dokumentus Duomenų valdytojui susipažinti, ypatingai, kai to reikalauja kompetentinga priežiūros institucija.

VI. SUBTVARKYTOJŲ PASITELKIMAS

6.1. Duomenų tvarkytojas, prieš pasitelkdamas subtvarkytoją (-us) konkrečiai Duomenų tvarkymo veiklai Duomenų valdytojo vardu atlikti, turi įgyvendinti Reglamento (ES) 2016/679 28 straipsnio 2 ir 4 dalyse ir šiame Susitarime nurodytus reikalavimus.

6.2. Duomenų tvarkytojas nepasitelkia subtvarkytojo Duomenų tvarkymui pagal šį Susitarimą be išankstinio konkretaus Duomenų valdytojo leidimo.

6.3. Duomenų tvarkytojas privalo gauti išankstinį konkretų Duomenų valdytojo leidimą pasitelkti konkretų subtvarkytoją, pateikdamas Duomenų valdytojui rašytinį prašymą dėl tokio leidimo gavimo prieš 30 (trisdešimt) kalendorinių dienų iki subtvarkytojo pasitelkimo. Prašyme nurodoma kokį subtvarkytoją ketinama pasitelkti, kokius asmens duomenis bus pavedama tvarkyti, kokius asmens duomenų tvarkymo veiksmus bus pavedama atlikti, kokios organizacinės ir techninės priemonės bus įgyvendintos apsaugant asmens duomenis, ar yra pasirašyta sutartis pagal Reglamento (ES) 2016/679 28 straipsnio 4 dalį su ketinamu pasitelkti subtvarkytoju ir kitą papildomą informaciją, reikšmingą tokio leidimo gavimui.

6.4. Duomenų tvarkytojas gali ir toliau naudotis iki šio Susitarimo pasitelkto (-ų) subtvarkytojo (-ų) paslaugomis, tačiau ne ilgiau negu galioja su juo (-ais) sudarytos sutartys ar susitarimai. Pasitelktų subtvarkytojų sąrašas pateikiamas Susitarimo 1 priede.

6.5. Pratęsiant sutartis ar susitarimus su subtvarkytoju (-ais), nurodytu (-ais) šio Susitarimo 6.4 papunktyje, Duomenų tvarkytojas privalo gauti išankstinį konkretų Duomenų valdytojo leidimą, kaip tai numatyta Susitarimo 6.3 papunktyje.

6.6. Duomenų tvarkytojas įsipareigoja pasirašyti rašytinius susitarimus su subtvarkytoju (-ais) ir juose nustatyti tas pačias duomenų apsaugos prievoles, kaip ir prievoles, nustatytas šiame Susitarime, visų pirma, prievolė savo lėšomis, tinkamomis techninėmis ir organizacinėmis priemonėmis užtikrinti Susitarimo vykdymo tikslais tvarkomų asmens duomenų apsaugą pagal Susitarimo, Reglamento (ES) 2016/679 ir kitų teisės aktų reikalavimus. Šis įsipareigojimas taikomas ir šio Susitarimo 6.4 papunktyje nustatytu atveju.

6.7. Duomenų tvarkytojas įsipareigoja reguliariai prižiūrėti savo pasitelkto (-ų) subtvarkytojo (-ų) veiksmus ir kai subtvarkytojas (-ai) nevykdo asmens duomenų apsaugos prievolių, Duomenų tvarkytojas išlieka visiškai atsakingas Duomenų valdytojui už subtvarkytojo (-ų) prievolių vykdymą. Tai nedaro įtakos duomenų subjektų teisėms pagal Reglamentą (ES) 2016/679, ypač toms, kurios numatytos Reglamento (ES) 2016/679 79 ir 82 straipsniuose, Duomenų valdytojo ir Duomenų tvarkytojo, įskaitant subtvarkytojus, atžvilgiu.

6.8. Pagal Duomenų valdytojo prašymą ir šiame prašyme nustatytais terminais Duomenų tvarkytojas įsipareigoja pateikti susitarimo (-ų) tarp Duomenų tvarkytojo ir subtvarkytojo (-ų) kopiją ir vėlesnius jo pakeitimus, suteikiant Duomenų valdytojui galimybę užtikrinti, kad būtų taikomos tos pačios duomenų apsaugos prievolės, kaip ir prievolės nustatytos šiame Susitarime.

VII. ASMENS DUOMENŲ PERDAVIMAS Į TREČIĄSIAS VALSTYBES AR TARPTAUTINĖMS ORGANIZACIJOMS

7.1. Pagal šį Susitarimą Duomenų tvarkytojas įsipareigoja ir sutinka tvarkyti Duomenis (įskaitant nuotolinę prieigą prie Duomenų) Europos ekonominės erdvės šalyse. Šis reikalavimas taip pat taikomas Duomenų tvarkytojo pasitelktam (-iems) subtvarkytojui (-ams) atliekant Duomenų tvarkymo veiksmus Duomenų valdytojo vardu.

7.2. Duomenų tvarkytojas gali perduoti Duomenis į trečiąsias valstybes, įskaitant perduoti Duomenų tvarkymą subtvarkytojui toje pačioje trečiojoje valstybėje ar kitoje trečiojoje valstybėje, tik gavęs Duomenų valdytojo dokumentais įformintus nurodymus ir laikantis Reglamento (ES) 2016/679 V skyriaus reikalavimų.

7.3. Nesant Duomenų valdytojo dokumentais pagrįstų nurodymų dėl Duomenų perdavimo į trečiąją valstybę, Duomenų tvarkytojas neturi teisės atlikti tokį perdavimą pagal Susitarimą.

7.4. Jei Duomenis trečiosioms valstybėms ar tarptautinėms organizacijoms reikia perduoti pagal Europos Sąjungos ar Lietuvos Respublikos 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.

7.5. Šis Susitarimas nėra standartinės duomenų apsaugos sąlygos, apibrėžtos Reglamento (ES) 2016/679 46 straipsnio 2 dalies c ir d punktuose, ir Šalys negali remtis Susitarimu kaip asmens duomenų perdavimo į trečiąsias valstybes ar tarptautinėms organizacijoms pagrindu pagal Reglamento (ES) 2016/679 V skyrių.

VIII. PAGALBA DUOMENŲ VALDYTOJUI

8.1. Atsižvelgdamas į Duomenų tvarkymo pobūdį, Duomenų tvarkytojas įsipareigoja padėti Duomenų valdytojui taikydamas tinkamas technines ir organizacines priemones, kiek tai įmanoma, kad būtų įvykdyta Duomenų valdytojo prievolė atsakyti į prašymus pasinaudoti Reglamento (ES) 2016/679 III skyriuje nustatytomis duomenų subjekto teisėmis (informavimas, susipažinti su duomenimis, reikalauti ištaisyti, papildyti ar ištrinti duomenis, apriboti duomenų tvarkymą, perkelti duomenis, nesutikti su duomenų tvarkymu, kai taikoma).

8.2. Gavus bet kokį valstybės institucijų ar duomenų subjekto paklausimą, prašymą ar reikalavimą, susijusį su Duomenų tvarkymu pagal Susitarimą, nedelsiant, bet ne vėliau kaip per 2 (dvi) darbo dienas, persiųsti jį Duomenų valdytojui registruotu paštu ar elektroniniu paštu. Duomenų tvarkytojas įsipareigoja pateikti visą turimą informaciją ir (ar) dokumentus, susijusius su Duomenų tvarkymu.

8.3. Jei taikoma, Duomenų tvarkytojas turi tvarkyti duomenų tvarkymo veiklos, vykdomos Duomenų valdytojo vardu pagal šį Susitarimą, įrašus. Duomenų valdytojui pareikalavus, ne vėliau kaip per 5 (penkias) darbo dienas, Duomenų tvarkytojas turi pateikti minėtus duomenų tvarkymo veiklos įrašus.

8.4. Jei taikoma, Duomenų tvarkytojas įsipareigoja suteikti Duomenų valdytojui reikiamą pagalbą atliekant poveikio duomenų apsaugai vertinimą, įskaitant vertinimui reikalingos techninės ir kitos turimos informacijos apie Duomenų tvarkytojo atliekamą ar planuojamą atlikti Duomenų valdytojo valdomų Duomenų tvarkymą (su sąlyga, kad ji nėra komercinė paslaptis), pateikimą Duomenų valdytojui ir konsultavimą šiais klausimais. Duomenų valdytojui konsultuojantis su priežiūros institucija Duomenų tvarkytojas turi suteikti turimą informaciją, kuri reikalinga konsultavimuisi.

8.5. Per Duomenų valdytojo nurodytą protingą terminą Duomenų tvarkytojas įsipareigoja pateikti Duomenų valdytojui turimą informaciją, būtiną siekiant įrodyti, kad vykdomos Susitarime, Reglamente (ES) 2016/679 ir kituose teisės aktuose nustatytos prievolės Duomenų tvarkytojui.

8.6. Susitarimas neatleidžia Šalių nuo kitų pareigų, kurios joms taikomos pagal Reglamento (ES) 2016/679 ir kitų teisės aktų reikalavimus.

IX. DUOMENŲ GRĄŽINIMAS IR SUNAIKINIMAS

9.1. Pagal Susitarimą Duomenų tvarkytojas saugo Duomenis smėliadėžėje debesyje Duomenų valdytojo nustatytą terminą. Suėjus nustatytam terminui, Duomenys yra sunaikinami.

X. AUDITAS IR TIKRINIMAS

10.1. Audito ar tikrinimo atlikimo procedūros, kai duomenis pagal Susitarimą tvarko Duomenų tvarkytojas:

10.1.1. Duomenų tvarkytojas įsipareigoja sudaryti sąlygas, neatlygintinai skirti auditui ar patikrinimui atlikti reikiamus išteklius bei padėti Duomenų valdytojui arba kitam Duomenų valdytojo įgaliotam auditoriui ar nepriklausomos trečios šalies auditoriui (toliau – Duomenų valdytojo atstovas) atlikti auditą, įskaitant patikrinimus.

10.1.2. Duomenų valdytojas informuoja Duomenų tvarkytoją apie planuojamą auditą ar patikrinimą ne vėliau kaip prieš 30 (trisdešimt) kalendorinių dienų.

10.1.3. Duomenų valdytojas padengia visas su audito atlikimu susijusias išlaidas, įskaitant, bet neapsiribojant ir apmokėjimą Duomenų valdytojo atstovui.

10.1.4. Vadovaudamasis tokio audito / patikrinimo išvadomis, Duomenų valdytojas gali reikalauti Duomenų tvarkytoją imtis papildomų priemonių, kad būtų užtikrinta atitiktis Reglamentui (ES) 2016/679, galiojančioms Europos Sąjungos ar Lietuvos Respublikos teisės aktų, reglamentuojančių asmens duomenų tvarkymą ir privatumo apsaugą, nuostatoms ir šio Susitarimo

sąlygoms. Duomenų tvarkytojas įsipareigoja nedelsdamas ištaisyti pastebėtus pažeidimus ir trūkumus ir apie tai raštu nedelsiant informuoti Duomenų valdytoją.

10.1.5. Duomenų valdytojas arba Duomenų valdytojo atstovas turi teisę tikrinti, įskaitant fiziškai tikrinti, vietas, kuriose Duomenų tvarkytojas tvarko Duomenis, įskaitant fizines patalpas ir informacines sistemas, naudojamas Duomenų tvarkymui ir susijusias su juo, siekiant įsitikinti, ar Duomenų tvarkytojas laikosi Reglamento (ES) 2016/679, galiojančių Europos Sąjungos ar Lietuvos Respublikos teisės aktų, reglamentuojančių asmens duomenų tvarkymą ir privatumo apsaugą, nuostatų ir šio Susitarimo sąlygų. Toks patikrinimas atliekamas, kai Duomenų valdytojas mano, kad to reikia.

10.1.6. Bet koks auditas / patikrinimas Duomenų tvarkytojo patalpose bus vykdomas tik Duomenų tvarkytojo darbo valandomis sukeliant kuo mažesnį įprastos darbo tvarkos sutrikdymą. Duomenų valdytojo atstovu negali būti Duomenų tvarkytojo ar jo pasitelktų subtvarkytojų konkurentas.

10.2. Audito ar tikrinimo atlikimo procedūros, kai Duomenis pagal Susitarimą tvarko subtvarkytojas:

10.2.1. Duomenų valdytojui pareikalavus, Duomenų tvarkytojas privalo pateikti audito / patikrinimo ataskaitą, siekiant patikrinti, ar subtvarkytojo (-ų) atliekamas Duomenų tvarkymas atitinka Reglamento (ES) 2016/679, galiojančių Europos Sąjungos ar Lietuvos Respublikos teisės aktų, reglamentuojančių asmens duomenų tvarkymą ir privatumo apsaugą, ir šio Susitarimo reikalavimus.

10.2.2. Duomenų valdytojas gali užginčyti audito / patikrinimo ataskaitos apimtį ir (arba) metodiką ir tokiais atvejais gali paprašyti naujo audito / patikrinimo pagal pakeistą taikymo sritį ir (arba) kitokią metodiką.

10.2.3. Vadovaudamasis tokio audito / patikrinimo išvadomis, Duomenų valdytojas gali reikalauti Duomenų tvarkytoją imtis papildomų priemonių, kad būtų užtikrinta atitiktis Reglamentui (ES) 2016/679, galiojančioms Europos Sąjungos ar Lietuvos Respublikos teisės aktų, reglamentuojančių asmens duomenų tvarkymą ir privatumo apsaugą, nuostatoms ir šio Susitarimo sąlygoms. Duomenų tvarkytojas įsipareigoja nedelsdamas imtis priemonių ar veiksmų, kad būtų ištaisyti pastebėti pažeidimai ir trūkumai ir apie tai nedelsiant raštu informuoti Duomenų valdytoją.

10.2.4. Duomenų tvarkytojas arba Duomenų tvarkytojo atstovas turi teisę tikrinti, įskaitant fiziškai tikrinti, vietas, kuriose subtvarkytojas (-ai) tvarko Duomenis, įskaitant fizines patalpas ir informacines sistemas, naudojamas Duomenų tvarkymui ir susijusias su juo, siekiant įsitikinti, ar subtvarkytojas (-ai) laikosi Reglamento (ES) 2016/679, galiojančių Europos Sąjungos ar Lietuvos Respublikos teisės aktų, reglamentuojančių asmens duomenų tvarkymą ir privatumo apsaugą, nuostatų ir šio Susitarimo sąlygų. Toks patikrinimas atliekamas, kai Duomenų valdytojas ar Duomenų tvarkytojas mano, kad to reikia.

10.2.5. Duomenų tvarkytojas nedelsiant turi pateikti Duomenų valdytojui susipažinti tokių patikrinimų dokumentus. Duomenų valdytojas gali užginčyti patikrinimo ataskaitos apimtį ir (arba) metodiką ir tokiais atvejais gali paprašyti atlikti naują patikrinimą pagal patikslintą taikymo sritį ir (arba) kitokią metodiką.

10.2.6. Vadovaudamasis tokio patikrinimo išvadomis, Duomenų valdytojas gali reikalauti Duomenų tvarkytoją imtis papildomų priemonių, kad būtų užtikrinta atitiktis Reglamentui (ES) 2016/679, galiojančioms Europos Sąjungos ar Lietuvos Respublikos teisės aktų, reglamentuojančių asmens duomenų tvarkymą ir privatumo apsaugą, nuostatoms ir šio Susitarimo sąlygoms. Duomenų tvarkytojas įsipareigoja nedelsdamas imtis priemonių ar veiksmų, kad būtų ištaisyti pastebėti pažeidimai ir trūkumai ir apie tai nedelsiant raštu informuoti Duomenų valdytoją.

10.2.7. Duomenų valdytojas gali, jei to reikia, inicijuoti ir dalyvauti fiziniame subtvarkytojo (-ų) tikrinime. Tai gali būti taikoma, jei Duomenų valdytojas mano, kad Duomenų tvarkytojo prižiūrimas subtvarkytojas (-ai) nepateikė Duomenų valdytojui pakankamai dokumentų, kad būtų galima nustatyti, ar subtvarkytojas (-ai) tvarko Duomenis Duomenų valdytojo vardu pagal Susitarimo sąlygas. Duomenų valdytojo dalyvavimas atliekant subtvarkytojo (-ų) patikrinimą nekeičia fakto, kad Duomenų tvarkytojui ir toliau tenka visa atsakomybė už subtvarkytojo (-ų) atitiktį Reglamentui (ES) 2016/679, galiojančioms Europos Sąjungos ar Lietuvos Respublikos teisės aktų, reglamentuojančių asmens duomenų tvarkymą ir privatumo apsaugą, nuostatoms ir šio Susitarimo sąlygoms.

10.2.8. Visi su auditu ar patikrinimu susiję kaštai bus padengiami tos Šalies, kuri užsakė auditą ar patikrinimą.

10.3. Duomenų tvarkytojas privalo suteikti Valstybinei duomenų apsaugos inspekcijai ar kitoms priežiūros institucijoms, kurios pagal galiojančius teisės aktus turi prieigą prie Duomenų

valdytojo ar Duomenų tvarkytojo įrenginių, arba jų įgaliotiems atstovams, veikiantiems tokių priežiūros institucijų vardu, visą informaciją, reikalingą atliekant duomenų apsaugos auditus ar patikrinimus, ir, laikantis Europos Sąjungos ir Lietuvos Respublikos teisės aktų reikalavimų, suteikti prieigą prie visos Duomenų tvarkymo įrangos ir (arba) fizinių priemonių tinkamam identifikavimui ar atlikti kitus Valstybinės duomenų apsaugos inspekcijos nurodytus veiksmus auditui ar kitam patikrinimui atlikti.

XI. ASMENS DUOMENŲ TVARKYMO TRUKMĖ

11.1. Duomenų tvarkytojas tvarko Duomenis ne ilgiau, nei tai yra būtina Susitarimo 1.2 papunktyje nurodytam Duomenų tvarkymo tikslui įgyvendinti. Užbaigus teikti su Duomenų tvarkymu pagal Susitarimą susijusias paslaugas arba Duomenų valdytojui raštu pareikalavus, Duomenų tvarkytojas atlieka Susitarimo IX skyriuje nurodytus veiksmus.

XII. ATSAKOMYBĖ

12.1. Duomenų tvarkytojas privalo atlyginti tiesioginius Duomenų valdytojo patirtus nuostolius, įskaitant ir Duomenų valdytojo sumokėtas netesybas, nuostolių atlyginimą ir / ar baudas, atsiradusias Duomenų tvarkytojui pažeidus šį Susitarimą, Reglamentą (ES) 2016/679, kitų teisės aktų reikalavimus ir (ar) Duomenų valdytojo nurodymus.

XIII. GINČŲ SPRENDIMAS

13.1. Šiam Susitarimui ir visoms iš šio Susitarimo kylančioms teisėms ir pareigoms taikomas Reglamentas (ES) 2016/679 ir Lietuvos Respublikos teisės aktai. Susitarimas sudarytas ir jam taikoma / Susitarimas turi būti aiškinamas vadovaujantis Lietuvos Respublikos teise.

13.2. Bet kokie nesutarimai ar ginčai, kylantys tarp Šalių dėl šio Susitarimo, sprendžiami abipusiu susitarimu / derybomis. Šalims nepavykus susitarti, bet kokie ginčai, nesutarimai ar reikalavimai, kylantys iš šio Susitarimo ar susiję su juo, jo pažeidimu, nutraukimu ar galiojimu, neišspręsti Šalių susitarimu, sprendžiami Lietuvos Respublikos įstatymų nustatyta tvarka Lietuvos Respublikos teismuose pagal Pirkėjo registruotą buveinę (išskyrus Lietuvos Respublikos teisės aktų imperatyviai nustatytus atvejus).

XIV. BAIGIAMOSIOS NUOSTATOS

14.1. Susitarimas sudarytas lietuvių kalba 1 (vienu) egzemplioriumi, Šalių pasirašytu kvalifikuotais elektroniniais parašais (teisinė galia nustatyta Lietuvos Respublikos elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų įstatymo 5 straipsnio 4 dalyje) Lietuvos Respublikos teisės aktų nustatyta tvarka.

14.2. Susitarimo sąlygos galioja visą laiką, kol Duomenų tvarkytojas teikia paslaugas pagal Susitarimą. Visais atvejais Susitarimas galioja ne ilgiau nei Sutartis / pagal Sutartį teikiamos Paslaugos. Susitarimo pasibaigimas ar nutraukimas neturi įtakos Susitarimo 4.1.9 papunkčio ar kitų Susitarimo nuostatų galiojimui, jeigu šios nuostatos pagal savo esmę išlieka galioti ir po Susitarimo pasibaigimo ar nutraukimo.

14.3. Visos išlaidos, patiriamos Duomenų tvarkytojui vykdant Susitarimą, patenka į Sutarties kainą. Joks kitas papildomas atlygis Duomenų tvarkytojui vykdant Susitarimo nuostatas nėra mokamas.

14.4. Esant prieštaravimams ar neatitikimams tarp Susitarimo ir Sutarties nuostatų, reglamentuojančių tuos pačius asmens duomenų tvarkymo santykius ar aspektus, pirmenybė yra teikiama Susitarimo nuostatoms.

14.5. Jei bet kuri šio Susitarimo nuostata tampa ar pripažįstama visiškai ar iš dalies negaliojanti, tai neturi įtakos kitų šio Susitarimo nuostatų galiojimui.

14.6. Šio Susitarimo priedai:

14.6.1. 1 priedas – „Pasitelktų subtvarkytojų sąrašas“, 1 lapas;

14.6.2. 2 priedas – „Techninės ir organizacinės priemonės“, 3 lapai.

XV. ŠALIŲ REKVIZITAI:

Duomenų valdytojas, Pirkėjas:	**Duomenų tvarkytojas, Tiekėjas:**
Valstybės įmonė Valstybinių miškų urėdija	UAB „Heksimus“

Įmonės kodas 132340880
PVM mokėtojo kodas LT323408811
Registracijos adresas:
Pramonės pr. 11A-9, 51327 Kaunas
Buveinės adresas:
Savanorių pr. 176, 03154 Vilnius
AB SEB bankas
A.s. LT84 7044 0600 0812 3597
Tel. +370 5 273 4021
El. p.: info@vmu.lt

Generalinis direktorius
Valdas Kaubrė

Įmonės kodas 300580894
PVM mokėtojo kodas LT100002552113
Adresas: Mindaugo g. 23A, LT-03231 Vilnius

Swedbank
A.s. LT867300010108076975
Tel. +370 5 2137307
El.p.: info@heximus.lt

Direktorė
Giedrė Ruginytė-Čepienė

Susitarimo dėl asmens duomenų tvarkymo
1 priedas

PASITELKTŲ SUBTVARKYTOJŲ SĄRAŠAS

Eil. Nr.	Juridinio asmens pavadinimas, kodas ar fizinio asmens vardas ir pavardė	Adresas	Duomenų tvarkymo aprašymas
1.			
2.			

Susitarimo dėl asmens duomenų
tvarkymo
2 priedas

TECHNINĖS IR ORGANIZACINĖS PRIEMONĖS

1. Organizacinės saugumo priemonės, kurias Duomenų tvarkytojas privalo įdiegti ir užtikrinti, kad jų būtų laikomasi yra šios:

1.1. Saugumo valdymas:

1.1.1. Saugumo politika. Duomenų tvarkytojas turi nustatyti dokumentuotą asmens duomenų saugumo politiką ir kasmet ją peržiūrėti.

1.1.2. Vaidmenys ir atsakomybės. Vaidmenys ir atsakomybės, susijusios su asmens duomenų tvarkymu, turi būti aiškiai apibrėžtos ir paskirstytos vadovaujantis saugumo politika. Keičiantis darbuotojams, teisių ir atsakomybės atšaukimo tvarka turi būti aiškiai apibrėžta, numatant ir aiškias jų perdavimo procedūras. Turi būti atliktas aiškus asmenų, atsakingų už konkrečias saugumo užduotis, paskyrimas, įskaitant saugos specialisto (saugos įgaliotinio) paskyrimą.

1.1.3. Prieigos valdymo politika. Nustatytas ir dokumentuotas prieigos valdymo procesas. Duomenų tvarkytojas šiame dokumente turi nustatyti atitinkamas prieigos kontrolės taisykles, prieigos teises ir apribojimus pagal konkrečias naudotojų ir privilegijuotų naudotojų pareigas, susijusias su asmens duomenų tvarkymo procesais ir procedūromis. Prieigos kontrolę užtikrinančių funkcijų atskyrimas (pvz., prieigos užklausų, prieigos leidimų, pačios prieigos administravimas) turi būti aiškiai apibrėžtas ir dokumentuotas. Prieiga prie duomenų ar informacinių technologijų (toliau – IT) infrastruktūros suteikiama tik tam darbuotojui, kuriam duomenys yra reikalingi konkrečioms darbo funkcijoms vykdyti pagal būtinumo žinoti principą. Darbo santykiams pasibaigus, prieigos darbuotojui panaikinamos ne vėliau, kaip paskutinę darbuotojo darbo dieną.

1.1.4. Pakeitimų valdymas. Duomenų tvarkytojas turi užtikrinti, kad visi IT pakeitimai būtų registruojami ir stebimi konkretaus asmens (pvz., IT skyriaus ar saugos įgaliotinio). Šis procesas turi būti reguliariai prižiūrimas. Programinės įrangos kūrimas turi būti atliekamas specialioje aplinkoje, kuri nebūtų sujungta su sistema, kurioje tvarkomi asmens duomenys. Kai reikalingas testavimas, turi būti naudojami išgalvoti (ne tikrieji) duomenys, o kai tai neįmanoma, turi būti taikomos specialios procedūros testavimui naudojamų asmens duomenų apsaugai. Turi būti įdiegta išsami ir dokumentais pagrįsta pokyčių valdymo politika. Pokyčių valdymo politiką turi apibrėžti: pokyčių įvedimo ir įdiegimo procedūras, pareigybes ir naudotojus, kurių teisės buvo pakeistos, pokyčių įdiegimo laiko terminus. Pokyčių valdymo politika turi būti reguliariai atnaujinama.

1.1.5. Duomenų tvarkytojai. Kai Duomenų tvarkytojas pasitelkia kitus duomenų tvarkytojus, jis privalo turėti nustatytas ir dokumentuotas gaires ir procedūras, reguliuojančias kitų duomenų tvarkytojų atliekamą asmens duomenų tvarkymą, kurios būtų taikomos kitiems duomenų tvarkytojams. Šios procedūros turi privalomai nustatyti tokį patį duomenų apsaugos lygį kaip ir Duomenų tvarkytojo saugumo politikoje. Duomenų tvarkytojas turi įpareigoti kitus duomenų tvarkytojus nedelsiant pranešti Duomenų tvarkytojui apie asmens duomenų saugumo pažeidimus, taip pat pateikti įrodymus dėl tinkamų saugumo priemonių įgyvendinimo.

1.2. Incidentų valdymas:

1.2.1. Asmens duomenų saugumo pažeidimai ir saugumo incidentai. Duomenų tvarkytojas privalo turėti reagavimo į saugumo incidentus planą su detaliomis procedūromis. Apie asmens duomenų saugumo pažeidimus ir saugumo incidentus nedelsiant turi būti informuojama Duomenų tvarkytojo vadovybė ir Duomenų valdytojas.

1.3. Veiklos tęstinumas:

1.3.1. Duomenų tvarkytojas turi nustatyti pagrindines procedūras, kurių reikia laikytis saugumo incidento ar asmens duomenų saugumo pažeidimo atveju, kad būtų užtikrintas reikiamas asmens duomenų tvarkymo IT sistemomis tęstinumas ir prieinamumas.

1.3.2. Veiklos tęstinumo planas turi būti išsamiai apibūdintas ir patvirtintas dokumentais (laikantis bendros saugumo politikos). Jame turi būti pateiktas aiškus veiksmų planas ir funkcijų paskirstymas. Veiklos tęstinumo plane turi būti apibrėžtas garantuotos paslaugų kokybės lygis, nustatytas pagrindiniams veiklos procesams, kurie užtikrina asmens duomenų saugumą.

1.4. Žmogiškieji ištekliai:

1.4.1. Konfidencialumo įsipareigojimai. Duomenų tvarkytojas privalo užtikrinti, kad visi darbuotojai suprastų savo pareigas ir atsakomybę, susijusią su asmens duomenų tvarkymu. Vaidmenys ir pareigos turi būti aiškiai išdėstyti darbuotojams prieš pradedant vykdyti jiems priskirtas funkcijas ir darbus. Darbuotojai, prieš pradėdami eiti savo pareigas, turi būti pasirašytinai supažindinti su organizacijos saugumo politika, taip pat pasirašyti atitinkamus informacijos konfidencialumo ir neatskleidimo susitarimus.

1.4.2. Mokymai. Duomenų tvarkytojas privalo užtikrinti, kad visi darbuotojai būtų tinkamai informuoti apie informacinės sistemos saugumo kontrolę, kuri susijusi su jų kasdieniu darbu. Darbuotojai, kurių darbas susijęs su asmens duomenų tvarkymu, turi būti informuojami apie atitinkamus asmens duomenų apsaugos reikalavimus ir teisinius įpareigojimus rengiant reguliarius mokymus, informavimo renginius ar instruktažus.

2. Techninės saugumo priemonės, kurias Duomenų tvarkytojas privalo įdiegti ir užtikrinti, kad jų būtų laikomasi yra šios:

2.1. Prieigų kontrolė ir autentifikavimas. Duomenų tvarkytojas turi įdiegti prieigų kontrolės sistemą, taikomą visiems naudotojams, prieinantiems prie informacinių technologijų sistemų, kuri leistų kurti, patvirtinti, peržiūrėti ir pašalinti naudotojų paskyras. Turi būti vengiama naudoti bendras naudotojų paskyras. Vietose, kur bendra naudotojų paskyra yra būtina, turi būti užtikrinta, kad visi bendros paskyros naudotojai turi tokias pat teises ir pareigas. Turi būti įdiegtas autentifikavimo mechanizmas, suteikiantis prieigą prie informacinės sistemos pagal prieigų kontrolės politiką. Autentifikavimui turi būti naudojamas bent jau naudotojo prisijungimo vardas ir slaptažodis, kuris atitiktų nustatytą sudėtingumo lygį. Prieigų kontrolės sistema turi gebėti nustatyti slaptažodžius, kurie neatitinka sudėtingumo lygio ir neleisti jų naudoti. Turi būti nustatytos ir dokumentais patvirtintos slaptažodžių naudojimo taisyklės. Taisyklėse turi būti apibrėžtas slaptažodžio ilgis, sudėtingumas, galiojimo laikas, nesėkmingų bandymų įvesti slaptažodį skaičius. Naudotojo slaptažodžiai turi būti saugomi naudojant kodavimo formą (angl. hash form).

2.2. Techninių žurnalų įrašai ir stebėsena. Techninių žurnalų įrašai turi būti įgyvendinti kiekvienai IT sistemai, taikomajai programai, naudojamai asmens duomenų tvarkymui. Turi būti saugomi įrašai apie prisijungimus, atsijungimus, nesėkmingus bandymus prisijungti. Techniniuose žurnaluose turi būti matomi visi įmanomi prieigų prie asmens duomenų įrašų tipai (pvz., data, laikas, peržiūrėjimas, keitimas, panaikinimas, kas atliko veiksmus). Visi sistemų administratorių (taip pat ir jų atliekamas naudotojo teisių papildymas, panaikinimas, keitimas) ir naudotojų veiksmai turi būti registruojami. Rekomenduojamas saugojimo terminas – ne trumpiau kaip 1 metai. Techninių žurnalų įrašai turi turėti laiko žymas ir būti apsaugoti nuo galimo sugadinimo, suklastojimo ar neautorizuotos prieigos. IT sistemose naudojami laiko apskaitos mechanizmai turi būti sinchronizuoti pagal bendrą laiko atskaitos šaltinį. Turi būti neįmanoma ištrinti ar pakeisti techninių įrašų turinio. Prieiga prie įrašų taip pat turi būti registruojama, siekiant atlikti neįprastų veiksmų susekimo stebėseną. Stebėsenos sistema turi apdoroti techninius žurnalų įrašus, ruošti sistemos būklės ataskaitas ir įspėti apie galimus pavojus. Techniniuose žurnalų įrašuose turi būti fiksuojami ir subtvarkytojų atliekami tvarkymo veiksmai.

2.3. Tarnybinių stočių, duomenų bazių apsauga. Duomenų bazės ir taikomųjų programų tarnybinės stotys turi būti sukonfigūruotos taip, kad veiktų korektiškai ir naudotų atskirą paskyrą su priskirtomis žemiausiomis operacinės sistemos privilegijomis. Duomenų bazės ir taikomųjų programų tarnybinės stotys turi apdoroti tik tuos asmens duomenis, kurie yra reikalingi darbo funkcijų atlikimui.

2.4. Darbo vietų apsauga. Duomenų tvarkytojo kompiuterinėse darbo vietose naudotojams turi būti apribota galimybė išjungti ar apeiti, išvengti saugumo nustatymų. Antivirusinės taikomosios programos ir jų informacijos apie virusus bei kenkimo programinę įrangą duomenų bazės turi būti atnaujinamos kasdien. Naudotojams negalima turėti privilegijų diegti, šalinti, administruoti neautorizuotos programinės įrangos. IT sistemos turi turėti nustatytą sesijos laiką, t. y. naudotojui esant neaktyviam sistemoje nustatytą laiką, sesija privalo būti nutraukta. Kritiniai operacinės sistemos saugos atnaujinimai, išleidžiami operacinės sistemos gamintojo, turi būti įdiegiami reguliariai ir nedelsiant.

2.5. Tinklų ir komunikacijos sauga. Visais atvejais, kai prieiga prie naudojamų IT sistemų yra vykdoma internetu, ryšys turi būti šifruojamas kriptografiniais protokolais. Belaidis ryšys prie IT sistemų turi būti leidžiamas tik tam tikriems naudotojams ir procesams. Belaidžio ryšio potinklis turi būti atskirtas nuo kitų potinklių. Belaidė prieiga turi būti apsaugota patikimais šifravimo

mechanizmais. Bet koks duomenų judėjimas iš, į IT sistemą turi būti stebimas ir kontroliuojamas naudojant ugniasienes ir įsibrovimo (įsilaužimo) aptikimo sistemas.

2.6. Mobilieji, nešiojamieji įrenginiai. Duomenų tvarkytojas nustato ir dokumentuoja Duomenų tvarkytojo naudojamų mobiliųjų, nešiojamųjų įrenginių (toliau – mobilieji, nešiojamieji įrenginiai) administravimo procedūras, aiškiai aprašant tinkamą tokių įrenginių naudojimą. Mobilieji, nešiojamieji įrenginiai prieš naudojimąsi turi būti užregistruoti ir autorizuoti. Mobilieji, nešiojamieji įrenginiai turi būti pakankamo prieigos kontrolės procedūrų lygio, kaip ir kita naudojama įranga asmens duomenims tvarkyti. Mobiliųjų, nešiojamųjų įrenginių valdymo funkcijos ir atsakomybės turi būti aiškiai apibrėžtos. Mobiliųjų, nešiojamųjų įrenginių vidiniai duomenų kaupikliai yra pilnai šifruojami.

2.7. Programinės įrangos sauga. Informacinės sistemose naudojama programinė įranga, skirta asmens duomenims apdoroti, turi atitikti programinės įrangos saugos gerąją praktiką, programinės įrangos kūrime taikomą saugos gerąją praktiką, programinės įrangos kūrimo struktūras, standartus. Specifiniai saugos reikalavimai turi būti apibrėžti pradiniuose programinės įrangos kūrimo etapuose. Turi būti laikomasi duomenų saugą užtikrinančių programavimo standartų ir gerosios praktikos. Programinės įrangos kūrimo, testavimo ir verifikacijos etapai turi vykti atsižvelgiant į pagrindinius saugos reikalavimus. Prieš paleidžiant programinę įrangą, turi būti atliktas šios įrangos pažeidžiamumo, pritaikomumo ir infrastruktūros atsparumo skverbimuisi įvertinimas. Programinė įranga negali būti patvirtinta, kol nėra pasiektas reikiamas saugumo lygis. Turi būti atliekami periodiški infrastruktūros atsparumo skverbimuisi testavimai. Programinės įrangos atnaujinimai turi būti ištestuoti ir įvertinti prieš juos diegiant į darbo aplinką atitinkamomis veiklos sąlygomis.

3. Atsižvelgiant į pavojaus asmens duomenų saugumui lygį, Duomenų tvarkytojas turi pasirinkti griežtesnes saugumo priemones, kad būtų užtikrinta tinkama asmens duomenų apsauga.