

TECHNINĖ SPECIFIKACIJA

1. SĄVOKOS IR SUTRUMPINIMAI

- 1.1. **Paslaugų tiekėjas** - ūkio subjektas – fizinis asmuo, privatusis juridinis asmuo, viešasis juridinis asmuo, kitos organizacijos ir jų padaliniai ar tokių asmenų grupė, su kuriuo Perkantysis subjektas sudaro Sutartį.
- 1.2. **Perkantysis subjektas** - AB „Amber Grid“, Lietuvos gamtinių dujų perdavimo sistemos operatorius.
- 1.3. **Perkančiojo subjekto darbo valandos** – darbo valandos, skaičiuojamos Perkančiojo subjekto darbo metu: I – IV 7:30 – 16:30, V 8:00 – 15:15. Darbo dienos trukmė prieš šventines dienas – viena valanda trumpiau.

2. PIRKIMO OBJEKTAS IR APIMTYS

- 2.1. Pirkimo objektas – Perkančiajam subjektui skirta, per išorinį internetinį adresą pasiekiamą erdvė skirta el. pasirašymo, parašų surinkimo ir kitų su el. dokumentais susijusių procesų valdymui (toliau – **Portalas**). Pirkimo objektas turi būti įskaičiuota Portalo konfigūravimo ir pritaikymo Perkančiojo subjekto poreikiams ir stiliui paslaugas.
- 2.2. Pradinis užsakomas naudotojų skaičius Portalui – 350 vnt.
- 2.3. Preliminarus el. parašų kiekis sutarties galiojimo laikotarpiui pasirašant Portale – **60 000** parašų.
- 2.4. Maksimali sutarties vertė – 30 000,00 Eur.
- 2.5. Perkančiajam subjektui turi būti sudaryta galimybė kiekvieną sutarties galiojimo mėnesį keisti pradinį Portalo naudotojų skaičių nurodytą 2.2 punkte. Tokiu atveju paslaugos Tiekėjas privalo perskaiciuoti mėnesinį paslaugos mokestį.
- 2.6. Perkantysis subjektas neįsipareigoja sutarties galiojimo laikotarpiu pirkti viso 2.3 punkte nurodyto preliminarus el. parašų kiekio, Perkantysis subjektas pirs el. parašų kiekį pagal poreikį.
- 2.7. Perkančiajam subjektui turi būti sudaryta galimybė kiekvieną sutarties galiojimo mėnesį keisti el. parašų kiekį nurodytą 2.3 punkte. Tokiu atveju paslaugos Tiekėjas privalo perskaiciuoti el. parašo ir el. parašo patikros įkainius, tuo atveju jei nuo perkamo kiekio priklauso įkainiai.

3. PASLAUGŲ TEIKIMO TERMINAI

- 3.1. Paslaugos pradedamos teikti nuo sutarties pasirašymo dienos ir teikiamos 36 mėnesius. Per 10 darbo dienų nuo sutarties pasirašymo dienos Paslaugų tiekėjas Perkančiojo subjekto administratoriams turi suteikti prieigą prie Portalo administravimo funkcijų.
- 3.2. Apmokėjimas už per kalendorinį mėnesį, kuris baigiasi einamojo mėnesio paskutinę dieną, mokėjimas už suteiktas paslaugas vykdomas per 30 d. po PVM sąskaitos faktūros pateikimo per informacinę e. sistemą dienos.

4. PAGRINDINIAI FUNKCINIAI REIKALAVIMAI PASLAUGOMS

- 4.1. Perkančiajam subjektui turi būti skirta atskira Portalo erdvė, pasiekiamą per interneto naršyklę HTTPS protokolu, dokumentų pasirašymui kvalifikuotu el. parašu, apimanti parašų surinkimo funkcionalumą, naudotojų paskyrų valdymą. Portalas ir jo siunčiami el. laiškai pasirašančioms šalims turi būti pritaikyti Perkančiojo subjekto (organizacijos) naudojamam įvaizdžio stiliui.
- 4.2. Portalas turi turėti funkcionalumą pasirašyti dokumentus Baltijos šalyse naudojamomis priemonėmis - Mobile-ID ir Smart-ID.
- 4.3. Portalas neturi reikalauti papildomų komponentų/įskiepių diegimo kompiuteryje.
- 4.4. Pagrindiniai Portalo funkcionalumai turi būti suderinami ir pasiekiami iš mobiliųjų įrenginių t.y. išmaniųjų mobiliųjų telefonų ir planšetinių kompiuterių su iOS ir Android operacinėmis sistemomis.
- 4.5. Turi būti galimybė įkelti pasirašomo el. dokumento failus į Portalą. Sekti pasirašomų dokumentų būsena (veiklos istoriją), kuri leidžia:

- 4.5.1. Matyti, kuris darbuotojas ir kada įkėlė dokumentą pasirašymui;
- 4.5.2. Matyti, kada ir kieno pasirašomas dokumentas buvo peržiūrėtas;
- 4.5.3. Matyti, kada ir kieno dokumentas buvo pasirašytas.
- 4.6. Portalas turi leisti įkelti, pasirašyti bei patikrinti (ar el. parašas galioja ir turi juridinę galią) tokius Europos Parlamento ir Tarybos reglamentą Nr. 910/2014 („eIDAS“) atitinkančius el. parašo dokumentų formatus: Portable Document Format (PDF), Associated Signature Container (ASiCE) bei Baltijos šalyse naudojamus formatus ADoc, BDoc (Edoc).
- 4.7. Portale pasirašyti dokumentai turi būti paženklinėti pasirašiusiojo asmens el. parašo atvaizdavimu/anotacija.
- 4.8. Portalas turi turėti galimybę peržiūrėti pasirašiusių asmenų sertifikatų informaciją.
- 4.9. Turi būti užtikrinta galimybė, Portale sukurtus parašus pakelti iki ilgalaikio saugojimo lygmens.
- 4.10. Portale turi būti galimybė kurti bei koreguoti dokumentų pasirašymo procesus, dokumentų pasirašymo sekas, keisti pasirašančių asmenų sąrašą ir eiliškumą.
- 4.11. Portalas turi turėti galimybę išsiųsti informacinius pranešimus apie pateiktą dokumentą pasirašančiajam asmeniui, apie sėkmingą dokumentu pasirašymą iniciatoriui.
- 4.12. Portalas turi turėti galimybę modifikuoti pasirašančių asmenų sąrašą, kol asmuo nėra pasirašęs dokumento.
- 4.13. Portalas turi turėti administravimo sistemę (Perkančiojo subjekto vartotojų administravimui, licencijų vartotojams priskyrimui bei veiklos auditui) su funkcijomis:
 - 4.13.1. Galimybė valdyti naudotojų/pasirašančiųjų teises;
 - 4.13.2. Galimybė peržiūrėti atliktų veiksmų istoriją (informacija, kada dokumentas buvo sukurtas, peržiūrėtas ar pasirašytas);
 - 4.13.3. Galimybė nustatyti dokumento pasirašymo terminus;
 - 4.13.4. Galimybė siųsti automatinis pranešimus (priminimus) kitoms pasirašančioms šalims, kad jos spėtų pasirašyti dokumentus laiku;
 - 4.13.5. Galimybė išsaugoti kontaktus adresų knygoje bei juos kategorizuoti;
 - 4.13.6. Galimybė kategorizuoti įkeltus dokumentus;
 - 4.13.7. Galimybė atlikti grupinius veiksmus t. y. keleto dokumento atsissiuntimas. Pasirašymas ar panaikinimas vienu mygtuko paspaudimu.
- 4.14. Portalas turi gebėti atlikti dokumentų validaciją ir žiniatinklio resursų pagalba pateikti pasirašytų dokumentų struktūrą, metaduomenis, juose esančius dokumentus. Portalas turi gebėti nuskaityti XAdES, PAdES tipo parašus ir nustatyti jų formatą.
- 4.15. Portalas turi turėti galimybę vienu el. parašu pasirašyti kelis skirtingus dokumentus, taip pat palaikyti funkcionalumą, užtikrinantį, kad vienu metu kelių pasirašomų dokumentų formatų tipai ir versijos gali būti skirtingos (ADoc, PDF ir pan., nepriklausomai nuo formatų versijų).
 - 4.15.1. Portalas turi gebėti atlikti naudotojų identifikaciją (prisijungimą) naudojant Mobile-ID;
 - 4.15.2. Portalas turi gebėti atlikti naudotojų identifikaciją (prisijungimą) naudojant didžiųjų Lietuvos bankų (Swedbank, SEB, Luminor, „Artea“ bankas) išduotu kvalifikuotu Smart-ID.
- 4.16. Dokumentų pasirašymo Portalas turi palaikyti lietuvių ir anglų kalbas.
- 4.17. Tiekėjas turi turėti pagalbos tarnybą, kuria Perkančiojo subjekto atstovai galėtų pranešti apie Portalo sutrikimus ar gauti konsultacijas Portalo naudojimosi ar administravimo klausimais.
- 4.18. Tiekėjas turi apmokyti Perkančiojo subjekto darbuotojus naudotis Portalu (įtraukiant, bet neapsiribojant apmokymo temomis: vartotojų kūrimas, Portalo administravimas, kiti Perkančiojo subjekto Portalo nustatymai), taip pat pateikti Portalo ir jame teikiamų paslaugų bazinę techninę dokumentaciją (vartotojų ir administravimo instrukcijas).
- 4.19. Tiekėjas turi atlikti Perkančiojo subjekto naudotojų paskyrų importavimo paslaugą.
- 4.20. Tiekėjas turi pritaikyti Perkančiojo subjekto organizacijos stiliaus pritaikymą visuose portalo siunčiamuose el. laiškuose.
- 4.21. Tiekėjas turi užtikrinti, kad visuose portalo siunčiamuose el. laiškuose siuntėjo adresas ir (ar) siuntėjo pavadinimas aiškiai nurodytų Perkančiojo subjekto portalo erdvės adresą pavadinimą

5. KITI REIKALAVIMAI PASLAUGOMS

- 5.1. Dokumentų talpos vieta Portale turi būti neribojama.
- 5.2. Paslaugos turi būti teikiamos nepertraukiamai, 7 dienas per savaitę, 24 valandas per parą.
- 5.3. Tiekėjo informacijos vadybos sistema turi atitikti informacijos saugumo valdymo standarto ISO 27001 reikalavimus.

5.4. Perkančiojo subjekto duomenys, esantys Portale, privalo būti fiziškai saugomi duomenų centre, esančiame Europos ekonominės erdvės ribose ne trumpiau nei iki tarpusavio sutarties pabaigos.

5.5. Tiekėjas privalo užtikrinti incidentų ir problemų registravimo, sekimo bei valdymo procesą ir pateikti aiškų kontaktą (el. paštu, telefonu ir (ar) aptarnavimo sistemoje), skirtą incidentams registruoti, taip pat užtikrinti incidentų būklės stebėjimą ir informavimą apie jų sprendimo eigą galimybę.

5.6. Tiekėjas, jo subtiekiejai, ūkio subjektai, kurių pajėgumais remiamasi, gamintojai, techninės ar programinės įrangos priežiūrą ir palaikymą vykdančias asmenys ar juos kontroliuojantys asmenys negali teikti paslaugų iš valstybių ar teritorijų, nurodytų LRV 2022 m. kovo 30 d. nutarime Nr. 280 Dėl Lietuvos Respublikos viešųjų pirkimų įstatymo 92 straipsnio 13, 14 ir 15 dalių nuostatų įgyvendinimo (e-tar.lt) (aktualioje redakcijoje).

5.7. Sistema turi veikti informacijos saugos ISO27001 arba lygiavertės sertifikatuose tiekėjų debesijos (angl. „Cloud“) duomenų centruose.

5.8. Reikalavimai šifravimui:

5.8.1. Sistema turi būti saugoma šifruotoje saugykloje;

5.8.2. Sistemoje turi būti naudojami šifravimo raktai. Turi būti užtikrinamas šifravimo raktų saugumas. Šifravimo raktų ilgis turi būti ne mažesnis kaip 256 bitai;

5.8.3. Sistema turi užtikrinti pilną duomenų šifravimą (angl. end-to-end encryption), t.y. duomenys turi būti šifruojami perdavimo metu tarp paslaugos ir naudotojų kompiuterių metu, bei duomenų bazėse, tarnybinėse stotyse ir atsarginėse kopijose;

5.8.4. Sistemoje saugoma jautri ir (ar) konfidenciali informacija turi būti apsaugota taip, kad ji negalėtų būti dešifruota ar pasiekama iš išorės, t. y. be tinkamos autorizacijos ir prieigos teisės. Net jei visa sistema yra šifruojama, turi būti užtikrinta, kad vidinė prieigos kontrolė ribotų prieigą prie skirtingo jautrumo informacijos, o šifravimo raktai ir mechanizmai nebūtų prieinami neautorizuotiems naudotojams ar trečiosioms šalims.

5.9. Reikalavimai žurnalizavimui:

5.9.1. Sistemoje turi būti kaupiama ir ne mažiau kaip 6 mėnesius saugoma audito informacija apie operacijas su duomenimis (angl. logs). Turi būti saugoma informacija apie veiksmus su duomenimis, naudotojus, kurie atliko veiksmus su duomenimis, veiksmų datas ir laikus;

5.9.2. Numatyti Sistemos naudotojai turi galėti lengvai peržiūrėti konkrečių audito įrašų informaciją (tiek ekraninėje formoje, tiek ataskaitoje);

5.9.3. Sistemos administratoriams turi būti panaikinta galimybė ištrinti ar redaguoti administratoriaus veiksmų žurnalinius įrašus;

5.9.4. Sistemos audito įrašai negali būti redaguojami ar kitaip keičiami;

5.9.5. Turi būti kaupiami šie (neapsiribojant, tikslus sąrašas derinamas) žurnalizavimo įrašai:

- a) Naudotojo identifikatorius;
- b) Įvykių laikai;
- c) Kompiuterio, iš kurio jungiamasi, informacija, šaltinio IP;
- d) Sėkmingų / nesėkmingų bandymų prisijungti įrašai;
- e) Administratoriaus teisių naudojimas;
- f) Prieigos teisių pokyčiai;
- g) Sistemos konfigūracijos keitimas;
- h) Sistemos / tinklo parametrų, laiko ir (ar) datos pakeitimai;
- i) Įvykių registravimo funkcijos įjungimas / išjungimas;
- j) Įvykių trynimas, kūrimas ir (ar) keitimas;
- k) Resursai, prie kurių buvo suteikta prieiga;
- l) Sisteminiai ir saugumo pranešimai;
- m) Informacija apie veiksmus su naudotojais.

5.10. Perkančiojo subjekto administruojami duomenys, duomenų atsarginės kopijos privalo būti apsaugotos bent dviejų lygių autentifikavimo sistema;

5.11. Sistemoje turi būti užtikrintas atsarginio kopijavimo sistemos veikimas, kad sistemos atkūrimas tenkintų tokius reikalavimus (reikalavimas taikomas Sistemos darbo aplinkai):

5.12. Atkūrus duomenis turi būti atliekamas duomenų atkūrimo kokybės patikrinimas, norint įsitikinti ar buvo išlaikytas duomenų teisingumas ir vientisumas;

5.13. Sistema turi būti internetinė taikomoji sistema (angl. Web Application). Sistemos naudotojo kompiuteryje (darbo vietoje) neturi būti instaliuojami jokie Sistemos komponentai, išskyrus naudotojo kompiuteryje gali būti instaliuojamas papildomas bendrinis programinis komponentas, jei toks programinis komponentas pasiūlomas įdiegti jungiantis prie Sistemos, nereikalaujantis papildomo licencijų įsigijimo ar nesukelia įsipareigojimo Perkančiajam subjektui mokėti naudojimo mokesčius, jo įdiegimas nereikalauja specialių žinių, ir jei toks programinis komponentas nebuvo įdiegtas anksčiau.

5.14. Sistema turi atitikti sesijos valdymo reikalavimus. Privalomas funkcionalumas HTTPS sesijos apsaugai:

- 5.14.1. Apsaugoti lankytojo/naudotojo visą sesiją SSL (nežemesnė kaip 1.3 versija), TLS pagalba;
- 5.14.2. Neįtraukti sesijos ID į URL adresą arba nesiųsti jo siunčiamos užklausoje antraštėje (angl. Referrer header);
- 5.14.3. Užtikrinti, kad sesijos ID yra ilgas, sudėtingas, sugeneruotas iš atsitiktinių skaičių ir negali būti lengvai atspėjamas;
- 5.14.4. Draudžiama saugoti sesijos ID;
- 5.14.5. Sesijos ID turi būti šifruojamas ne mažesniu kaip 128 bitų ilgio raktu;
- 5.14.6. Išvalomas sesijos objektas naudotojui išsiregistravus arba sesijai nustojus galioti;
- 5.14.7. Sistemos naudotojui neatliekant veiksmų ilgiau kaip 30 minučių, prisijungimo sesija automatiškai turi būti uždaryta (angl. „logged off“).

5.15. Sistemos naudotojo sąsajos turi būti suderinamos su šiomis naršyklėmis:

- 5.15.1. Microsoft Edge (iki Sistemos naudojimo etapo pradžios vėliausios išleistos versijos).
- 5.15.2. Google Chrome (iki Sistemos naudojimo etapo pradžios vėliausios išleistos versijos).

5.16. Sistemoje turi būti galimybė įveikinti vieno prisijungimo sistemą (angl. Single Sign-On, SSO);

5.17. Naudotojų autorizacija:

- 5.17.1. Sistemoje pateikiamą informaciją gali matyti ir veiksmus atlikti tik autentifikavęsi naudotojai;
- 5.17.2. Sistemoje autorizavimo mechanizmas turi būti realizuotas remiantis rolių modeliu (angl. Role-based Model) ir valdomas centralizuotai;
- 5.17.3. Sistemoje naudotojas turi galėti peržiūrėti tik tokią informaciją ir naudotis tik tokiomis funkcijomis, kurios yra nustatytos priėmimo teisėmis, pvz., jei Sistemoje naudotojas nori peržiūrėti informaciją, kuri yra nepriskirta jo rolei, Sistema turi rodyti pranešimą naudotojui, kad jis neturi prieigos prie informacijos teisės ir kitais būdais apriboti informacijos peržiūrą;
- 5.17.4. Sistema turi turėti integraciją su Perkančiojo subjekto MS Entra ID ir būti pritaikyta saugiai pasiekti iš bet kur ir iš bet kokio įrenginio. Integracijos realizacija Perkantysis subjektas rūpinsis pats, o Tiekėjas suteiks reikalingą pagalbą. Nesant MS Entra ID Integracijos funkcionalumui, MFA yra privalomas;
- 5.17.5. Suspendavus naudotoją Perkančiojo subjekto Microsoft Entra ID paslaugoje, naudotojas turi būti suspenduotas Sistemoje;
- 5.17.6. Prieigos teisių valdymui turi būti galimybė sukonfigūruoti kelių veiksmų autentifikavimą (angl. multi-factor authentication), suderinami su Perkančiojo subjekto naudojama tapatybės valdymo infrastruktūra:

a Palaikomi MFA metodai, bet neapsiriboja:

- i TOTP (Time-based One-Time Password), generuojamas mobiliojoje programėlėje (pvz., Microsoft Authenticator, Google Authenticator);
- ii SMS žinutės su vienkartinio kodu;
- iii El. pašto laiškas su patvirtinimo kodu;
- iv Push notifications į mobiliųjų įrenginių;
- v Kiti metodai, suderinami su Perkančiojo subjektu, užtikrinantys saugų autentifikavimą.

b MFA sesijos galiojimo laikas: maksimaliai 8 valandos;

c Blokavimas po 5 nesėkmingų bandymų 15 minučių.

- 5.18. Sistemoje slaptažodžiai negali būti saugomi atviru tekstu;
- 5.19. Sistema turi būti apsaugota nuo nesankcionuotos prieigos;
- 5.20. Sistemoje turi būti užtikrintos priėjimo prie Sistemos apsaugos priemonės nuo kenkėjiškų programų atakų, pvz., IPS / IDS sistemos, ugniasienė;
- 5.21. Turi būti užtikrintas ne mažesnis kaip 99,95% paslaugos pasiekiamumas;
- 5.22. Paslaugų atstatymo taškas (RPO) turi būti ne ilgesnis nei 1 valanda, paslaugų atstatymo laikas (RTO) turi būti ne ilgesnis nei 2 valandos;
- 5.23. Ilgiausias leistinas paslaugų sutrikimo periodas (MTPOD) turi būti ne didesnis nei 4 valandos;
- 5.24. Paslaugų tiekėjas turi taikyti nuolaidas mėnesiniam paslaugų mokesčiui, jeigu:
 - 5.24.1. Paslaugos pasiekiamumas yra 99,5% - 99,0% - 10% nuolaida mėnesiniam mokesčiui;
 - 5.24.2. Paslaugos pasiekiamumas yra 99,0% - 95,0% - 30% nuolaida mėnesiniam mokesčiui;
 - 5.24.3. Paslaugos pasiekiamumas yra mažesnis nei 95% - 100% nuolaida mėnesiniam mokesčiui.

6. BENDRIEJI SAUGOS REIKALAVIMAI

6.1. Kibernetinio saugumo incidentų valdymas:

- 6.1.1. Tiekėjas, nustatęs arba sužinojęs, kad jo valdomoje infrastruktūroje įvyko kibernetinio saugumo incidentas, galintis paliesti Perkančiojo subjekto duomenis ar informacinius išteklius, privalo nedelsdamas, bet ne vėliau kaip per 24 (dvidešimt keturias) valandas nuo šio fakto nustatymo ar sužinojimo pateikti Užsakovui ankstyvą įspėjimą.
- 6.1.2. Per 72 val. nuo sužinojimo Tiekėjas pateikia išsamų pranešimą kuriame nurodo:
 - 6.1.2.1. Incidento pobūdį ir mastą,
 - 6.1.2.2. Poveikio vertinimą,
 - 6.1.2.3. Taikytas pirmines priemones.
- 6.1.3. Tiekėjas teikia tarpines ir galutinę ataskaitą pagal Perkančiojo subjekto prašymą.
- 6.1.4. Tarpinių ir galutinės ataskaitos turinį ir pateikimo terminus Tiekėjas teikia Užsakovui pagal Perkančiojo subjekto nurodymus, vadovaudamasis LR kibernetinio saugumo įstatymo ir NKSC nustatytomis incidentų pranešimo pareigomis.
- 6.1.5. Informavimo kanalai: Pranešimai teikiami už sutarties vykdymą atsakingiems Perkančiojo subjekto darbuotojams arba Perkančiojo subjekto Informacijos saugos atstovams. Informacija turi būti autentiška ir, jei prašoma, užšifruota.

6.2. Perkančiajam subjektui pareikalavus, Tiekėjas turi pateikti saugumo testavimo ataskaitą arba sudaryti sąlygas Perkančiajam subjektui atlikti saugumo testavimą (angl. „Pentest“).

6.3. Tiekėjo darbuotojų darbo priemonėse:

- 6.3.1. naudojama gamintojų palaikoma aparatinė įranga, kuriai įdiegtos visos gamintojo išleistos saugos pataisos (įskaitant aparatinės programinės įrangos atnaujinimus);
- 6.3.2. privalo būti įdiegta ir veikianti galiojanti antivirusinė sistema, atitinkanti tarptautinius saugumo standartus (pvz., ESET, Microsoft Defender for Endpoint ar kiti lygiaverčiai sprendimai). Antivirusinė programinė įranga neturi būti kilusi iš šalių, kurių gamintojai ar produktai pagal galiojančius teisės aktus gali kelti grėsmę nacionaliniam saugumui, kaip tai apibrėžta Lietuvos Respublikos viešųjų pirkimų įstatymo 37 str. 9 d. ir 47 str. 9 d. nuostatose, t. y., naudojama antivirusinė programinė įranga negali prieštarauti Perkančiajam subjektui taikomiems nacionalinio saugumo reikalavimams. Perkančiajam subjektui pareikalavus, Tiekėjas turi pateikti informaciją apie naudojamos antivirusinės programinės įrangos gamintoją ir kilmę.

6.4. Duomenų tvarkymas ir saugojimas:

- 6.4.1. Duomenų minimizavimas: Tiekėjas įsipareigoja nenaudoti, nekopijuoti ir nesaugoti daugiau Perkančiojo subjekto informacijos, nei yra būtina sutarties tikslams pasiekti.
- 6.4.2. Duomenų šifravimas:

6.4.2.1. Saugomųjų duomenų šifravimas (Encryption at Rest): Visa Perkančiojo subjekto informacija, laikinai saugoma Tiekėjo įrenginiuose, privalo būti užšifruota (pvz., BitLocker, FileVault).

6.4.2.2. Perduodamųjų duomenų šifravimas (Encryption in Transit): Visi duomenys, perduodami tinklais, privalo būti šifruojami naudojant saugius protokolus (pvz., TLS 1.3, SFTP, VPN).

6.4.2.3. Draudimas naudoti asmenines priemones: Griežtai draudžiama Perkančiojo subjekto informaciją tvarkyti naudojant asmenines el. pašto dėžutes, nepatvirtintas debesijos paslaugas ar asmenines laikmenas.

6.4.2.4. Duomenų Lokalizacija: Tiekėjas įsipareigoja užtikrinti, kad visi Perkančiojo subjekto duomenys bus saugomi ir tvarkomi tik Europos Sąjungos (ES) / Europos Ekonominės Erdvės (EEE) valstybių narių teritorijoje arba šalyse, kurioms Europos Komisija yra priėmusi sprendimą dėl tinkamo duomenų apsaugos lygio. Bet koks duomenų perdavimas už šių jurisdikcijų ribų yra galimas tik gavus išankstinį raštišką Perkančiojo subjekto sutikimą.

6.5. Veiksmai po Sutarties pabaigos:

6.5.1. Saugus duomenų perdavimas ir sunaikinimas:

6.5.1.1. Visa Perkančiojo subjekto informacija saugiai perduodama Perkančiajam subjektui, sutartu formatu.

6.5.1.2. Perkančiojo subjekto informacijos sunaikinimas (ištrynimasis), Perkančiajam subjektui pateikus prašymą, turi būti atliktas nedelsiant, bet ne vėliau kaip per 30 (trisdešimt) kalendorinių dienų nuo prašymo gavimo dienos, atsižvelgiant į technines, organizacines ir ekonomines galimybes. Informacija, kuri dėl techninių apribojimų išlieka atsarginėse kopijose, turi būti automatiškai ir negrįžtamai ištrinama per įprastą atsarginių kopijų saugojimo ciklą, tačiau ne vėliau kaip per 90 (devyniasdešimt) kalendorinių dienų. Perkančiajam subjektui pareikalavus, Tiekėjas pateikia rašytinį sunaikinimo patvirtinimą (sunaikinimo aktą).

6.5.1.3. Perkančiajam subjektui pareikalavus, Tiekėjas privalo pateikti raštišką patvirtinimą (sunaikinimo aktą), kad visa Perkančiojo subjekto informacija buvo sunaikinta.

6.5.2. Perkantysis subjektas pasilieka teisę, iš anksto įspėjęs ne vėliau kaip prieš 60 (šešiasdešimt) kalendorinių dienų, atlikti Tiekėjo taikomų saugumo priemonių auditą, siekdamas įsitikinti šioje specifikacijoje nurodytų reikalavimų laikymąsi. Auditą Tiekėjas gali atlikti savo jėgomis arba pasitelkti nepriklausomus trečiųjų šalių atstovus (auditorius). Tiekėjas įsipareigoja bendradarbiauti su Perkančiuoju subjektu ir (arba) jo pasitelktais atstovais audito atlikimo metu.