DUOMENŲ VALDYMO PLATFORMOS, REIKALINGOS VALSTYBĖS DUOMENŲ VALDYSENOS INFORMACINEI SISTEMAI ĮGALINTI IR VEIKTI, LICENCIJOS, ĮSKAITANT PLATFORMOS DIEGIMĄ, PIRKIMO SUTARTIS

2020 m. lapkričio 6 d. Nr. STAT-114 (2020)
Vilnius

Lietuvos statistikos departamentas, juridinio asmens kodas 188600177, buveinės adresas Gedimino pr. 29, 01500 Vilnius, atstovaujamas generalinės direktorės Jūratės Petrauskienės (toliau – Užsakovas), ir Palantir Technologies UK, Ltd., juridinio asmens kodas 7042994, atstovaujama Matt Long, kuris yra Palantir Technologies UK, Ltd. įgaliotas atstovas (toliau – Tiekėjas), toliau kartu vadinamos „Šalimis", o kiekviena iš jų atskirai – „Šalimi", atsižvelgdamos į Viešosios įstaigos CPO LT atlikto pirkimo Nr. 497018 „Duomenų valdymo platformos, reikalingos Valstybės duomenų valdysenos informacinei sistemai įgalinti ir veikti, licencija, įskaitant platformos diegimą", vykdyto atviro konkurso būdu (toliau – pirkimas) rezultatus, sudarė šią pirkimo sutartį (toliau – Sutartis):

1. SUTARTIES DALYKAS

1.1. Tiekėjas įsipareigoja pristatyti Užsakovui bei parengti darbui duomenų valdymo platformos, reikalingos Valstybės duomenų valdysenos informacinei sistemai įgalinti ir veikti, licenciją (toliau – prekės) tokia apimtimi ir sąlygomis, kaip detalizuota Sutarties priede „Techninė specifikacija" (toliau – Techninė specifikacija), o Užsakovas įsipareigoja atsiskaityti su Tiekėju Sutarties sąlygų 3 skyriuje nustatyta tvarka.

2. ŠALIŲ TEISĖS IR ĮSIPAREIGOJIMAI

2.1. Tiekėjas įsipareigoja:

2.1.1 tinkamai ir laiku pristatyti prekes, atitinkančias Sutartyje ir Techninėje specifikacijoje nustatytus reikalavimus:

2.1.1.1 duomenų valdymo platforma turi būti įdiegta per 1 (vieną) mėnesį (31 kalendorinę dieną) nuo Sutarties pasirašymo dienos;

2.1.1.2 COVID-19 informacinės sistemos duomenų įsisavinimo, transformacijų ir realizuotų duomenų vizualizavimo sprendimų perkėlimas turi būti atliktas per 1 (vieną) mėnesį (31 kalendorinę dieną) nuo pirkimo sutarties pasirašymo dienos;

2.1.1.3 tarpžinybinės duomenų saugyklos ir Integruotos statistikos informacinės sistemos duomenų šaltinių duomenų paėmimas turi būti atliktas per 9 (devynis) mėnesius nuo pirkimo sutarties pasirašymo dienos;

2.1.1.4 duomenų valdymo platformos licencija turi galioti ne trumpiau nei 12 (dvylika) mėnesių nuo Sutarties 2.1.1.1 punkte nustatyto Tiekėjo įsipareigojimo įvykdymo dienos;

2.1.1.5 duomenų valdymo platformos palaikymas ir reikiamų infrastruktūros paslaugų teikimas turi būti užtikrintas ne trumpiau nei 12 (dvylika) mėnesių nuo Sutarties 2.1.1.1 punkte nustatyto Tiekėjo įsipareigojimo įvykdymo dienos;

2.1.1.6 turi būti apmokyta iki 10 Užsakovo specialistų (iki 2 sistemos ir duomenų administratorių ir iki 8 duomenų analitikų) ir pateikti išsamią platformos administratorių ir naudotojų mokymo medžiagą;

2.1.2. vykdydamas sutartinius įsipareigojimus, laikytis konfidencialumo, neatskleisti tretiesiems asmenims žodžiu, raštu ar kitokiu pavidalu gautos dalykinės, finansinės bei kitokios konfidencialios informacijos, su kuria buvo supažindintas arba ji tapo prieinama ir žinoma bendradarbiaujant su Užsakovu;

2.1.3. nedelsdamas informuoti Užsakovą laikantis pirkimo sutarties sąlygų apie aplinkybes, trukdančias laiku ir kokybiškai vykdyti prisiimtus įsipareigojimus;

2.1.4. pasikeitus už pirkimo sutarties vykdymą atsakingam asmeniui ir (ar) jo kontaktiniams duomenims, ne vėliau kaip per 5 (penkias) darbo dienas apie tai informuoti Užsakovą arba jo įgaliotą asmenį.

LICENCE (ACCOMPANIED BY SYSTEM DEPLOYMENT SERVICE) FOR THE DATA MANAGEMENT PLATFORM NECESSARY FOR THE SETTING UP AND OPERATION OF THE STATE DATA GOVERNANCE INFORMATION SYSTEM PURCHASE CONTRACT

Year 2020 November 6 , No. STAT-114 (2020)
Vilnius

The Lithuanian Department of Statistics (Lietuvos statistikos departamentas), incorporation number 188600177, office address Gedimino Ave. 29, 01500 Vilnius, Lithuania, represented by Director General Jūratė Petrauskienė (hereinafter referred to as the "Customer"), and Palantir Technologies UK, Ltd., incorporation number 7042994, represented by Matt Long, Authorised Signatory of Palantir Technologies UK, Ltd. (hereinafter referred to as the "Supplier"), hereinafter both together referred to as "parties" and each one separately as "party", based on the results of the procurement process No. 497018 "Licence (accompanied by system deployment service) for the data management platform necessary for the setting up and operation of the State Data Governance Information System" carried out by the public authority CPO LT in the form of an open tender (hereinafter – purchase) have entered into the following purchase Contract (hereinafter – Contract):

1. SUBJECT OF THE CONTRACT

1.1. The Supplier shall supply to the Customer and set up for operation the licence (hereinafter – the goods) of the data management platform necessary for the setting up and operation of the State Data Governance Information System within such scope and under such conditions as laid out in the Contract's annex titled "Technical Specification" (hereinafter – technical specification), while the Customer shall carry out the payment to the Supplier in accordance with the terms and conditions laid out in chapter 3 of the Contract.

2. RIGHTS AND RESPONSIBILITIES OF THE PARTIES

2.1. The Supplier shall:

2.1.1. supply the goods in a suitable and timely manner so that they suit the requirements laid out in the Contract and in the technical specification:

2.1.1.1. the data management platform shall be installed within 1 (one) month (i.e., 31 calendar days) starting from the signature date of the Contract;

2.1.1.2. the migration of the COVID-19 information system's solutions of data acquisition, transformation and visualisation of the implemented data shall be carried out within 1 (one) month (i.e., 31 calendar days) starting from the signature date of the purchase Contract;

2.1.1.3. the acquisition of data from the interdepartmental data storage and from the Integrated Statistical Information Systems' data sources shall be implemented within 9 (nine) months starting from the signature date of the purchase Contract;

2.1.1.4. the data management platform's licence shall remain valid for no less than 12 (twelve) months after the date on which the Supplier fulfils its obligation laid out in paragraph 2.1.1.1 of the Contract.

2.1.1.5. the data management platform support and provision of the required infrastructure services shall be ensured for no less than 12 (twelve) months after the date on which the Supplier fulfils its obligation laid out in paragraph 2.1.1.1 of the Contract;

2.1.1.6. training of up to 10 specialists of the Customer (up to 2 system and data administrators and up to 8 data analysts) shall be carried out and detailed training material for platform administrators and users shall be provided;

2.1.2. by carrying out its contractual obligations, maintain confidentiality and not disclose (in spoken, written or any other form) to any third parties the confidential information concerning the material, financial or any other aspects which have been introduced to it or which it could access or find out while collaborating with the Customer;

2.1.3. immediately notify the Customer, in the manner laid out in the Contract, about any circumstances that might prevent it from carrying out its contractual obligations in a proper and timely way;

2.1.4. if the person responsible for carrying out the purchase Contract and/or his or her contact information is changed, notify the Customer or its authorised person about it within 5 (five) business days.

2.2. Šalys susitaria, kad Sutarties 2.1.1 punkte nustatyti Tiekėjo įsipareigojimai yra esminė Sutarties sąlyga.
2.3. Tiekėjas turi kitas Sutarties bei Lietuvos Respublikos galiojančių teisės aktų nustatytas pareigas ir teises.
2.4. Užsakovas įsipareigoja:
2.4.1. užtikrinti visokeriopą, operatyvų bendradarbiavimą su Tiekėju, būtiną Sutarčiai tinkamai ir laiku įvykdyti;
2.4.2. priimti tinkamai ir laiku pristatytas (atitinkančias Sutartyje ir Techninėje specifikacijoje nustatytus reikalavimus) prekes ir sumokėti Tiekėjui už tinkamai ir laiku pristatytas prekes Sutartyje nustatytomis sąlygomis ir tvarka;
2.4.3. pasikeitus Užsakovo atstovui, atsakingam už pirkimo sutarties vykdymą ir (ar) jo kontaktams, nedelsiant, bet ne vėliau kaip per 5 (penkias) darbo dienas nuo minėto pasikeitimo dienos informuoti Tiekėją apie pasikeitimus.
2.5. Užsakovas turi teisę tikrinti prekių tiekimo procesą tiek, kiek tai susiję su prekių tiekimu, pareikšti Tiekėjui pastabas ir pasiūlymus dėl prekių tiekimo. Užsakovo pastebėti trūkumai fiksuojami raštu arba el. paštu ir turi būti Tiekėjo sąskaita ištaisyti per Užsakovo nurodytą terminą.
2.6. Užsakovas turi kitas Sutarties bei Lietuvos Respublikos galiojančių teisės aktų nustatytas pareigas ir teises.
2.7. Šalys susitaria, kad Sutarties 2.4.2 punkte nustatytas Užsakovo įsipareigojimas yra esminė Sutarties sąlyga.

2.2. The parties agree that the obligations for the Supplier set forth in paragraph 2.1.1 of the Contract are an essential part of the conditions of the Contract.
2.3. The Supplier is also subject to other rights and obligations set forth in the Contract as well as in laws and regulations effective in the Republic of Lithuania.
2.4. The Customer shall:
2.4.1. ensure an all-encompassing and responsive cooperation with the Supplier, as necessary for the suitable and timely implementation of the Contract;
2.4.2. accept the goods as they are supplied in a suitable and timely manner (i.e., fulfilling the requirements set forth in the Contract and in the technical specification) and make the payment, by following the conditions and procedures laid out in the Contract, for the goods supplied in a suitable and timely manner;
2.4.3. if the person the Customer has designated as responsible for the purchase Contract and/or his or her contact information is changed, notify the Supplier about this change without undue delay but no later than within 5 (five) business days.
2.5. The Customer is entitled to inspect the process of supplying the goods to such extent as it is related to the supplying of the goods and to express its remarks and recommendations to the Supplier concerning the supplying of the goods. The defects observed by the Customer shall be documented in writing or by email, and they shall be rectified by using the Supplier's own resources within the deadline indicated by the Customer.
2.6. The Customer is also subject to other rights and obligations set forth in the Contract as well as in laws and regulations effective in the Republic of Lithuania.
2.7. The parties agree that the obligation for the Customer set forth in paragraph 2.4.2 of the Contract is an essential part of the conditions of the Contract.

3. SUTARTIES KAINA IR ATSISKAITYMO TVARKA

3.1. Vadovaujantis Kainodaros taisyklių nustatymo metodikos, patvirtintos 2017 m. birželio 28 d. Viešųjų pirkimų tarnybos direktoriaus įsakymu Nr. 1S-95 „Dėl kainodaros taisyklių nustatymo metodikos patvirtinimo" (toliau – Metodika), 10.1 ir 11 punktais, Sutarčiai taikoma fiksuotos kainos kainodara.
3.2. Sutarties kaina už Sutarties 1.1 punkte nurodytas prekes ir paslaugas:

Pirkimo objektas	Kaina Eur be PVM	Kaina Eur su PVM
Duomenų valdymo platformos licencija kartu su infrastruktūros paslaugomis	2 100 000,00	2 541 000,00
Pirkimo objektas	**Kaina Eur be PVM**	**Kaina Eur su PVM**
Duomenų valdymo platformos diegimo paslauga	600 000,00	726 000,00
Iš viso	**2700 000,00**	**3 267 000,00**

Į Sutarties kainą įskaičiuoti visi Tiekėjo mokami mokesčiai ir rinkliavos bei kitos išlaidos. Tiekėjas neturi teisės reikalauti padengti jokių išlaidų, viršijančių Sutarties kainą.
3.3. Sutarties 2.1.1.1–2.1.1.3 punktuose nustatytų Tiekėjo įsipareigojimų įvykdymas yra įforminamas Šalims pasirašant perdavimo–priėmimo aktą, kuriuo Užsakovas patvirtina, kad Tiekėjo įsipareigojimai įvykdyti tinkamai. Tiekėjas pateikia Užsakovui sąskaitą faktūrą ne anksčiau nei Užsakovas pasirašo perdavimo–priėmimo aktą.
3.4. Užsakovas sumoka Sutarties 3.2 punkte nurodytą kainą už duomenų valdymo platformos licenciją kartu su infrastruktūros paslaugomis Tiekėjui tinkamai įvykdžius Sutarties 2.1.1.1 ir 2.1.1.2 punktuose nustatytus įsipareigojimus ir Šalims pasirašius perdavimo–priėmimo aktą ne vėliau kaip per 30 (trisdešimt) kalendorinių dienų nuo sąskaitos faktūros gavimo iš Tiekėjo dienos.

3. CONTRACT PRICE AND PAYMENT PROCEDURES

3.1. In accordance with the Methodology for Determining of Pricing Rules, as authorised by the 28th of June 2017 decree 1S-95 of the director of the Public Procurement Service "Concerning the approval of the Methodology for Determining of Pricing Rules" (hereinafter – the methodology), specifically its sections 10.1 and 11, this Contract is subject to the rule of fixed price formulation.
3.2. The contract price for the goods specified in section 1.1 of the Contract:

Subject of the procurement procedure	Price in euros, VAT excluded	Price in euros, VAT included
Data management platform's licence accompanied with infrastructure-related services	2,100,000.00	2,541,000.00
Subject of the procurement procedure	**Price in euros, VAT excluded**	**Price in euros, VAT included**
Data management platform's deployment service	600,000.00	726,000.00
Total	**2,700,000.00**	**3,267,000.00**

The contract price includes all taxes, fees and other expenses to be paid or incurred by the Supplier. The Supplier may not require a compensation for any expense that surpasses the contract price.
3.3. The completion of the Supplier's obligations set forth in paragraphs 2.1.1.1 to 2.1.1.3 of the Contract shall be documented by the parties signing the commissioning/acceptance protocol, by which the Customer affirms that the Supplier's obligations have been properly fulfilled. The Supplier shall issue its invoice to the Customer only after the Customer has signed the commissioning/acceptance protocol.
3.4. The Customer shall pay the price set forth in section 3.2 of the Contract for the data management platform's licence accompanied with infrastructure-related services upon the Supplier's proper fulfilment of its obligations set forth in paragraphs 2.1.1.1 and 2.1.1.2 of the Contract and upon the parties having signed the commissioning/acceptance protocol, within 30 (thirty) calendar days after the date of reception of the invoice from the Supplier.

3.5. kainą už duomenų valdymo platformos diegimo paslaugą Tiekėjui tinkamai įvykdžius Sutarties 2.1.1.3 punkte nustatytus įsipareigojimus ne vėliau kaip per 30 (trisdešimt) kalendorinių dienų nuo sąskaitos faktūros gavimo iš Tiekėjo dienos.
3.6. Sumokėjimo diena – tai diena, kai lėšos išskaitomos iš Užsakovo sąskaitos. Vykdant Sutartį, sąskaitos faktūros teikiamos tik elektroniniu būdu. Elektroninės sąskaitos faktūros, atitinkančios Europos elektroninių sąskaitų faktūrų standartą, kurio nuoroda paskelbta 2017 m. spalio 16 d. Komisijos įgyvendinimo sprendime (ES) 2017/1870 dėl nuorodos į Europos elektroninių sąskaitų faktūrų standartą ir sintaksių sąrašo paskelbimo pagal Europos Parlamento ir Tarybos direktyvą 2014/55/ES (OL 2017 L 266, p. 19) (toliau – Europos elektroninių sąskaitų faktūrų standartas), teikiamos Tiekėjo pasirinktomis priemonėmis. Europos elektroninių sąskaitų faktūrų standarto neatitinkančios elektroninės sąskaitos faktūros gali būti teikiamos tik naudojantis informacinės sistemos „E. sąskaita“ priemonėmis. Išlaidas, susijusias su atsiskaitymo dokumentų pateikimu per informacinę sistemą „E. sąskaita“, apmoka Tiekėjas.
3.7. Sutarties kaina nebus perskaičiuojama pagal bendrą kainų lygio kitimą, prekių grupių kainų pokyčius bei dėl mokesčių pasikeitimų.
3.8. Sutarčiai taikomas atvirkštinis apmokestinimas, t. y. pridėtinės vertės mokestį (PVM) į Lietuvos valstybės biudžetą sumoka Užsakovas, o Tiekėjui sumokama kaina be PVM.

4. SUTARTIES GALIOJIMAS

4.1. Sutartis įsigalioja ją pasirašius abiem Šalims ir galioja iki visiško Šalių įsipareigojimų įvykdymo.
4.2. Jei bet kuri Sutarties nuostata tampa ar pripažįstama visiškai ar iš dalies negaliojančia, tai neturi įtakos kitų Sutarties nuostatų galiojimui.
4.3. Sutarties sąlygos Sutarties galiojimo laikotarpiu gali būti keičiamos šios Sutarties ir Viešųjų pirkimų įstatyme nustatytais atvejais.
4.4. Sutarties keitimas galioja tik tuo atveju, jeigu jis yra sudaromas rašytiniu Sutarties šalių susitarimu. Šalių susitarimai dėl Sutarties keitimo tampa neatskiriama Sutarties dalimi.

5. NENUGALIMOS JĖGOS APLINKYBĖS

5.1. Šalis atleidžiama nuo atsakomybės už Sutarties neįvykdymą, jeigu ji įrodo, kad Sutartis neįvykdyta dėl aplinkybių, kurių ji negalėjo kontroliuoti bei protingai numatyti Sutarties sudarymo metu, ir kad negalėjo užkirsti kelio šių aplinkybių ar jų pasekmių atsiradimui (*force majeure*).
5.2. Šalis negalinti vykdyti pagal šią Sutartį savo įsipareigojimų dėl nenugalimos jėgos aplinkybių veikimo privalo raštu apie tai pranešti kitai Šaliai per 10 (dešimt) dienų nuo tokių aplinkybių atsiradimo pradžios.
5.3. Nenugalimos jėgos aplinkybėmis (*force majeure*) laikomos aplinkybės, nurodytos Lietuvos Respublikos civilinio kodekso (toliau – Civilinis kodeksas) 6.212 straipsnyje ir Atleidimo nuo atsakomybės esant nenugalimos jėgos (*force majeure*) aplinkybėms taisyklėse, patvirtintose Lietuvos Respublikos Vyriausybės 1996 m. liepos 15 d. nutarimu Nr. 840 „Dėl atleidimo nuo atsakomybės esant nenugalimos jėgos (*force majeure*) aplinkybėms taisyklių patvirtinimo“.

6. ŠALIŲ ATSAKOMYBĖ

6.1. Šalys atsako už tai, kad Sutarties sąlygos būtų tinkamai vykdomos.
6.2. Užsakovui laiku nesumokėjus Tiekėjui dėl Užsakovo kaltės, Tiekėjas turi teisę reikalauti 0,02 (dviejų šimtųjų) procento dydžio delspinigių už kiekvieną uždelstą kalendorinę dieną nuo vėluojamos sumokėti sumos.
6.3. Tiekėjas, neįvykdęs arba netinkamai įvykdęs savo sutartinius įsipareigojimus, nurodytus Sutarties 2.1.1.1–2.1.1.3 punktuose, sumoka Užsakovui 0,02 (dviejų šimtųjų) procento dydžio delspinigius už kiekvieną uždelstą kalendorinę dieną nuo Sutarties 3.2 punkte nurodytos duomenų valdymo platformos diegimo paslaugos kainos.

3.5. The Customer shall pay the price set forth in section 3.2 of the Contract for the data management platform's deployment service upon the Supplier's proper fulfilment of its obligations set forth in paragraph 2.1.1.3 of the Contract, within 30 (thirty) calendar days after the date of reception of the invoice from the Supplier.
3.6. The transaction date means the day when the funds are transferred from the Customer's bank account. For the purposes of this Contract, all invoices shall be submitted electronically. The electronic invoices that meet the requirements of the European standard of electronic invoices, as referenced in the 16th of October 2017 Commission Implementing Decision (EU) 2017/1870 on the publication of the reference of the European standard on electronic invoicing and the list of its syntaxes pursuant to Directive 2014/55/EU (OJ 2017 L 266, p. 19) (hereinafter – European standard of electronic invoices) shall be submitted by the means chosen by the Supplier. Electronic invoices that do not meet the European standard of electronic invoices can be submitted only by using the tools of the "E. sąskaita" information system. Expenses related to the submission of payment documents by using the "E. sąskaita" information system shall be paid by the Supplier.
3.7. The contracted price shall not be revised to reflect a general change in pricing level, scaling of prices of goods' groups or alterations in taxes.
3.8. The Contract is subject to reverse charge whereby the value added tax (VAT) is paid directly by the Customer to the relevant tax authorities, and the Supplier is paid the Price excluding VAT.

4. VALIDITY OF THE CONTRACT

4.1. The Contract shall take effect when both parties sign it and remains in effect until the obligations of the parties are fully implemented.
4.2. If any one of the conditions of the Contract is found to be invalid, it shall not alter the validity of other conditions of the Contract.
4.3. During the validity period of the Contract, the conditions of the Contract can only be amended in situations laid down in this Contract and the Law on Public Procurement.
4.4. An amendment of the Contract shall take effect only when carried out in writing by mutual accord of the parties. Such accords by the parties resulting in amendments become integral parts of the Contract.

5. FORCE MAJEURE

5.1. A contracting party shall be released from its responsibility for noncompletion of its contractual obligations if it can prove that the noncompletion of obligations resulted from circumstances that the party could not control or reasonably predict during the signing of the Contract and that it could not prevent these circumstances and their consequences from occurring (also called *force majeure*).
5.2. The party that finds itself unable to complete its obligations under this Contract because of the impact of *force majeure* circumstances shall notify the other party accordingly in writing within 10 (ten) days from the start of such circumstances.
5.3. For circumstances to be considered *force majeure*, they have to correspond to those set forth in Article 6.212 of the Lithuanian Civil Code (hereinafter – Civil Code) and the regulation "On circumstances enabling a release from obligations due to *force majeure*", approved by the Lithuanian Government's 15th of July 1996 decree No. 840 titled "Concerning the approval of the regulation on circumstances enabling a release from obligations due to *force majeure*".

6. RESPONSIBILITIES OF THE PARTIES

6.1. The parties shall be responsible for a proper fulfilment of the terms of this Contract.
6.2. Should the Customer fail to pay the Supplier, then the Supplier is entitled to demand a 0.02 (two hundredths) percent late fee, calculated from the actual arrears, for each calendar day the payment has been delayed.
6.3. The Supplier, upon failing to fulfil its contractual obligations set forth in paragraphs 2.1.1.1 to 2.1.1.3 of the Contract fully or fulfilling them improperly, shall pay the Customer a 0.02 (two hundredths) percent late fee, calculated from the data management platform's deployment service price set forth in section 3.2 of the Contract, for each calendar day of the actual delay.

6.4. Delspinigių sumokėjimas neatleidžia Šalių nuo prievolių pagal šią Sutartį tinkamo įvykdymo.
6.5. Užsakovas turi teisę vienašališkai išskaičiuoti delspinigius iš bet kokių Tiekėjui atliekamų mokėjimų.

7. SUBTIEKIMAS

7.1. Tiekėjas savo pasiūlyme nurodė, kad, vykdant Sutartį bus pasitelkiami subtiekėjai *(jei pasitelkiama)*: –.
Nurodytus subtiekėjus *(jei jie nurodyti)* galima keisti tik raštu informavus apie tai Užsakovą nurodant pagrįstas keitimo priežastis ir gavus raštišką Užsakovo sutikimą. Naujai siūlomas subtiekėjas turi atitikti pirkimo sąlygose keičiamam subtiekėjui numatytus reikalavimus. Tiekėjas bet kokiu atveju atsako už visus pagal Sutartį prisiimtus įsipareigojimus, nepaisant to, ar jiems vykdyti bus pasitelkiami subtiekėjai. Pagrįstomis subtiekėjo keitimo priežastimis laikomos priežastys, kai tiekėjo pasiūlytas subtiekėjas dėl objektyvių priežasčių (subtiekėjui bankrutavus ar susidarius analogiškai situacijai, nutrūkus teisiniams santykiams su tiekėju, subtiekėjui atsisakius tiekti Prekes ir pan.) nebegali suteikti visų ar dalies Sutartyje nurodytų Prekių. Užsakovui sutikus su subtiekėjo pakeitimu, Užsakovas kartu su Tiekėju raštu sudaro susitarimą dėl subtiekėjo pakeitimo. Šis susitarimas yra neatskiriama Sutarties dalis. Subtiekėjo keitimo tvarkos pažeidimas laikomas esminiu Sutarties pažeidimu.
7.2. Sudarius Sutartį, tačiau ne vėliau negu Sutartis pradedama vykdyti, Tiekėjas įsipareigoja Užsakovui raštu pranešti tuo metu žinomų subtiekėjų pavadinimus, kontaktinius duomenis ir jų atstovus. Tiekėjas taip pat įsipareigoja Užsakovui raštu pranešti apie minėtos informacijos pasikeitimus visu Sutarties vykdymo metu, taip pat apie naujus subtiekėjus, kuriuos Tiekėjas ketina pasitelkti vėliau.
7.3. Užsakovas ne vėliau kaip per 3 (tris) darbo dienas nuo Sutarties 7.2 papunktyje nurodytos informacijos gavimo dienos informuoja subtiekėjus apie tiesioginio atsiskaitymo galimybę. Subtiekėjas, norėdamas pasinaudoti tiesioginio atsiskaitymo galimybe, per 5 (penkias) darbo dienas nuo Užsakovo informavimo apie tiesioginio atsiskaitymo galimybę, Užsakovui pateikia prašymą raštu.
7.4. Subtiekėjui pateikus Užsakovui prašymą pasinaudoti tiesioginio atsiskaitymo galimybe, tarp Užsakovo, Sutartį sudariusio Tiekėjo ir jo subtiekėjo yra sudaroma trišalė sutartis, kurioje aprašoma tiesioginio atsiskaitymo su subtiekėju tvarka ir numatoma teisė Tiekėjui prieštarauti nepagrįstiems mokėjimams subtiekėjui.

8. GINČŲ SPRENDIMO TVARKA

8.1. Dėl Sutarties kylantys ginčai sprendžiami derybų būdu, o per 30 (trisdešimt) kalendorinių dienų nuo derybų pradžios nepavykus išspręsti ginčo derybų būdu, ginčas bus sprendžiamas Civilinio proceso kodekso nustatyta tvarka Lietuvos Respublikos teismuose.

9. SUTARTIES NUTRAUKIMO TVARKA

9.1. Sutartis gali būti nutraukta:
9.1.1. rašytiniu Šalių susitarimu;
9.1.2. Sutartyje nustatytais atvejais ir tvarka;
9.1.3. kitais Civilinio kodekso nustatytais atvejais.
9.2. Užsakovas, nesikreipdamas į teismą, gali vienašališkai nutraukti Sutartį, raštu įspėjęs Tiekėją prieš 15 (penkiolika) kalendorinių dienų, jeigu:
9.2.1. Tiekėjui iškeliama restruktūrizavimo arba bankroto byla, Tiekėjas likviduojamas, sustabdo savo ūkinę veiklą arba kai įstatymuose ar kituose teisės aktuose nustatyta tvarka susidaro analogiška situacija;
9.2.2. esant esminiam Sutarties pažeidimui;

6.4. Paying the late fees does not release the parties from the proper fulfilling of the responsibilities set forth in this Contract.
6.5. The Customer is entitled to unilaterally withhold late fees from any payments to be made toward the Supplier.

7. SUBCONTRACTING

7.1. The Supplier in its bid indicates that, for the purpose of this Contract, subcontractors will be involved (*in the case of subcontracting*): –. The specified subcontractors (*in the case they are indicated*) can only be changed after notifying the Customer in writing, substantiating the reasons for such change and obtaining the Customer's written approval. A newly appointed subcontractor shall meet the requirements set forth in relation to subcontractors in the procurement conditions. The Supplier, in every situation, shall be responsible for all responsibilities undertaken in relation to this Contract, regardless of whether or not subcontractors have been involved for carrying it out. Among substantial reasons for changing the subcontractor shall be considered such reasons as the Supplier's appointed subcontractor becoming unable to deliver partially or fully the goods specified in the Contract because of objective circumstances (bankruptcy of the subcontractor or a similar situation; termination of the legal relationship with the Supplier; subcontractor's refusal to deliver the goods; etc.). Upon the Customer's approval of the change of subcontractor, the Customer and the Supplier shall jointly draw up a written accord concerning the change of subcontractor. The accord shall become an integral part of this Contract. A violation of the procedure of change of subcontractor shall be considered an essential violation of the Contract.
7.2. Upon entering into the Contract, but no later than the date the Contract comes into effect, the Supplier shall inform the Customer in writing about the names, contact details and representatives of the subcontractors known at that point. The Supplier shall also, during the entire validity period of the Contract, inform the Customer in writing in the case the above information changes as well as in the case of an intended later involvement of new subcontractors by the Supplier.
7.3. The Customer shall within 3 (three) business days from the information reception date set forth in the subsection 7.2 of the Contract inform the subcontractors concerning the possibility of direct reporting. Should a subcontractor wish to make use of the direct reporting method, it shall within 5 (five) business days from the date the Customer notified it about the direct reporting possibility, file a written application with the Customer.
7.4. Upon the subcontractor's filing of an application with the Customer concerning the use of direct reporting, the Customer, the contracting Supplier and its subcontractor shall jointly draw up a tripartite accord detailing the procedure of direct reporting to be used with the subcontractor and providing the right to the Supplier to object against unsubstantiated payments toward the subcontractor.

8. PROCEDURE FOR RESOLUTION OF DISPUTES

8.1. Disputes arising in connection with the Contract shall be resolved by negotiation and, if a dispute remains unresolved 30 (thirty) calendar days after the start of such negotiations, the dispute shall be handled by Lithuanian courts of law in accordance with the procedures stipulated in the Civil Process Code.

9. PROCEDURE FOR TERMINATING THE CONTRACT

9.1. This Contract can be terminated:
9.1.1. by the parties agreeing in writing;
9.1.2. in the situations and by the procedures set forth in the Contract;
9.1.3. in other situations as provided for in the Civil Code.
9.2. The Customer is entitled, without turning to a court of law, to unilaterally terminate the Contract by alerting the Supplier in writing 15 (fifteen) calendar days in advance, if:
9.2.1. the Supplier becomes the subject of restructuring or bankruptcy, the Supplier is being dissolved, has suspended its business activity or a similar situation has arisen in accordance with the procedures set forth by laws or other relevant legal acts;
9.2.2. there exists a substantial violation of the Contract;

9.2.3. Sutartis buvo pakeista pažeidžiant Lietuvos Respublikos viešųjų pirkimų įstatymo (toliau – Viešųjų pirkimų įstatymas) 89 straipsnį;
9.2.4. paaiškėjo, kad Tiekėjas, su kuriuo sudaryta Sutartis, turėjo būti pašalintas iš pirkimo procedūros pagal Viešųjų pirkimų įstatymo 46 straipsnio 1 dalį;
9.2.5. paaiškėjo, kad su Tiekėju neturėjo būti sudaryta Sutartis dėl to, kad Europos Sąjungos Teisingumo Teismas procese pagal Sutarties dėl Europos Sąjungos veikimo 258 straipsnį pripažino, kad nebuvo įvykdyti įsipareigojimai pagal Europos Sąjungos steigiamąsias sutartis ir Direktyvą 2014/24/ES.
9.3. Tiekėjas, nesikreipdamas į teismą, gali vienašališkai nutraukti Sutartį, raštu įspėjęs Užsakovą prieš 15 (penkiolika) kalendorinių dienų, jeigu Užsakovas padaro esminį Sutarties pažeidimą.

10. KITOS SĄLYGOS

10.1. Sutarčiai ir visoms iš šios Sutarties atsirandančioms teisėms ir pareigoms taikomi Lietuvos Respublikos įstatymai bei kiti norminiai teisės aktai. Sutartis sudaryta ir turi būti aiškinama pagal Lietuvos Respublikos teisę.
10.2. Sutartis gali būti keičiama tik Viešųjų pirkimų įstatymo 89 straipsnyje nustatyta tvarka. Sutarties sąlygų pakeitimai įforminami Šalių rašytiniais susitarimais, kurie yra neatsiejama Sutarties dalis.
10.3. Jeigu Tiekėjo kvalifikacija dėl teisės verstis atitinkama veikla nebuvo tikrinama arba tikrinama ne visa apimtimi, Tiekėjas Užsakovui įsipareigoja, kad Sutartį vykdys tik tokią teisę turintys asmenys.
10.4. Vykdydamos Sutartį Šalys įsipareigoja asmens duomenų tvarkymą vykdyti teisėtai – laikydamosi 2016 m. balandžio 27 d. priimto Europos Parlamento ir Tarybos reglamento (ES) 2016/679 dėl fizinių asmenų apsaugos ir kitų teisės aktų, reglamentuojančių asmens duomenų tvarkymą. Šalių atstovų, darbuotojų ar kitų fizinių asmenų duomenų tvarkymo teisėtumas grindžiamas būtinybe įvykdyti Sutartį. Šalys įsipareigoja tinkamai informuoti visus fizinius asmenis (darbuotojus, savo subtiekėjų darbuotojus ir kitus atstovus), kurie bus pasitelkti Sutarčiai vykdyti, apie tai, kad jų asmens duomenys bus Šalių tvarkomi Sutarties vykdymo tikslais. Šalys pažymi, kad fiziniai asmenys, kurie yra pasitelkti Sutarčiai su Šalimis vykdyti ir išvardinti Sutartyje, yra supažindinti su Sutartyje pateiktais jų asmeniniais duomenimis, ir Šalies nustatyta tvarka tam davė savo sutikimą.
10.5. Tiekėjo ir Užsakovo vienas kitam siunčiami pranešimai turi būti raštiški. Pranešimai turi būti siunčiami paštu ar elektroniniu paštu Sutartyje Šalių nurodytais adresais.
10.6. Užsakovo paskirtas už Sutarties vykdymą atsakingas asmuo – Lietuvos statistikos departamento Sklaidos ir komunikacijos skyriaus

10.7. Asmuo atsakingas už tai, kad Sutartis ir jos pakeitimai būtų paskelbti Lietuvos Respublikos viešųjų pirkimų įstatyme nustatyta tvarka: Viešosios įstaigos CPO LT Biuro ir veiklos aptarnavimo srities pirkimų skyriaus

10.8. Tiekėjo paskirtas už Sutarties vykdymą asmuo

10.9. Šalys įsipareigoja per 5 (penkias) kalendorines dienas pranešti viena kitai apie Sutarties 12 dalyje „Šalių adresai, rekvizitai ir parašai“ nurodytų duomenų pasikeitimą. Šalis, laiku nepranešusi apie šių duomenų pakeitimus, negali reikšti pretenzijų dėl kitos Šalies veiksmų, atliktų vadovaujantis šioje Sutartyje pateiktais duomenimis.

9.2.3. the Contract has been amended in such a way that violates Article 89 of the Lithuanian Law on Public Procurement (hereinafter – Law on Public Procurement);
9.2.4. it has been found that the Supplier that has entered into Contract should have been excluded from the procurement procedure for reasons given in the part 1 of Article 46 of the Law on Public Procurement;
9.2.5. it has been found that an Contract with the Supplier should not have been entered into because, in a procedure carried out by the European Union's Court of Justice and following the Article 258 of the Contract on the functioning of the European Union, it is recognised that the responsibilities set forth in the European Union's foundational Contracts and in the Directive 2014/24/EU have not been fulfilled.
9.3. The Supplier is entitled, without turning to a court of law, to unilaterally terminate the Contract by alerting the Customer in writing 15 (fifteen) calendar days in advance, if the Customer has substantially violated the Contract.

10. MISCELLANEOUS CONDITIONS

10.1. This Contract including all rights and responsibilities arising from it are subject to the laws of the Republic of Lithuania and other regulatory legal acts. The Contract has been entered into and shall be interpreted in accordance with the laws of the Republic of Lithuania.
10.2. This Contract can only be amended by the procedure set forth in Article 89 of the Law on Public Procurement. Any amendments to the terms and conditions of the Contract shall be made by written accord, which shall become integral parts of the Contract.
10.3. In the case if the Supplier's qualification as regards the right to carry out the corresponding activity has not been verified or has been verified incompletely, the Supplier shall take it upon itself before the Customer that the Contract's fulfilment is carried out only by persons having the relevant rights.
10.4. While fulfilling the Contract, the parties shall carry out the processing of personal data in a legally conforming way, namely, by applying the European Parliament and Council Regulation (EU) 2016/679 of the 27th April 2016 concerning the protection of individuals as well as other relevant legal acts applicable to the processing of personal data. The legality of processing the personal data of the representatives and employees of the parties as well as of other individuals shall be based on the need to implement this Contract. The parties undertake to notify, in an appropriate manner, all the individuals (employees, employees of their subcontractors and other representatives) involved in the fulfilment of this Contract that the parties will process their personal data for the purpose of implementing this Contract. The parties assert that the individuals involved in the fulfilment of the Contract between the parties and named in the Contract have been informed as to which of their personal data have been included in the Contract and that they have expressed their acceptance of it, as set forth by the party.
10.5. The communications between the Supplier and the Customer shall be carried out in writing. The messages shall be sent either by post or by electronic mail to the addresses the parties have included in the Contract.
10.6. The Customer has designated the following person as responsible for the implementation of the Contract:

10.7. The person responsible for the announcing of the Contract and its amendments in accordance with the procedures set forth by the Law on Public Procurement:

10.8. The Supplier has designated the following person as responsible for the implementation of the Contract:

10.9. Should the details included in section 12 of the Contract "Addresses, details and signatures of the parties" change, the parties shall inform one another to that effect within 5 (five) calendar days. A party that has failed to notify such change of details is not entitled to object against the actions of the other party that have been carried out by using the details included in this Contract.

10.10. Sutartis sudaryta dviem egzemplioriais, turinčiais vienodą teisinę galią, po vieną kiekvienai Šaliai. Jei yra neatitikimų ar nesutapimų tarp anglų ir lietuvių kalbos teksto, vadovaujamasi Sutarties tekstu anglų kalba.

10.11. Sutarties priedai yra neatskiriama Sutarties dalis.

10.10. The Contract is drawn up in duplicate in English and Lithuanian language (one for each Party), each having equal legal force. In the event of inconsistency or discrepancy between the English version and Lithuanian version of this Contract, the English version shall prevail.

10.11. The annex of the Contract titled "Technical specification" is an integral part of the Contract.

11. SUTARTIES PRIEDAI

11.1. Sutarties 1 priedas: Duomenų valdymo platformos, reikalingos Valstybės duomenų valdysenos informacinei sistemai įgalinti ir veikti, licencijos, įskaitant platformos diegimą, pirkimo techninė specifikacija.

11.2. Sutarties 2 priedas: Asmens duomenų ir informacijos tvarkymas.

11. ANNEX

11.1. Annex 1: Technical specification for the licence (accompanied by system deployment service) for the data management platform necessary for the setting up and operation of the State Data Governance Information System.

11.2. Annex 2: Processing of personal data and information.

12. ŠALIŲ ADRESAI, REKVIZITAI IR PARAŠAI

UŽSAKOVAS

Lietuvos statistikos departamentas
Gedimino pr. 29, LT-01500 Vilnius
Įmonės kodas: 188600177
PVM mokėtojo kodas: nėra
A. s. Nr. LT51 7044 0600 0111 1285
AB SEB BANKAS
Banko kodas 70440
Tel. +370 5 236 4822
El. p. info@stat.gov.lt
http://www.stat.gov.lt

Generalinė direktorė Jūratė Petrauskienė

TIEKĖJAS

Palantir Technologies UK, Ltd.
New Penderel House
283-288 High Holborn
London, WC1V 7HP
Įmonės kodas: 7042994
PVM mokėtojo kodas: GB 101 2291 78
Bankas: JP Morgan Chase
Sąskaitos savininkas: Palantir Technologies UK, Ltd.
A. s. Nr.: 41036031
IBAN: GB36CHAS60924241036031
SWIFT: CHASGB2L
Tel. +44 7408 886228
El. p. legalnotices@palantir.com

Matt Long, įgaliotasis asmuo

12. ADDRESSES, DETAILS AND SIGNATURES OF THE PARTIES

CUSTOMER

The Lithuanian Department of Statistics (Statistics Lithuania)
Gedimino Ave. 29, LT-01500 Vilnius, Lithuania
Company code: 188600177
VAT number: none
Settlement Account No: LT51 7044 0600 0111 1285
AB SEB BANKAS
Bank code: 70440
Tel.: +370 5 236 4822
E-mail: info@stat.gov.lt
http://www.stat.gov.lt

Jūratė Petrauskienė, Director General

SUPPLIER

Palantir Technologies UK, Ltd.
New Penderel House
283-288 High Holborn
London, WC1V 7HP
Company number: 7042994
VAT number: GB 101 2291 78
Bank Name: JP Morgan Chase
Account Holder: Palantir Technologies UK, Ltd.
Account Number: 41036031
IBAN: GB36CHAS60924241036031
SWIFT: CHASGB2L
Phone No. +44 7408 886228
E-mail: legalnotices@palantir.com

Matt Long, Authorised Signatory

Duomenų valdymo platformos, reikalingos Valstybės duomenų valdysenos informacinei sistemai įgalinti ir veikti, licencijos, įskaitant platformos diegimą, pirkimo sutarties Nr. STAT-(2020)
1 priedas

License (accompanied by system deployment service) for the data management platform necessary for setting up and operation of the State Data Governance Information System, purchase Contract No STAT-(2020)
Annex 1

DUOMENŲ VALDYMO PLATFORMOS, REIKALINGOS VALSTYBĖS DUOMENŲ VALDYSENOS INFORMACINEI SISTEMAI ĮGALINTI IR VEIKTI, LICENCIJOS, ĮSKAITANT PLATFORMOS DIEGIMĄ, PIRKIMO TECHNINĖ SPECIFIKACIJA

TECHNICAL SPECIFICATION FOR THE PURCHASE OF THE LICENSE (ACCOMPANIED BY SYSTEM DEPLOYMENT SERVICE) FOR THE DATA MANAGEMENT PLATFORM NECESSARY FOR SETTING UP AND OPERATION OF THE STATE DATA GOVERNANCE INFORMATION SYSTEM

TURINYS

CONTENS

1. Sąvokos ir sutrumpinimai

Santrumpa/ sąvoka	Paaiškinimas
API	Integracinė sąsaja / aplikacijų programavimo sąsaja (angl. *Application Programming Interface*)
DVP, platforma	Duomenų valdymo platforma, apimanti duomenų įsisavinimo, transformacijų, analizės ir vizualizavimo funkcijas
Duomenų įsisavinimas	Duomenų valdymo platformos funkcionalumas, apimantis duomenų paėmimo, išarchyvavimo, struktūrizavimo ir įvedimo į platformos duomenų bazę funkcijas
IS	Informacinė sistema
IT	Informacinės technologijos
Perkančioji organizacija / Užsakovas	Lietuvos statistikos departamentas
Prekės	Valstybės duomenų valdysenos informacinę sistemą įgalinančios duomenų valdymo platformos licencija, įskaitant platformos diegimą
Tiekėjas	Valstybės duomenų valdysenos informacinę sistemą įgalinančios duomenų valdymo platformos licencijos pardavėjas ir platformos diegėjas
VDV IS	Valstybės duomenų valdysenos informacinė sistema

1. Terms and abbreviations

Abbreviation/ Term	Explanation
API	Integration Interface / Application Programming Interface
DMP, Platform	Data Management Platform that includes data ingress, transformations, analysis, and visualisation functions
Data ingress	Data Management Platform functionality that includes the functions of data ingestion, extraction from archives, structuring, and entering into the database of the platform
IS	Information System
IT	Information Technology
Purchasing organisation / Ordering party	Lithuanian Department of Statistics
Item	A license of the Data Management Platform which will enable the State Data Governance Information System, including the installation of the platform
Supplier	The seller of the license of Data Management Platform which will enable State Data Governance Information System and the installer of the platform
SDM IS	State Data Governance Information System

2. Įvadinė informacija

Perkančioji organizacija – Lietuvos statistikos departamentas, juridinio asmens kodas – 188600177, adresas – Gedimino pr. 29, LT-01500 Vilnius, telefonas (8 5) 236 4800, elektroninio pašto adresas – info@stat.gov.lt.

Prekių pateikimo vieta – Lietuvos statistikos departamentas, Gedimino pr. 29, LT-01500 Vilnius.

Pirkimo objektas – kompleksinės programinės įrangos – duomenų valdymo platformos licencijos su ne mažiau kaip 1 (vienų) metų trukmės palaikymu įsigijimas. Pirkimo tikslas yra įsigyti kuriamos Valstybės duomenų valdysenos informacinės sistemos veikimui reikalingą duomenų valdymo platformą, įskaitant jos diegimo ir priežiūros paslaugas.

2.1. Vykdomo projekto tikslai ir uždaviniai

Lietuvos statistikos departamentas siekia perkamos duomenų valdymo platformos pagrindu sukurti Valstybės duomenų valdysenos informacinę sistemą (VDV IS), kuri sudarytų sąlygas greitai ir efektyviai gauti sprendimams priimti reikalingus duomenis ir atlikti jų analizę, atsižvelgiant į valstybės informacinius poreikius ir užtikrinant duomenų saugumą bei konfidencialumą.

VDV IS tikslas – sukurti lanksčią informacinę sistemą, kuri leistų operatyviai reaguoti į valstybės informacijos poreikius ir užtikrinti jų tenkinimą.

VDV IS uždaviniai:

- Gebėti greitai ir efektyviai įsisavinti bet kokio formato ir apimties duomenis.
- Užtikrinti lanksčias bet kokios apimties duomenų transformacijas, analizę ir vizualizavimą.
- Užtikrinti sistemos ir jos duomenų saugumą ir efektyvų naudotojų rolių ir teisių valdymą.

2. Introductory information

Purchasing organisation – Lithuanian Department of Statistics, company code 188600177, address – Gediminas ave. 29, LT-01500 Vilnius, telephone (8 5) 236 4800, email address – info@stat.gov.lt.

Location of the delivery of goods – Lithuanian Statistics Department, Gediminas ave. 29, LT-01500 Vilnius.

The subject of the purchase is the acquisition of a license for a complex piece of software (the Data Management Platform) with a support contract of at least one year. The purpose of the purchase is to acquire the Data Management Platform which is necessary for the operation of the State Data Governance Information System which is under development, including its installation and maintenance services.

2.1. Goals and objectives of the project

The Lithuanian Department of Statistics aims to create the State Data Governance Information System (SDM IS) on the basis of the Data Management Platform that is being purchased, which would allow to rapidly and efficiently obtain the data needed for decision-making and to perform its analysis, taking into account the information needs of the state and ensuring data security and confidentiality.

The goal of the SDM IS is to create a flexible information system which would allow to promptly respond to the information needs of the state and ensure that they are met.

The objectives of the SDM IS are:

- To be able to quickly and efficiently absorb data of any format and size.
- To be able to ensure flexible data transformations, analysis, and visualisations for data of any size.
- To be able to ensure the security of the system and its data, and the efficient management of user roles and rights.

2.2. Esama situacija

Valstybės informacinių išteklių fragmentacija. Šiuo metu Registrų ir valstybės informacinių sistemų registre yra registruoti 95 registrai ir 275 valstybės informacinės sistemos. Šiuos registrus ir informacines sistemas valdo 134 skirtingi valdytojai ir tvarko 166 pagrindiniai tvarkytojai. Tokia informacinių išteklių gausa ir įvairovė apsunkina duomenų gavimą, jungimą, analizę ir atvaizdavimą. Savo ruožtu tai apsunkina arba padaro neįmanomą valstybei ir visuomenei svarbių sprendimų pagrindimą aktualiais ir išsamiais duomenimis. Ypač tai tampa aktualu kilus vienokio ar kitokio pobūdžio krizei, pvz., COVID-19 pandemijai.

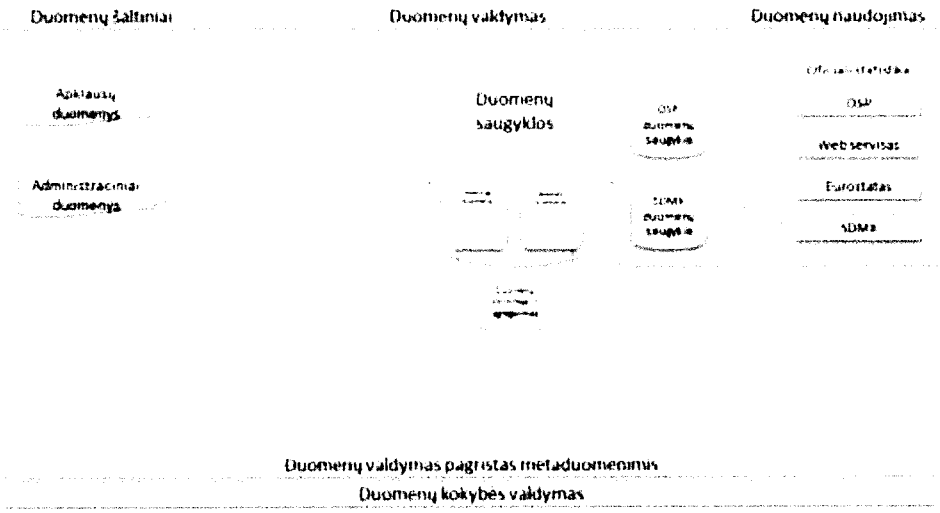
Lietuvos statistikos departamento vaidmuo tenkinant valstybės informacinius poreikius. Lietuvos statistikos departamentas valdo didžiausius valstybės ekonominės ir socialinės raidos duomenų išteklius, tačiau oficialiosios statistikos parengimo trukmė ir detalumas jau seniai atsilieka nuo skaitmeninės visuomenės informacinių poreikių gauti reikiamą informaciją „čia ir dabar“. Lietuvos statistikos departamento metodologinė kompetencija tvarkant didelius duomenų srautus, valdant informacijos poreikius, turima Integruotos statistikos informacinė sistema, ryšiai ir patirtis dirbant su duomenų šaltiniais, taip pat turimas žmogiškųjų išteklių potencialas leistų imtis lyderystės kuriant efektyvią informacinę sistemą, pajėgiančią, atsižvelgiant į poreikius, surinkti, apdoroti, analizuoti ar pateikti analizei kitiems naudotojams maksimaliai aktualius ir detalius socialinės ir ekonominės raidos duomenis, tuo pat metu užtikrinant jų saugumą ir kokybę.

2.2. Current situation

Fragmentation of state information resources. Currently there are 95 registers and 275 state information systems registered in the Register of Registries and State Information Systems. These registries and information systems are governed by 134 different controllers and managed by 166 primary processors. This abundance and variety of information resources complicates data retrieval, merging, analysis, and visualisation. This, in turn, complicates or makes it impossible to justify the decisions relevant to the state and society with relevant and comprehensive data. This is particularly true in the event of a crisis of one kind or another, such as the COVID-19 pandemic.

The role of the Lithuanian Department of Statistics in meeting the information needs of the state. The Lithuanian Department of Statistics manages the largest resources of state economic and social development data, but the duration and detail of the preparation of official statistics is long lagging behind the information needs of the digital society to obtain the necessary information "here and now". The methodological competence of the Lithuanian Department of Statistics in the management of large data flows, management of information needs, already available Integrated Statistics Information System, networking and experience in working with data sources, as well as the available human resources potential would allow to take leadership in the development of an efficient information system capable of, according to the needs, collecting, processing, analysing, or providing to other users, the most relevant and detailed data on socio-economic development, while ensuring their safety and quality.

1 pav. Apibendrinta esamos situacijos schema
Figure 1. The summarised scheme of the current situation



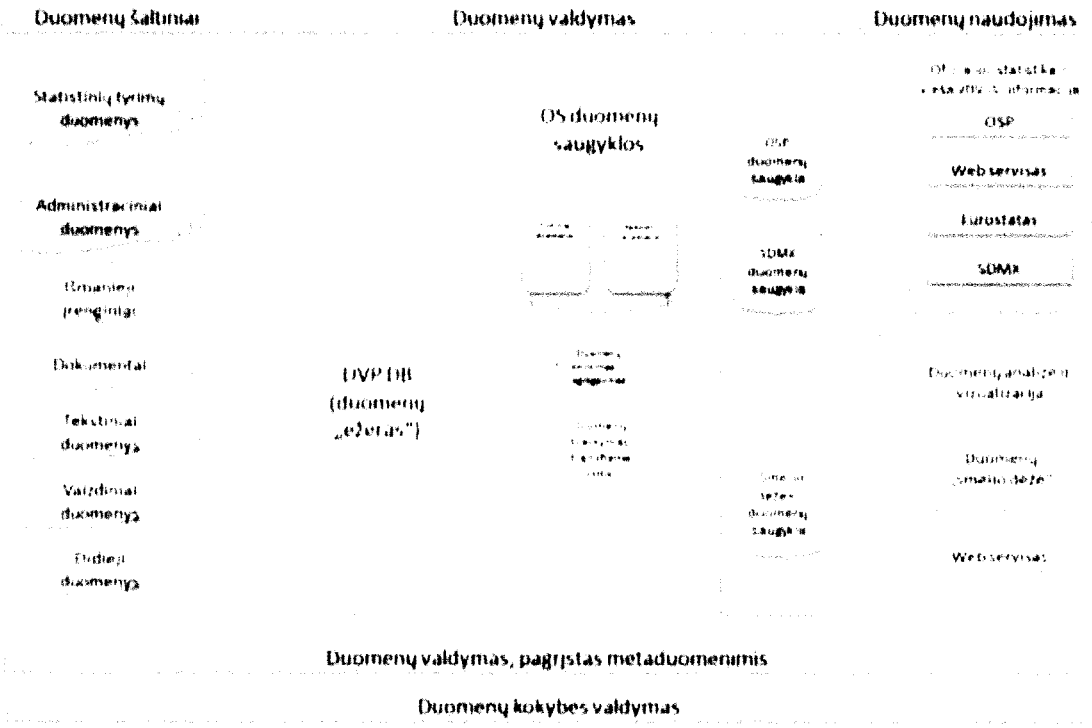
2.3. Siekiama situacija

Įsigijus duomenų valdymo platformą, siekiama Integruotą statistikos informacinės sistemos, perkeliant duomenų įsisavinimo procesą iš visų duomenų šaltinių, išskyrus statistinių tyrimų metu surinktus duomenis, kurie naudojami vadovaujantis Europos Parlamento ir Tarybos reglamentu (EB) Nr. 223/2009 dėl Europos statistikos, panaikinantis Europos Parlamento ir Tarybos reglamentą (EB, Euratomas) Nr. 1101/2008 dėl konfidencialių statistinių duomenų perdavimo Europos Bendrijų statistikos tarnybai, Tarybos reglamentą (EB) Nr. 322/97 dėl Bendrijos statistikos ir Tarybos sprendimą 89/382/EEB, Euratomas, įsteigiantį Europos Bendrijų statistikos programų komitetą, taip pat COVID-19 stebėsenos informacinės sistemos, tarpžinybinės duomenų saugyklos ir kitų valstybės informacinių sistemų duomenų pagrindu sukurti Valstybės duomenų valdysenos sistemą, gebančią operatyviai ir lanksčiai reaguoti į valstybės informacijos poreikį.

2.3. Expected situation

With the acquisition of the Data Management Platform, the aim is to have an integrated statistical information system by transferring the data uptake process from all data sources, with the exception of data collected during statistical surveys, which are used in accordance with the Regulation of the European Parliament and Council (EC) No. 223/2009 on European statistics which revokes Regulation of the European Parliament and Council (EC, Euratom) No. 1101/2006 on the transmission of data subject to statistical confidentiality to the Statistical Office of the European Communities, Council Regulation (EC) No 322/97 on Community statistics and Council Decision 89/382/EEC, Euratom, establishing a Committee on the Statistical Programmes of the European Communities, and also to create a State Data Governance Information System based on the data of the COVID-19 monitoring information system, interdepartmental data repository and other state information systems, that would be capable of responding promptly and flexibly to the state information needs.

2 pav. Apibendrinta siekiamos sistemos schema
Figure 2. Generalised scheme of expected situation



3. Pirkimo objektas

Perkančioji organizacija ketina įsigyti Valstybės duomenų valdysenos informacinę sistemą įgalinančios duomenų valdymo platformos licenciją. Įsigyjama licencija apima platformos diegimą, 4.3 punkte įvardytų duomenų šaltinių integravimą, 4.5 punkte apibrėžtų mokymų paslaugas, ne mažiau kaip vienų metų duomenų valdymo platformos palaikymą ir reikiamų infrastruktūros paslaugų teikimą.

4. Reikalavimai duomenų valdymo platformai ir jos diegimui

Ši techninė specifikacija nustato techninius reikalavimus, keliamus programinei įrangai. Tiekėjas privalo atsižvelgti į šiuos reikalavimus ir siūlyti prekę, tenkinančią žemiau nurodytus reikalavimus.

Jeigu techninėje specifikacijoje panaudoti konkretūs prekių pavadinimai, kilmės šalys, standartai, technologijos, medžiagos ar pan., tiekėjai turi teisę siūlyti lygiavertes ar geresnių charakteristikų prekes.

3. The object of the purchase

The contracting organisation intends to acquire a license for a Data Management Platform which would enable the State Data Governance Information System. The license to be acquired includes the installation of the platform, the integration of the data sources mentioned in requirement 4.3, the training services defined in requirement 4.5, the maintenance of the Data Management Platform for at least one year, and the provision of the necessary infrastructure services.

4. Requirements for Data Management Platform and its installation

This technical specification sets the technical requirements for the software. The Supplier must take these requirements into account and offer a product that meets the requirements below.

Where specific product names, countries of origin, standards, technologies, materials, etc., are used within the technical specification, the Suppliers have the right to offer goods of equivalent or better characteristics.

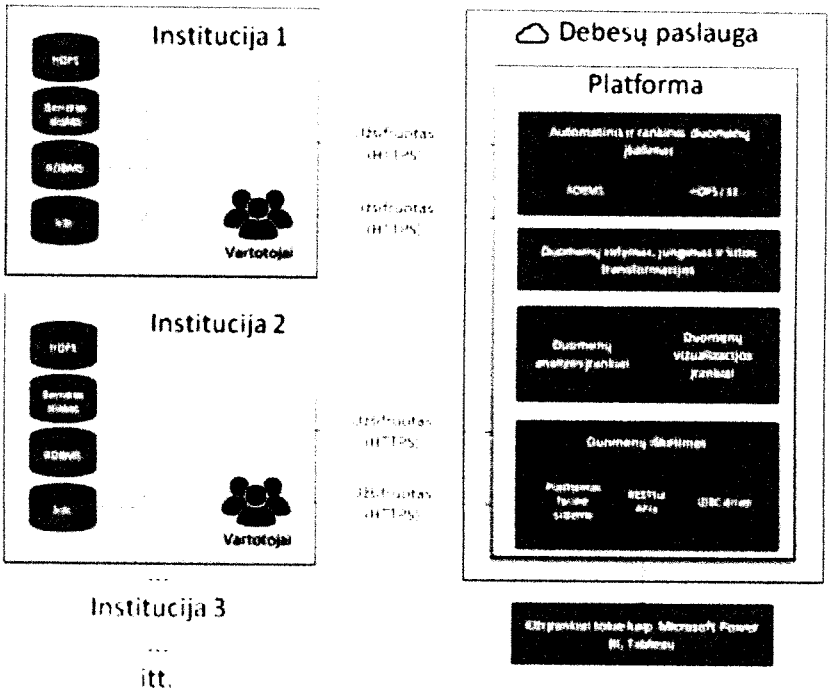
4.1. Reikalavimai duomenų valdymo platformos architektūrai

Reikalavimo Nr.	Reikalavimų detalizavimas
R1 Duomenų valdymo platforma turi būti sudaryta iš trijų susijusių sluoksnių, atsakingų už skirtingo funkcionalumo įgyvendinimą.	Duomenų valdymo platformą turi sudaryti šie sluoksniai: - duomenų sluoksnis, atsakingas už duomenų įsisavinimo iš duomenų šaltinių funkcionalumą ir apimantis jau parengtas jungtis įprastų tipų duomenims paimti ir atviras integracines sąsajas (API) sudėtingesniems duomenų paėmimo atvejams. Šis sluoksnis taip pat turi turėti praktiškai neribotos apimties duomenis ir naudotojų skaičiui pritaikytą saugyklą („duomenų ežerą“); - valdymo sluoksnis, atsakingas už duomenų tvarkymą, apdorojimą ir transformacijas, taip pat duomenų saugumo užtikrinimą bei duomenų perdavimą kitoms aplikacijoms; - analizės sluoksnis, atsakingas už duomenų analizės ir vizualizavimo funkcionalumą, leidžiantį naudotojams atlikti darbą su duomenimis, siekiant išsikeltų uždavinių.
R2 Platforma turi naudoti lengvai keičiamą ir plečiamą architektūrą.	Platforma turi veikti kaip ekosistema, prie kurios galima būtų pridėti naujas sistemas, funkcionalumus ar kitokius plėtinius Užsakovo poreikiams augant arba technologijoms keičiantis.
R3 Platforma turi įgalinti atitinkamas teises turinčius vartotojus platformos įrankiais kurti automatinius duomenų įkėlimo ir iškėlimo mechanizmus taip, kad skirtingų Lietuvos Respublikos valstybės ir (ar) savivaldybių institucijų, taip pat kitų šaltinių duomenys, esantys jų informacinėse sistemose, svetainėse ar kitur, galėtų būti naudojami kaip platformoje, taip ir už jos ribų.	
R4 Skirtingų institucijų darbuotojai, turintys atitinkamas teises, turi galėti naudojant paprastą vartotojo sąsają arba programavimo aplinką, rankiniu būdu įkelti duomenų rinkinius, sukurti automatinį duomenų įkėlimo mechanizmą, atlikti duomenų transformacijas, atlikti duomenų analizę, sukurti vizualizacijas ir rankiniu būdu iškelti duomenis arba sukurti automatizuotą duomenų iškėlimą į išorines savo pačių ar kitas informacines sistemas.	

4.1. Requirements for DMP architecture

Requirement No.	Requirement details
R1 Data management platform has to consist of three related layers which are responsible for implementation of different functionalities.	Data management platform has to consist of these layers: - data layer which is responsible for data ingress functionality from data sources and includes already prepared connections to ingest standard data types and open integration interfaces (API) for more complex data ingress cases. This layer should also have storage (data lake) tailored for practically unlimited data size and user count. - control layer which is responsible for data handling, processing, and transformations, also ensuring data security and data transfer to other applications. - analysis layer which is responsible for data analysis and visualisation functionality enabling users to perform work with data while achieving their goals.
R2 Platform has to use easily changeable and expandable architecture.	Platform has to work as an ecosystem to which it should be possible to add new systems, functionalities, or other extensions when the Customer needs increase or the technologies change.
R3 Platform has to enable users with respective rights using platform-provided tooling create automated data ingress and egress mechanisms in such a way that different national and municipal government institutions of the Republic of Lithuania, and also data from other sources, which is located in their information systems, websites, and in other places, could be used both in the platform and also outside of its boundaries.	
R4 The employees of different institutions, that have respective rights, by using a simple UI or programming interface, have to be able to manually upload datasets, create automatic data ingress mechanism, perform data transformations, perform data analysis, create visualisations, and manually take data out, or create automatic data egress to external systems of their own or other information systems.	

3 pav. Apibendrinta duomenų valdymo platformos architektūra
Figure 3. The architecture summary of the DMP



4.2. Reikalavimai duomenų valdymo platformos funkcionalumui

4.2.1. Reikalavimai duomenų įsisavinimo funkcionalumui

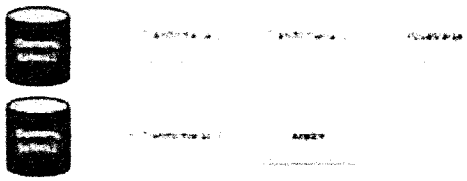
Reikalavimo Nr.	Reikalavimų detalizavimas
R5 Platforma turi įgalinti vartotojus įvesti ar įkelti įvairių rūšių duomenų rinkinius ar įkelti elektronines rinkmenas.	Turi būti galimybė sukurti teikiamų duomenų įvedimo formą ir suteikti kitiems vartotojams teisę ją pildyti. Turi būti galimybė naudojant paprastą vartotojo sąsają keliais paspaudimais įkelti duomenis iš CSV, XML ir pan. arba įkelti kitų formatų elektronines rinkmenas, tokias kaip nuotrauka ar nestruktūrizuotas tekstas. Lentelės pavidalo duomenims, tokiems kaip CSV, XLSX ir pan., platforma turi automatiškai pasiūlyti duomenų rinkinio struktūrą ir identifikuoti stulpelių duomenų tipus, kai jis yra įkeliamas pirmą kartą.
R6 Turi būti galimybė naudojant platformos funkcionalumą sąveikauti su trečiųjų šalių informacinėmis sistemomis	Turi būti galimybė vartotojui, turinčiam atitinkamas teises, aprašyti ir sukonfigūruoti duomenų priėmimo mechanizmą, leidžiantį išoriniams vartotojams ar sistemoms įkelti duomenų rinkinius arba elektronines rinkmenas. Turi būti galimybė vartotojui, turinčiam atitinkamas teises, naudojant paprastą vartotojo sąsają aprašyti ir sukonfigūruoti duomenų paėmimo mechanizmą, leidžiantį paimti duomenų rinkinius ar elektronines rinkmenas teisiai iš trečiųjų šalių informacinių sistemų. Platforma turi turėti iš anksto egzistuojančius prisijungimo būdus, kurie galėtų būti sukonfigūruoti duomenų paėmimui iš SQL duomenų bazių, HDFS ar kitokių failinę sistemą naudojančių bazių, debesyse veikiančių duomenų bazių bei duomenų srautų taip, kad daugeliu atvejų tai galima būtų įgyvendinti be papildomo kodo rašymo. Platforma turi turėti paruoštus prisijungimus prie dažniausiai pasitaikančių duomenų šaltinių, tokių kaip Oracle, SQL server, FTP server, SAS, SAP, Hive, Teradata, Sybase, DB2 ir pan. Jeigu prisijungimas būtų neįmanomas įgyvendinti anksčiau minėtais būdais turi būti galimybė sukurti trūkstamus prisijungimus.
R7 Platforma turi leisti automatizuoti duomenų ir elektroninių rinkmenų įkėlimo ir paėmimo procesus.	Turi būti galimybė vartotojui, turinčiam atitinkamas teises, kurti automatinius procesus, kurie pagal jo numatytą datą ir laiką galės atlikti duomenų ar elektroninių rinkmenų paėmimą, išarchyvavimą ir įkėlimą į platformos duomenų bazę. Turi būti galimybė vartotojui, turinčiam atitinkamas teises, kurti automatinius procesus, kurie iš vidinių ar išorinių vartotojų ar trečiųjų šalių sistemų įkeltus duomenų rinkinius ar elektronines rinkmenas galėtų priimti, išarchyvuoti ir įkelti į platformos duomenų bazę.

4.2. Requirements for DMP functionality

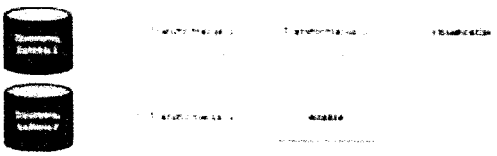
4.2.1. Requirements for data integration functionality

Requirement No.	Requirement details
R5 Platform has to enable users to input or upload datasets of different types or upload electronic files.	There has to be an ability to create data input form for provided data and grant other users the right to fill it out. There has to be an ability using a simple UI in a few clicks to upload data from CSV, XML, etc., or to upload electronic files of other formats, such as picture or unstructured text. For tabular data, such as CSV, XLSX, etc., the platform has to automatically offer a dataset structure and identify data types of columns, when the dataset is uploaded for the first time.
R6 There has to be an ability to interact with third party information systems using platform functionality.	There has to be an ability for a user, which has respective rights, to describe and configure data ingress mechanism, which allows external users or systems to upload datasets or electronic files. There has to be an ability for a user, which has respective rights, using a simple UI, to describe and configure data ingress mechanism, which allows ingesting datasets or electronic files directly from third party information systems. The platform has to have already existing connection methods, which are configurable for data ingress from SQL databases, HDFS or other filesystem-using databases, databases running in cloud, and data streams in such a way, that in most cases it would be possible to implement this without writing additional code. The platform has to have already available connections to most commonly encountered data sources, such as Oracle, SQL Server, FTP server, SAS, SAP, Hive, Teradata, Sybase, DB2, etc. If the connection is impossible to implement using the above mentioned methods, it should be possible to create the missing connections.
R7 The platform has to allow automation of data and electronic files' ingress and egress processes.	There has to be an ability for a user, which has respective rights, to create automatic processes, which could perform ingestion, extraction of archives, and uploading to the platform database the data or electronic files using the date and time defined by the user. There has to be an ability for a user, which has respective rights, to create automatic processes, which could accept, extract archives, and upload to the platform database the datasets or electronic files uploaded from internal or external users or third party information systems.

4.2.2. Reikalavimai duomenų apdorojimo funkcionalumui

Reikalavimo Nr.	Reikalavimų detalizavimas
R8 Platforma turi įgalinti vartotojus dirbti su įvairių rūšių duomenimis, leisti juos jungti, apdoroti bei prireikus šiuos veiksmus automatizuoti.	Turi būti galimybė vartotojui, turinčiam atitinkamas teises, atlikti duomenų valymą, jungimą ir transformaciją naudojant: - lengvai valdomą vartotojo sąsają duomenų įkėlimo metu leidžiančią atlikti paprastus duomenų valymo darbus, tokius kaip pasikartojančių įrašų šalinimas, reikšmių normalizacija, reikšmės pakeitimas į skaičių, išvestinių stulpelių kūrimas, stulpelių sujungimas, reikšmių pakeitimas kitomis reikšmėmis, įrašo išskaidymas į kelis stulpelius, stulpelio reikšmių užmaskavimas naudojant maišos funkcijas ir t. t. - lanksčią programavimo aplinką, leidžiančią rašyti kodą SQL, R (ar kita statistinės analizės programavimo kalba) ir Python (ar kita bendrosios paskirties programavimo kalba) kalbomis taip, kad skirtingi transformacijos etapai galėtų būti parašyti naudojant skirtingą programavimo kalbą. Testavimo reikmėms turi būti galimybė paleisti transformacijos kodą su mažais duomenų pavyzdžiais (angl. *subset*), sudarytais naudojant platformos filtrą prieš leidžiant juos su pilnais duomenų rinkiniais. - turi būti galimybė automatizuoti duomenų transformacijos procesus kuriant duomenų sekos planą (angl. *data pipeline*). Duomenų sekos grandinėje atsinaujinus duomenims prieš tai einančioje transformacijoje, duomenys turi atsinaujinti ir esamoje transformacijoje automatiškai pasileidžiant transformacijos kodui taip, kad atnaujinus pirmąjį duomenų šaltinį pasikeistų duomenys visuose sekos grandinės žingsniuose, įskaitant ir žingsnius, įgyvendinančius duomenų vizualizacijas. - naudojami duomenų šaltiniai gali ateiti iš skirtingų platformos duomenų bazių, bet jų jungimui turi būti naudojami tie patys įrankiai.
R9 Platforma turi turėti grafinį duomenų sekos planą (angl. *data pipeline*), kuris turi įgalinti vartotojus matyti viename lange viską, kas yra ar buvo atliekama su platformoje esančiais duomenimis: pradedant nuo duomenų šaltinių pereinant prie visų transformacijų bei iš jų išplaukiančių duomenų analizių bei vizualizacijų.	Paėmus bet kokią transformaciją, analizę ar vizualizaciją galima grafiškai atsekti visus žingsnius iki jos šaltinių, taip užtikrinant visų atliktų veiksmų eiliškumą, aiškumą ir suprantamumą.  Pasirinkus bet kokią transformaciją, turi būti galimybė matyti susijusio duomenų rinkinio pavyzdį, transformacijos programinį kodą bei metaduomenis, tokius kaip susijusio duomenų rinkinio atnaujinimo data, trukmė, būsena, dydis ir pan. Pasirinkus bet kokią transformaciją ir esant poreikiui turi būti galima atnaujinti atskirai konkretų susijusį duomenų rinkinį arba kartu ir visus tokiai transformacijai reikalingus įvesties (tėvinius) duomenų rinkinius iki pat pirminių duomenų šaltinių. Tais atvejais, kai su pasirinkta transformacija susijusio duomenų rinkinio atnaujinimui reikia atnaujinti ir visus įvesties (tėvinius) duomenų rinkinius iki pat pirminių duomenų šaltinių, platforma tai turi galėti padaryti automatiškai, t. y. automatiškai nustatyti priklausomybes tarp duomenų rinkinių pagal duomenų sekos planą.

4.2.2. Requirements for data processing functionality

Requirement No.	Requirement details
R8 The platform has to enable users to work with data of various types, allow to merge, process them, and automate these steps if necessary.	There has to be an ability for a user, which has respective rights, to perform data cleaning, merging, and transformation using: - easily manageable UI which allows to perform simple data cleaning tasks, such as removal of duplicate records, value normalisation, value change into a number, derived column creation, column merging, replacing values with other values, record split into several columns, column value masking using hash functions, etc. during data ingress. - flexible programming interface, which allows to write code in SQL, R (or other statistical analysis programming language), and Python (or other general-purpose programming language) languages in such a way, that different transformation stages could be written in a different programming language. For testing purposes there has to be an ability to run the transformation code on smaller data subsets, which are created using platform filter, before running them on full datasets. - there has to be an ability to automate data transformation processes by creating a data pipeline. When the data updates in a previous transformation in a data pipeline sequence, the data has to update in the current transformation by automatically launching data transformation code in such a way, that when the first data source is updated, the data should change in all data pipeline sequence steps, including the steps which implement data visualisations. - the data sources that are used could come from different databases of the platform, but the same tooling has to be used to join all these data sources.
R9 The platform must have a graphical data pipeline, which has to enable users to see in one window everything that has been performed with the data in the platform: starting from data sources and ending with all transformations and the consequent data analyses and visualisations.	After choosing any transformation, analysis, or visualisation, one can graphically trace all steps to its data sources, and in such way ensure the sequencing, clarity, and understandability of all performed actions.  After choosing any transformation, there has to be an ability to see an example of its related dataset, transformation code, and metadata such as its related dataset update date, update duration, status, size, etc. After choosing any transformation and if necessary, it should be possible to separately update a particular related dataset, or also update all parent datasets that are needed for that transformation up to its primary data sources. In those cases, when for the purpose of updating the dataset that is related to the chosen transformation it is needed to also update all parent datasets up to its primary data sources, the platform must be able to do that automatically, that is, automatically deduce the dependencies between datasets according to the data pipeline.

Reikalavimo Nr.	Reikalavimų detalizavimas
R10 Platforma turi turėti versijavimo funkcionalumą.	Versijavimo funkcionalumas turi būti taikomas ir duomenų rinkiniams, ir programiniam kodui. Prireikus turi būti galimybė atstatyti transformacijos paveiktus duomenų rinkinius ar pakeistą programinį kodą į pasirinktą versiją.
R11 Platformoje turi būti realizuoti konfigūruojami duomenų korektiškumo įspėjimai.	Vartotojas, turintis atitinkamas teises, turi galėti duomenų rinkiniams nustatyti duomenų korektiškumo parametrus. Turi būti galima nustatyti bent tokius duomenų korektiškumo parametrus: - eilučių skaičius - ar stulpelyje visos reikšmės yra unikalios - stulpelyje esančių null reikšmių skaičius Vartotojas, turintis atitinkamas teises, turi galėti nustatyti kritinę ribą kiekvienam duomenų korektiškumo parametrui, kuriuos platforma turi automatiškai stebėti. Duomenų korektiškumo parametrui pasiekus nustatytą kritinę ribą, platforma turi iškart apie tai pranešti vartotojui grafinėje vartotojo sąsajoje.
R12 Platformoje turi turėti atsišakojimo (angl. *branching*) funkcionalumą.	Atsišakojimo funkcionalumas turi leisti sukurti duomenų rinkinių ir transformacijų sekos kopiją, su kuria galima būtų dirbti neįtakojant pagrindinės platformoje naudojamos duomenų rinkinių bei transformacijų kopijos, taip, kad tai sumažintų tikimybę prarasti svarbią informaciją bei leistų kitiems vartotojams dirbti su tais pačiais duomenimis ir transformacijomis tuo pačiu metu. Po to, kai darbas su šaka yra baigtas, turi būti galimybė ją suderinti su pagrindine šaka ir įdiegti į pagrindinę platformoje naudojamą kopiją.

Requirement No.	Requirement details
R10 The platform must have a versioning functionality.	The versioning functionality has to be applied both to datasets, and to code. If necessary, there has to be an ability to restore the datasets affected by a transformation or the changed code to a chosen version.
R11 The platform must have data correctness warnings.	A user, which has respective rights, must be able to set data correctness parameters to datasets. It must be possible to set at least these data correctness parameters: - row count - whether all values in a column are unique - the amount of null values in a column A user, which has the respective rights, must be able to set a critical limit for each data correctness parameter, which have to be automatically monitored by the platform. When a data correctness parameter reaches a set critical limit, the platform has to immediately notify the user in the UI.
R12 The platform must have a branching functionality.	The branching functionality has to allow creation of a copy of datasets and transformation pipeline, with which one could work without affecting the main copy of the datasets and transformations used in the platform in such a way that would decrease the probability of losing important information and would allow other users to work with the same data and transformations at the same time. After the work with a branch is finished, there has to be an ability to merge it with the main branch and introduce it into the main copy used in the platform.

4.2.3. Reikalavimai duomenų analizės funkcionalumui

Reikalavimo Nr.	Reikalavimų detalizavimas
R13 Platformoje turi būti realizuota vartotojo darbo aplinka su įrankiais, kurie leidžia įvairaus žinių lygio vartotojams gauti duomenimis pagrįstus sprendimus ir atlikti įvairialypę didelės apimties duomenų analizę.	Platformoje turi būti realizuotas originalių duomenų kopijų išsaugojimas ir visų duomenims taikomų transformacijų sekimas, kad būtų išvengta svarbios informacijos praradimų. Turi būti užtikrintos įvairaus žinių lygio ir techninių gebėjimų vartotojų ir jų grupių (nuo duomenų analitikų iki paprastų vartotojų) galimybės atlikti įvairialypę duomenų analizę: - pažengusiems vartotojams (duomenų analitikams, matematikams, statistikams ir pan.) turi būti užtikrintos galimybės platformoje atlikti sudėtingą kompleksinę duomenų analizę (kurti modelius, taikyti mašininio mokymosi algoritmus ir pan.) naudojant platformoje palaikomas programavimo kalbas (žr. R8) ir tiesiogiai rašant programinį kodą; - paprastiems vartotojams turi būti užtikrintos galimybės atlikti duomenų analizę naudojant interaktyvius platformoje realizuotus įrankius.
R14 Platformoje turi būti realizuota galimybė keisti pradinio darbo aplinkos puslapio nustatymus.	Pradinio puslapio nustatymų keitimas turi leisti užtikrinti galimybę vartotojams ar specifinėms jų grupėms greitai ir sklandžiai pasiekti naudojamus įrankius ir duomenis.

4.2.3. Requirements for data analysis functionality

Requirement No.	Requirement details
R13 The platform must have a user work environment with tools which allow users of various levels of knowledge to derive data-based decisions and perform multifaceted big data analysis.	The platform must be able to preserve original data copies and track all transformations that are applied to the data for the purpose of not losing important data. The ability to perform multifaceted data analysis by users of various knowledge and technical skill levels and their groups (from data analysts to basic users) must be ensured: - advanced users (data analysts, mathematicians, statisticians, etc.) must be able to perform complex data analysis (create models, apply machine learning algorithms, etc.) in the platform by using the programming languages that are supported in the platform (see R8) and by directly writing code. - basic users must be able to perform data analysis by using interactive platform tools.
R14 It must be possible to change the settings of the home page of the workspace in the platform.	The changes in home page settings must allow users or specific user groups to quickly and easily access the tools and data they use.

Reikalavimo Nr.	Reikalavimų detalizavimas
R15 Turi būti realizuota galimybė įgaliotiems vartotojams sukurti bendrą vartotojų grupės darbo aplinką.	Šioje aplinkoje vartotojai galėtų dalytis tokiais ištekliais, kaip duomenų rinkiniais, informacijos suvestinėmis, analizėmis ir įrankiais, susijusiais su specifine vartotojų grupės užduotimi. Taip pat turi būti užtikrinta galimybė vartotojui ieškoti ir prisijungti prie kitų vartotojų grupių (atsižvelgiant į nustatytas prieigos teises ir roles), gauti darbo atnaujinimo informaciją bei dalytis komentarais apie vartotojų grupėse atliekamas užduotis.
R16 Platformoje turi būti realizuota išteklių paieškos, naršymo ir tvarkymo sistema, veikianti atsižvelgiant į vartotojų prieigos teises.	Platforma turi sudaryti galimybes vartotojams su atitinkamomis teisėmis: - nustatyti vartotojų teises peržiūrėti ir keisti išteklius; - priskirti išteklius vykdomoms užduotims (projektams); - priskirti išteklius į hierarchinę katalogų struktūrą; - dalytis ištekliais su kitais vartotojais - ieškoti prieinamų išteklių pagal raktažodžius.
R17 Platformoje turi būti realizuotas pranešimų valdymo ir tvarkymo funkcionalumas su galimybėmis vartotojui keisti nustatymus.	Vartotojui turi būti galimybė gauti sisteminius pranešimus apie duomenų sekos plano atnaujinimo statusą, duomenų korektiškumo įspėjimus ir kitus panašius techninius parametrus. Pranešimus vartotojui platforma turi pateikti grafinėje vartotojo sąsajoje. Vartotojas turi galėti nustatyti pranešimus taip, kad jie ateitų į el. pašto dėžutę, kuri yra susieta su vartotojo platformos paskyra. Vartotojas turi galėti matyti jam seniau atsiųstų pranešimų istoriją.
R18 Platformoje turi būti įgyvendintas objektų modelis.	Vartotojas turi galėti analizuoti duomenis ne tik kaip eilutes ir stulpelius, bet ir kaip atskirus objektus. Vartotojas, turintis atitinkamas prieigos teises, turi galėti atlikti šiuos veiksmus: - sukurti ir ištrinti skirtingus objektų tipus, pvz., organizacija, savivaldybė, įvykis ir pan.; - objektų tipams priskirti ir pašalinti savybes, pvz., organizacijos kodas, savivaldybės pavadinimas, įvykio data ir pan.; - kurti ir naikinti sąsajas tarp skirtingų objektų ir jų tipų, pvz., tam tikra organizacija yra registruota tam tikroje savivaldybėje; - pagal poreikį konfigūruoti objekto tipo korteles nurodant, kokia informacija jose turi atsispindėti; - atidaryti ir uždaryti objektų korteles, kuriose būtų matoma visa aktuali objekto informacija atsižvelgiant į objekto tipo kortelės konfigūraciją; - vykdyti paieškas tarp visų suintegruotų bei pagal vartotojo prieigos teises prieinamų šaltinių ir atlikti rezultatų analizę. Platformoje turi būti realizuotas: - paieškos funkcionalumas pagal įvairius kriterijus, bet tokius kaip raktažodžiai, pakaitos ženklai (angl. wildcards), loginiai operatoriai; - paieškos rezultatų apžvalgos funkcionalumas, leidžiantis matyti tiek agreguotus duomenis pagal objektų tipus bei jų savybes, tiek atskirų objektų sąrašą; - patogus vartotojo sąsają turintis objektų ir jų tipų filtravimo bei rūšiavimo funkcionalumas.

Requirement No.	Requirement details
R15 Authorised users must be able to create a common workspace for a user group.	In this environment the users could share resources, such as datasets, reports, analyses, and tools, which are related to a specific task of a user group. The ability for a user to search and join other user groups (in accordance with configured access rights and roles), get information updates, and share comments on the tasks performed in user groups also must be ensured.
R16 The platform must have a system for searching, browsing and managing resources in accordance with user access rights.	The platform has to provide the ability for users with respective rights to: - set user rights to view and change resources - assign resources to projects - assign resources to a hierarchical folder structure - share resources with other users - search accessible resources using keywords
R17 The platform must have a notification management functionality with user configurable settings.	The user must have an ability to receive system notifications about data pipeline update status, data correctness warnings, and other similar technical parameters. Platform notifications must be displayed in a graphical UI. The user must be able to configure notifications such that they would arrive to the user's email mailbox, which is tied to the user's platform account. The user must be able to see the history of their previously received notifications.
R18 The platform must have an object model.	The user must be able to analyse data not only as columns and rows but also as separate objects. The user, which has the respective access rights, must be able to perform the following actions: - create and delete different object types, e.g. organisation, municipality, event, etc. - add and remove properties on object types, e.g. organisation code, municipality name, event date, etc. - create and delete links between different objects and their types, e.g. a certain organisation is registered in a certain municipality - configure views for object types by specifying what information has to be reflected in them - open and close object views which would display all up-to-date object information, by taking into account the configuration of the object type - search across all integrated data sources, and perform analysis of the results based on user's access rights. The platform must have: - search functionality by various criteria, such as keywords, wildcards, logical operators - search result overview functionality, which allows to see both aggregated data by object types and their properties, and a list of individual results - convenient UI for filtering and sorting objects and their types.

Reikalavimo Nr.	Reikalavimų detalizavimas
R19 Platformoje turi būti realizuotas duomenų analizės funkcionalumas su patogia vartotojo sąsaja.	Sąsaja vartotojams, neturintiems specifinių programavimo įgūdžių, turi leisti atlikti įvairialypę duomenų analizę keliais paspaudimais ar pan.: - pateikti bendrą informaciją apie duomenų lentelę: eilučių ir stulpelių skaičius, atnaujinimo datą ir pan.; - išrinkti pirminių duomenų aibę bei analizuoti schemas; - braižyti duomenų histogramas; - braižyti duomenų pasiskirstymo grafikus; - braižyti laiko eilutes; - vaizduoti duomenis žemėlapiuose; - filtruoti duomenis; - tvarkyti duomenų rinkinio stulpelius: šalinti, pervadinti, keisti tvarką, kurti naujus stulpelius; - jungti duomenų rinkinius; - eksportuoti duomenų rinkinius atvirais duomenų formatais, pvz., CSV ar pan.; - rūšiuoti duomenis.
R20 Platformoje turi būti realizuotas skaičiuoklės programinės įrangos funkcionalumas, leidžiantis atlikti operacijas su duomenimis.	Turi būti užtikrintas toks minimalus skaičiuoklės funkcionalumas: - duomenų įvedimas į skaičiuoklę; - funkcijų rašymas naudojant nuorodas į langelius. Į skaičiuoklę suvestus duomenis turi būti galima analizuoti naudojant bet kuriuos kitus platformos analizės įrankius.
R21 Turi būti realizuota vartotojo darbo aplinka, kuri leistų vartotojams rašyti programinį kodą ir atlikti sudėtingas duomenų analizes ir vaizdavimą.	Šis funkcionalumas turi leisti naudoti platformoje palaikomas programavimo kalbas (žr. R8). Taip pat turi būti realizuotas programinio kodo, atskirų jo elementų ir transformacijų bei rezultatų grafinis vaizdavimas.
R22 Platformoje turi būti realizuotas vartotojo sąsają turintis internetinių aplikacijų kūrimo funkcionalumas, leidžiantis kurti papildomas duomenų vizualizacijas pagal poreikį.	Šis funkcionalumas turi leisti kurti tiek paprastas ataskaitas, tiek sudėtingos analizės atvejų ataskaitas. Prieiga prie ataskaitų turi būti kontroliuojama naudojant platformos prieigos teisių modelį.

Requirement No.	Requirement details
R19 The platform must have a data analysis functionality with a convenient UI.	The interface for users, who do not have specific programming skills, has to allow a multifaceted data analysis in a few clicks or similar: - provide a dataset summary: row and column count, last update date, etc. - view a data subset and analyse schemas - plot histograms - plot distribution charts - plot time series - display data on maps - filter data - edit dataset columns: remove, rename, change order, create new columns - join datasets - export datasets in open data formats such as CSV or similar - sort data.
R20 Platform must have a spreadsheet functionality which allows operations on data.	The following minimal spreadsheet functionality must be ensured: - data entry into spreadsheet - writing functions by using references to cells It must be possible to analyse the data entered into a spreadsheet using any other platform analysis tools.
R21 There must be a user workspace which would allow users to write code and perform complex data analyses and visualisation.	This functionality must allow the use of programming languages supported in the platform (see R8). It must be possible to graphically display the code, its separate elements and transformations along with its results.
R22 The platform must have a web application development functionality with a UI which would allow development of additional data visualisations based on need.	This functionality must allow both simple reports, and reports of complex analyses to be developed. Access to the reports must be controlled according to the platform's access rights model.

4.2.4. Reikalavimai duomenų vizualizavimo funkcionalumui

Reikalavimo Nr.	Reikalavimų detalizavimas
R23 Platformoje turi būti realizuotas interaktyvių ataskaitų kūrimo funkcionalumas.	Šis funkcionalumas turi leisti dalytis sukurtomis ataskaitomis pagal prieigos teises įvairiems vartotojams ar jų grupėms. Turi būti galimybė ataskaitas eksportuoti į PPT ar PDF formatus, spausdinti. Atsinaujinus ataskaitose naudojamiems duomenų rinkiniams, turi būti galimybė automatiškai atnaujinti ir pačią ataskaitą.
R24 Turi būti realizuotas paprastų duomenų įvedimo formų kūrimo funkcionalumas.	Turi būti galimybė sukonfigūruoti laukus pagal duomenų pildytojo poreikius. Turi būti galimybė pasirinkti lauko reikšmę iš sistemoje egzistuojančių reikšmių. Turi būti galimybė automatiškai užtikrinti duomenų korektiškumą prieš leidžiant išsaugoti formą. Įvestus duomenis turi būti galima analizuoti naudojantis bet kokiais platformoje esančiais analizės įrankiais.

4.2.4. Requirements for data visualisation functionality

Requirement No.	Requirement details
R23 It must be possible to create interactive reports in the platform.	This functionality has to allow sharing of the created reports according to the access rights for various users or user groups. There has to be an ability to export the reports to PPT or PDF formats and print. When the datasets used in a report are updated, there has to be an ability to automatically update the report itself.
R24 It must be possible to create simple data entry forms.	There has to be an ability to configure fields according to the needs of data entry person. There has to be an ability to select a value from a list of values that already exist in the system. There has to be an ability to automatically ensure data correctness before allowing to save the form. It has to be possible to analyse the entered data using any already existing analysis tools in the platform.

4.2.5. Reikalavimai duomenų iškėlimo funkcionalumui

Reikalavimo Nr.	Reikalavimų detalizavimas
R25 Platforma turi galėti saugoti ir eksportuoti tiek pirminius, tiek apdorotus duomenis atvirais formatais.	Platforma turi galėti pateikti duomenis atvirais formatais, tokiais kaip CSV ar XLSX.
R26 Platforma turi turėti JDBC tvarkyklę bei RESTful API.	Šis funkcionalumas turi leisti išoriniams įrankiams pasiekti platformoje esančius duomenis. Tai turėtų apimti tokius įrankius kaip Microsoft Power BI, Tableau ir pan. Turi būti pateikta RESTful API dokumentacija.
R27 Turi būti galimybė platformos įrankiais sukonfigūruoti duomenų eksportą.	Turi būti galimybė duomenų rinkinius pagal nustatytą datą ir laiką iškelti po vieną ar daugiau į kitas duomenų bazes, aplikacijas ar failines sistemas. Platformoje duomenų atidavimui turi būti paruošti prisijungimai prie JDBC, lokalios failų sistemos, HDFS, SFTP, S3, ABFS.

4.2.6. Reikalavimai naudotojų ir prieigos teisių valdymo funkcionalumui

Reikalavimo Nr.	Reikalavimų detalizavimas
R28 Prieiga prie platformoje esančių išteklių turi būti ribojama pagal prieigos teises.	Platformoje sukurtus išteklius, tokius kaip duomenų rinkiniai, ataskaitos, skaičiuoklės, katalogai ir pan., turi būti galima apsaugoti priskiriant mažiausiai šias prieigos teises: - vartotojai ar vartotojų grupės, kuriems suteikta skaitytojo prieigos teisė, turi galėti peržiūrėti išteklius; - vartotojai ar vartotojų grupės, kuriems suteikta redaktoriaus prieigos teisė, turi galėti peržiūrėti ir keisti išteklius; - vartotojai ar vartotojų grupės, kuriems suteikta savininko prieigos teisė, turi galėti peržiūrėti ir keisti išteklius bei keisti tų išteklių prieigos teises. Prieigos teisės turi būti visada naudojamos vartotojui bandant pasiekti sistemos išteklius tiek naudojantis grafine vartotojo sąsaja, tiek automatizuotai per platformos RESTful API.
R29 Platforma turi palaikyti hierarchinį grupių modelį.	Platformoje turi būti įmanoma kurti grupes ir joms priskirti vartotojus ir kitas (vaikines) grupes. Pvz., vartotojai į grupes gali būti skirstomi pagal organizaciją, organizacijos padalinį, darbo grupę, pareigas ir pan. Platformoje sukurtas grupes ir priskyrimus į grupes vartotojams su atitinkamomis teisėmis turi būti galima valdyti grafinėje vartotojo sąsajoje.
R30 Platformos RESTful API turi palaikyti ilgalaikį prisijungimą iš išorinių sistemų.	Platforma turi galėti išduoti ilgalaikį prisijungimo atpažinimo ženklą (angl. *authentication token*) ar slaptažodžius, kuriuos išorinės sistemos galėtų panaudoti automatizuotai pasiekiant sistemos išteklius naudojantis RESTful API. Turi būti įmanoma lengvai atšaukti tokius atpažinimo ženklus ar slaptažodžius, jei jie būtų prarasti ar paviešinti už sistemos ribų.

4.2.5. Requirements for data export functionality

Requirement No.	Requirement details
R25 The platform must be able to save and export both the initial data and processed data in open formats.	The platform must be able to provide data in open formats such as CSV or XLSX.
R26 The platform must have a JDBC adapter and RESTful API.	This functionality has to allow external tools to access the data inside the platform. This has to include tools such as Microsoft Power BI, Tableau, etc. RESTful API documentation has to be provided.
R27 It must be possible to configure data export using platform tools.	It must be possible to transfer datasets one by one or multiple of them to other databases, applications, or file systems according to a set date and time schedule. For the purpose of data egress, the platform must have prepared connections to JDBC, local file system, HDFS, SFTP, S3, ABFS.

4.2.6. Requirements for user and access control management functionality

Requirement No.	Requirement details
R28 Access to the resources in the platform must be restricted according to access rights.	It must be possible to secure the resources created in the platform, such as datasets, reports, spreadsheets, folders, etc., using at least these access rights: - users or user groups, which were granted the reader access right, must be able to view the resources - users or user groups, which were granted the editor access right, must be able to view and change the resources - users or user groups, which were granted the owner access right, must be able to view and change the resources, and also change the access rights of those resources The access rights must be always used when a user is attempting to access system's resources both through the graphical UI and in automated fashion through the RESTful API of the platform.
R29 The platform has to support a hierarchical group model.	It has to be possible to create groups and assign users and other (child) groups to them in the platform. For example, users can be assigned to groups by organisation, organisational unit, working group, work position, etc. Users with respective rights must be able to manage the groups that were created in the platform and assignments to these groups.
R30 The RESTful API of the platform has to support long term connection from external systems.	The platform has to be able to issue a long-term login authentication token or passwords which external systems could use to access system's resources using RESTful API in an automated fashion. It must be possible to easily revoke such authentication tokens or passwords in case they are lost or published outside the system.

Reikalavimo Nr.	Reikalavimų detalizavimas
R31 Platforma turi palaikyti išteklių saugojimą katalogų hierarchijoje.	Platforma turi palaikyti pagrindinių katalogų kūrimą, į kuriuos vartotojai turi galėti dėti išteklius pagal jų šaltinį, organizacijos struktūrą, projektinę veiklą ar kitą loginę tvarką. Kataloguose vartotojai turi galėti dėti išteklius ar kitus (vaikinius) katalogus. Turi būti galimybė kiekvieną katalogą hierarchijoje apsaugoti prieigos teisėmis. Vaikiniai katalogai ir ištekliai turi paveldėti savo prieigos teises iš visų savo tėvinių katalogų.
R32 Vartotojų paieškos rezultatuose rodomi ištekliai turi atitikti kiekvieno iš rodomų išteklių prieigos teises.	Paieškos rezultatuose turi būti rodomi tik tie ištekliai, kuriuos ieškantis vartotojas turi prieigos teises matyti.
R33 Platforma turi palaikyti išteklių apsaugojimą saugumo žymomis.	Papildomai prie aukščiau aprašytų prieigos teisių, turi būti galimybė ištekliams suteikti vieną ar kelias saugumo žymas. Turi būti galimybė vartotojams ir grupėms suteikti prieigą prie vienos ar kelių saugumo žymų. Saugumo žymų vartotojams priskyrimą turi galėti atlikti tik vartotojai, turintys atitinkamas teises. Ištekliai kataloguose turi paveldėti katalogams priskirtas saugumo žymas. Ištekliai, kurie naudoja duomenis iš kitų saugumo žymomis apribotų išteklių, turi paveldėti jų saugumo žymas. Saugumo žymos atsiradimas ant išteklių turi apriboti vartotojų turėtas prieigos teises prie išteklių. Pvz., vartojas, turintis savininko prieigos teisę prie išteklių, bet neturintis visų ištekliams suteiktų saugumo žymų, turi negalėti jų pasiekti. Vartotojas turi turėti kiekvieną išteklių saugumo žymą tam, kad galėtų pasiekti išteklius. Vartotojai turi negalėti priskirti ištekliams tokios saugumo žymos, po kurios priskyrimo jie patys nebegalėtų pasiekti išteklių.

Requirement No.	Requirement details
R31 The platform has to support saving of resources in a folder hierarchy.	The platform has to support creating main folders, into which users could place resources by their source, organisational structure, project work, or any other logical order. The users have to be able to place resources or other (child) folders inside folders. It has to be possible to secure each folder in a hierarchy using access rights. Child folders and resources have to inherit the access rights from all of their parent folders.
R32 The resources shown in user search results have to respect the access rights of each of the shown resources.	Only those search results, for which the user that is performing the search has access rights to view, have to be shown.
R33 The platform has to support protecting the resources using security markings.	In addition to the above described access rights, there has to be an ability to assign one or more security markings to resources. There has to be an ability to assign access to one or more security markings for users and groups. Only the users that have respective rights can assign security markings to users. Resources that are in folders have to inherit the security markings of folders. Resources that use data from other resources that are restricted using security markings have to inherit the security markings of those resources. The addition of a security marking on resources has to restrict the previous rights that users had on those resources. For example, a user that has owner access right to resources but does not have all the security markings assigned to those resources, has to be unable to access them. The user must have each security marking of the resources to be able to access such resources. The users must be unable to assign such security marking to resources, if after assigning it they themselves would not be able to access these resources.

4.3. Reikalavimai duomenų integracijai

R34 Duomenų valdymo platformos diegimo metu, turi būti integruoti ir apdoroti nurodyti Užsakovo pateiktų duomenų šaltinių duomenys. Sąsajos su duomenų šaltiniais ir duomenys turi būti integruoti tokiais etapais, apimtimi ir terminais:

4.3. Requirements for data integration

R34 During the course of DMP installation a list of Customer defined data sources must be integrated and processed. Data source connections and data integration must be implemented in the following stages and under the following scope and timelines:

Užduotis	**Duomenų šaltiniai**	**Registrai / IS**	**Preliminari apimtis**	**Integracijos terminas**
COVID-19 informacinės sistemos duomenų įsisavinimo, transformacijų ir realizuotų duomenų vizualizavimo sprendimų perkėlimas	Aplinkos apsaugos agentūra; Informatikos ir ryšių departamentas prie Lietuvos Respublikos vidaus reikalų ministerijos; Higienos institutas; Lietuvos bankas; Lietuvos Respublikos sveikatos apsaugos ministerija; AB „Litgrid“; Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos; Policijos departamentas prie Lietuvos Respublikos vidaus reikalų ministerijos; Sveikatos priežiūros institucijos; Valstybės sienos apsaugos tarnyba; Valstybinė ligonių kasa prie Sveikatos apsaugos ministerijos; COVID-19 testavimo laboratorijos	Elektroninė sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinė sistema; Mirties atvejų ir jų priežasčių valstybės registras; Policijos registruojamų įvykių registras; Administracinių nusižengimų registras; Integruota statistikos informacinė sistema; Sveikatos priežiūros institucijų, savivaldybių administracijų, Nacionalinio visuomenės sveikatos centro; Lietuvos banko interneto svetainė; Ekonominės stebėsenos institucijų duomenys	Duomenų įsisavinimas: iki 40 lentelių, iki 80 transformacijų; Duomenų vizualizavimas: iki 160 grafikų, iki 50 lentelių, iki 40 žemėlapių	Per 1 mėn. nuo pirkimo sutarties pasirašymo
Tarpžinybinės duomenų saugyklos ir Integruotos statistikos informacinės sistemos duomenų šaltinių duomenų paėmimas	Lietuvos Respublikos finansų ministerija; Migracijos departamentas prie Lietuvos Respublikos vidaus reikalų ministerijos; Muitinės departamentas prie Lietuvos Respublikos finansų ministerijos; Nacionalinė mokėjimo agentūra prie Žemės ūkio ministerijos; Valstybinė mokesčių inspekcija; Valstybinės teritorijų planavimo ir statybos inspekcija; Valstybinio socialinio draudimo fondo valdyba prie Socialinės apsaugos ir darbo ministerijos; VĮ „Regitra“; VĮ Registrų centras	Valstybės biudžeto, apskaitos ir mokėjimų informacinė sistema (VBAMS); Viešojo sektoriaus apskaitos ir ataskaitų konsolidavimo informacinė sistema (VSAKIS); Europos Sąjungos struktūrinės paramos kompiuterinė informacinė valdymo ir priežiūros sistema; Informacinė sistema „Migris“; Integruota muitinės informacinė sistema; Paramos administravimo informacinė sistema; Integruota mokesčių informacinė sistema; PVM informacijos mainams tarp Europos Sąjungos valstybių skirta informacinė sistema (ITIS_EU); Gyventojų pajamų mokesčio informacinė sistema; Mokesčių mokėtojų registras; Mokesčių apskaitos informacinė sistema (MAIS); Akcizų informacinė sistema; Duomenų saugyklos informacinė sistema; Statybos leidimų ir statybos valstybinės priežiūros informacinė sistema „Infostatyba“; Apdraustųjų valstybiniu socialiniu draudimu (SODRA) informacinė sistema; Lietuvos Respublikos kelių transporto priemonių registras; Nekilnojamojo turto registras ir sandorių duomenų bazės; Juridinių asmenų registras; Juridinių asmenų dalyvių informacinė sistema; Lietuvos Respublikos adresų registras; Lietuvos Respublikos gyventojų registras	Iki 200 duomenų lentelių	Per 9 mėn. nuo pirkimo sutarties pasirašymo

Task	Data sources	Registries / IS	Preliminary scope	Integration timeline
Transfer of data integrations, transformations and visualisations from the COVID-19 information system	Environmental Protection Agency; Department of Informatics and Communications under the Ministry of the Interior of the Republic of Lithuania; Institute of Hygiene; Bank of Lithuania; Ministry of Health of the Republic of Lithuania; AB Litgrid; National Center for Public Health under the Ministry of Health; Police Department under the Ministry of the Interior of the Republic of Lithuania; Health care institutions; State Border Guard Service; State Patient Fund under the Ministry of Health COVID-19 testing laboratories	Electronic health services and collaboration infrastructure information system; State Register of Deaths and Their Causes; Register of events registered by the police; Register of Administrative Offenses; Integrated statistical information system; Health care institutions, municipal administrations, National Center for Public Health; Website of the Bank of Lithuania; Data of economic monitoring institutions	Data integration: up to 40 tables, up to 80 transformations; Data visualisation: up to 160 graphs, up to 50 tables, up to 40 maps	Within 1 month from the signing of the procurement contract
Interdepartmental data warehouse and Integrated Statistical Information System data source data integration	Ministry of Finance of the Republic of Lithuania; Migration Department under the Ministry of the Interior of the Republic of Lithuania; Customs Department under the Ministry of Finance of the Republic of Lithuania; National Paying Agency under the Ministry of Agriculture; State Tax Inspectorate; State Territorial Planning and Construction Inspectorate; Board of the State Social Insurance Fund under the Ministry of Social Security and Labor; SE Regitra; SE Center of Registers	State Budget, Accounting and Payment Information System (VBAMS); Public Sector Accounting and Reporting Consolidation Information System (VSAKIS); European Union structural assistance computer information management and monitoring system; Information system "Migris"; Integrated customs information system; Support administration information system; Integrated tax information system; Information system for the exchange of VAT information between the countries of the European Union (ITIS_EU); Personal income tax information system; Taxpayer Register; Tax Accounting Information System (MAIS); Excise information system; Data warehouse information system; Information system for building permits and state supervision of construction "Infostatyba"; State Social Insurance Insured Information System (SODRA); Register of Road Vehicles of the Republic of Lithuania; Real estate registry and transaction databases; Register of Legal Entities; Information system for participants of legal entities; Register of Addresses of the Republic of Lithuania; Population Register of the Republic of Lithuania.	Up to 200 data tables	Within 9 months from the signing of the procurement contract

R35 Prieš įgyvendinant duomenų šaltinių integravimą, bet ne vėliau nei per 14 kalendorinių dienų nuo sutarties pasirašymo datos, užsakovas pateikia Tiekėjui detalesnę informaciją apie kiekvieną duomenų šaltinį ir kartu su Tiekėju sudaro detalų duomenų integravimo planą, patikslinantį, kokie duomenys turi būti integruojami iš kiekvieno duomenų šaltinio, bei, prireikus, nurodantį detalesnius duomenų integravimo terminus kiekvienam duomenų šaltiniui.

R36 Tiekėjas turi užtikrinti įvardytų duomenų įsisavinimą nurodyta apimtimi ir terminais. Tiekėjas, nustatęs kliūtis, dėl kurių negali realizuoti numatytų duomenų srautų (pvz., duomenų turėtojas nepateikia reikalingos informacijos laiku), turi iš karto informuoti Užsakovą.

R37 Tiekėjas yra atsakingas už duomenų sukėlimą į platformą. Atlikdamas analizę tiekėjas turi įvertinti esamą (COVID-19 IS) duomenų aibę ir tinkamai suplanuoti duomenų perkėlimą. Už duomenų paėmimo formalizavimą – sutarčių su duomenų turėtojais pasirašymą ir pan., atsakingas yra Užsakovas.

R35 Prior to the integration of data sources, but not later than within 14 calendar days from the date of signing the contract, the Customer shall provide the Supplier with more detailed information on each data source and together with the Supplier draw up a data integration plan specifying which data will be integrated from each data source, and indicating, where appropriate, more detailed data integration deadlines for each data source.

R36 Supplier must ensure that data from the above listed data sources will be integrated under agreed scope and timelines. Supplier must immediately inform the Customer in case there are obstacles preventing Supplier from integrating data (e.g. owner of the data doesn't provide required information on time).

R37 Supplier is responsible for data integration into the platform. Supplier must evaluate current set of data (COVID-19 IS) and plan its transfer accordingly. Customer is responsible for formalisation of data access, e.g. handling data sharing agreements with data owners, etc.

4.4. Reikalavimai duomenų valdymo platformos diegimui

R38 Duomenų valdymo platforma turi būti įdiegta per 1 (vieną) mėnesį (31 kalendorinę dieną) nuo pirkimo sutarties pasirašymo dienos.

4.5. Reikalavimai mokymams ir mokymų medžiagai

R39 Tiekėjas įsipareigoja sutarties galiojimo metu apmokyti iki 10 Užsakovo specialistų (iki 2 sistemos ir duomenų administratorių ir iki 8 duomenų analitikų).

R40 Turi būti pateikta išsami platformos administratorių ir naudotojų mokymo medžiaga, kuri turi apimti, bet neapsiriboti: naudojimo bendrąja informacija, su konkrečiais platformos naudojimo procesais ir funkcijomis susijusia informacija, administratorių ir naudotojų instrukcijomis.

R41 Mokymams naudojamą mokymų medžiagą turi būti galima panaudoti kitų naudotojų mokymams (mokymus turi galėti pravesti anksčiau apmokinti atitinkamos valstybės institucijos naudotojai) be papildomų minėtos informacijos keitimo, koregavimo ar konfigūravimo darbų.

4.6. Reikalavimai dokumentacijai

R42 Duomenų valdymo platformos dokumentacija, įskaitant techninį pasiūlymą, mokymų medžiagą ir RESTful API užklausų aprašymus, turi būti pateikta lietuvių arba anglų kalba.

4.7. Reikalavimai licencijavimui

R43 Įsigyta licencija negali riboti duomenų valdymo platformos naudotojų skaičiaus.

R44 Įsigyta licencija turi užtikrinti platformos atnaujinimus jos galiojimo metu, be papildomų Užsakovo sąnaudų, ne rečiau kaip vieną kartą per mėnesį.

R45 Įsigyta licencija ne trumpiau kaip 1 (vienus) metus turi užtikrinti duomenų valdymo platformos palaikymą, įskaitant klaidų taisymą ir atnaujinimus.

R46 Tuo atveju, kai platformoje yra naudojami trečiųjų šalių programiniai komponentai, pvz., atvirojo kodo (angl. open source) programiniai komponentai, Tiekėjas turi pateikti tokių komponentų sąrašą ir visas su jais susijusias licencijas.

5. Reikalavimai duomenų valdymo platformos infrastruktūrai

R47 Tiekėjas turi užtikrinti duomenų valdymo platformai reikalingą infrastruktūrą.

R48 Platformos duomenų saugojimo funkcionalumas turi palaikyti paskirstytas, saugias ir plačiai pasiekiamas duomenų saugojimo infrastruktūras, tokias kaip, pvz., Azure Blob Store, HDFS ar Amazon S3.

R49 Naudojama infrastruktūra turi galėti dinamiškai plėstis (angl. horizontal scaling) pagal realaus laiko resursų poreikį, taip užtikrindama reikalingus resursus turimam duomenų kiekiui ir naudotojų skaičiui.

R50 Platforma turi būti įgyvendinta „vieno langelio“ principu, t. y. turi būti patogi vartotojo aplinka, per kurią galima lengvai pasiekti visus suintegruotus duomenų šaltinius bei platformos įrankius neišeinant už platformos ribų ir nesinaudojant papildomomis taikomosiomis programomis.

R51 Platformos tarnybinių stočių veikimas turi būti nuolatos stebimas. Į iškilusius incidentus turi būti operatyviai reaguojama ir sutrikimai turi būti šalinami pagal standartines veiklos procedūras.

R52 Platforma turi turėti integruotą (-us) autentifikavimo ir autorizavimo servisą (-us), kuris (-ie) gebėtų integruotis su išoriniais tapatybių teikėjais (angl. identity provider) ir kuris (-ie) palaiko vieno prisijungimo (angl. single-on) su dviejų veiksnių autentifikacija (angl. two factor authentication) schemą.

R53 Platformos autentifikavimo ir autorizavimo servisas (-ai) turi gebėti gauti papildomą informaciją apie vartotoją: pašto adresą, priklausomybę grupėms ir pan., bei vartotojų grupes, kuri turės būti naudojamos prieigos prie duomenų rinkinių nustatymui ir kontroliavimui.

R54 Turi būti galimybė perkelti duomenų valdymo platformą į kitą nei Tiekėjo infrastruktūrą (pvz., valstybinę) Užsakovo sąnaudomis.

4.4. Requirements for DMP installation

R38 DMP must be installed no later than 1 (one) month (31 calendar days) after contract signing date.

4.5. Requirements for user training and training materials

R39 During the term of the contract, the Supplier will train up to 10 Customer specialists (up to 2 system and data administrators and up to 8 data analysts).

R40 Detailed training materials for platform administrators and users must be provided. Such training materials must contain, but not be limited to, general instructions for use, information related to specific platform processes and functionalities, administrator and user instructions.

R41 Training materials provided during user training must be reusable (previously trained users of a relevant public institution must be able to carry out the training) without additional content changes, corrections or changes in platform configuration.

4.6. Requirements for documentation

R42 DMP documentation, including technical proposal, training materials and descriptions of RESTful API calls, must be provided in Lithuanian or English.

4.7. Requirements for licensing

R43 Software license cannot limit the number of DMP users.

R44 Software license must include DMP software upgrades during the term of the license and at least once a month without additional cost to the Customer.

R45 Software license must include operations and maintenance support, including bug fixes and upgrades for at least 1 (one) year.

R46 In case there are any third party software components, e.g. open-source software components, used in the platform, the Supplier must provide a list of such components and their licenses.

5. Requirements for DMP infrastructure

R47 The Supplier must provide the necessary infrastructure for the DMP.

R48 The storage functionality of the platform must support distributed, secure, and widely available storage infrastructures such as Azure Blob Store, HDFS, or Amazon S3.

R49 The infrastructure must scale dynamically according to the real time need of computing resources, thus ensuring that the necessary resources are available for the amount of stored data and the number of users.

R50 The platform must be implemented on a one-stop-shop basis, i.e. there must be a user-friendly environment through which all integrated data sources and platform tools can be easily accessed without leaving the platform and without the use of additional external applications.

R51 The operation of DMP servers must be constantly monitored. Incidents must be responded promptly and resolved in accordance with standard operating procedures.

R52 DMP must have integrated authentication and authorization service(s) that can be integrated with external identity providers and that support(s) single sign-on with two factor authentication scheme.

R53 The platform authentication and authorization service(s) must be able to obtain additional information about the user: email address, group membership, etc., and user groups, which will be used to set and control access to the datasets.

R54 It must be possible to move DMP to an infrastructure other than the Supplier's (e.g. Government's) at the Customer's expense.

6. Reikalavimai saugumui

Duomenų valdymo platforma turi atitikti šiuos informacinei infrastruktūrai keliamus techninius kibernetinio saugumo reikalavimus:

R55 Tarptautinį standartą ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems — Requirements.

R56 Tarptautinį standartą ISO/IEC 27002:2013 Information technology – Security techniques – Code of practice for information security controls. Duomenų valdymo platformoje saugomi duomenys turi būti apsaugoti nuo nesankcionuoto priėjimo, naudojimo, pakeitimo, atskleidimo, sunaikinimo ar praradimo.

R57 Siekiant užtikrinti perduodamos informacijos saugą, turi būti naudojama ne žemesne nei TLS 1.2 kriptografijos protokolo versija šiuose komunikacijos scenarijuose: sistema–naudotojas ir pagal poreikį sistema–sistema.

R58 Duomenys platformoje turi būti šifruojami tiek tranzito metu (angl. in transit), tiek ramybės būsenoje (angl. at rest).

R59 Turi būti galimybė Užsakovui naudoti savo šifravimo raktą (angl. bring your own key) duomenims šifruoti platformoje ir prireikus jį ištrinti, taip užtikrinant, kad duomenys liks užšifruoti ir nepasiekiami.

R60 Duomenų valdymo platforma turi būti apsaugota nuo:

- neautentifikuotos prieigos;
- naudotojų veiksmų, neatitinkančių jų autorizacijos rolės;
- nesankcionuoto naudotojo sesijos perėmimo;
- nesankcionuoto duomenų perėmimo ar jų įterpimo;
- žalingo kodo įterpimo (angl. *Injection*, XSS (*Cross-site scripting*));
- kitų saugumo pažeidimų, kurie įvardijami OWASP
- TOP 10 (https://www.owasp.org) arba lygiaverčiame sąraše.

R61 Sistemos slaptažodžiai negali būti saugojami programiniame kode.

R62 Sistemos svetainė turi drausti išsaugoti slaptažodžius.

R63 Atliekant sistemos svetainės administravimo darbus ryšys turi būti šifruojamas naudojant ne trumpesnį kaip 128 bitų raktą.

R64 Šifruojant naudojami skaitmeniniai sertifikatai privalo būti išduoti patikimų sertifikavimo tarnybų. Sertifikato raktas turi būti ne trumpesnis kaip 2048 bitų.

R65 Svetainės kriptografinės funkcijos turi būti įdiegtos tarnybinės stoties, kurioje yra svetainė, dalyje arba kriptografiniame saugumo modulyje (angl. Hardware security module).

R66 Visi kriptografiniai moduliai turi gebėti saugiai sutrikti (angl. fail securely).

R67 Draudžiama sistemos tarnybinėje stotyje saugoti sesijos duomenis (identifikatorių), pasibaigus susijungimo sesijai.

R68 Turi būti naudojama svetainės saugasienė (angl. Web *Application Firewall*). Įsilaužimo atakų pėdsakai (angl. *attack signature*) turi būti atnaujinami naudojant patikimus aktualią informaciją teikiančius šaltinius. Naujausi įsilaužimo atakų pėdsakai turi būti įdiegiami ne vėliau kaip per dvidešimt keturias valandas nuo gamintojo paskelbimo apie naujausius įsilaužimo atakų pėdsakus datos arba ne vėliau kaip per septyniasdešimt dvi valandas nuo gamintojo paskelbimo apie naujausius įsilaužimo atakų pėdsakus datos, jeigu valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros valdytojo sprendimu atliekamas įsilaužimo atakų pėdsakų įdiegimo ir galimo jų poveikio valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros veiklai vertinimas (testavimas).

6. Security requirements

DMP must meet the following cyber security requirements for the information infrastructure:

R55 International standard ISO/IEC 27001: 2013 *Information technology - Security techniques - Information security management systems - Requirements.*

R56 International standard ISO/IEC 27002: 2013 *Information technology – Security techniques – Code of practice for information security controls.* Data stored on the DMP must be protected from unauthorized access, use, alteration, disclosure, destruction or loss.

R57 To ensure the security of transferred information, a cryptographic protocol version not lower than TLS 1.2 has to be used in these communication scenarios: system–user and, where necessary, system–system.

R58 The data on the DMP must be encrypted both during transit and at rest.

R59 It must be possible to use Customer generated private key (BYOK) to encrypt the data on the platform and delete the key if necessary, thus ensuring that the data remains encrypted and inaccessible.

R60 The DMP must be protected against:

- unauthenticated access;
- actions by users that do not correspond to their authorization role;
- unauthorized user session interception;
- unauthorized interception or insertion of data;
- injection, XSS (Cross-site scripting);
- other security breaches listed in the OWASP TOP 10 (https://www.owasp.org) or equivalent list.

R61 System passwords cannot be stored in the source code.

R62 System website must prohibit saving passwords.

R63 During site administration, the connection must be encrypted using a key of at least 128 bits.

R64 Digital certificates used for encryption must be issued by trusted certification authorities. The certificate key must be at least 2048 bits long.

R65 The cryptographic features of the site must be installed in the part of the server where the site is located or in the hardware security module.

R66 All cryptographic modules must be able to "fail securely".

R67 It is forbidden to store session data (identifier) on the server after connection session ends.

R68 The Web Application Firewall must be used. Attack signatures must be updated using reliable sources that provide up-to-date information. The latest traces of hacking attacks must be installed no later than twenty-four hours from the date of the manufacturer's announcement of the latest traces of hacking attacks, or no later than seventy-two hours from the date of the manufacturer's announcement of the latest traces of hacking attacks if, by the decision of the manager of state information resources or critical information infrastructure, the assessment (testing) of the implementation of traces of intrusion attacks and their possible impact on the activities of state information resources or critical information infrastructure is being performed.

R69 Turi būti naudojama sistemos svetainė naudotojo įvedamų duomenų tikslumo kontrolė (angl. validation).

R70 Tarnybinė stotis, kurioje yra sistemos svetainė, neturi rodyti sistemos svetainės naudotojui klaidų pranešimų apie svetainės programinį kodą ar tarnybinę stotį.

R71 Sistemos svetainė saugumo priemonės turi gebėti uždrausti prieigą prie tarnybinės stoties iš IP adresų, vykdžiusių grėsmingą veiklą (nesankcionuoti mėginimai prisijungti, įterpti SQL intarpus ir panašiai).

R72 Tarnybinė stotis, kurioje yra sistemos svetainė, turi leisti tik svetainės funkcionalumui užtikrinti reikalingus protokolo metodus.

R73 Turi būti uždrausta naršyti sistemos svetainės aplankuose (angl. directory browsing).

R74 Turi būti įdiegta sistemos svetainė turinio nesankcionuoto pakeitimo (angl. defacement) stebėsenos sistema.

R75 Duomenų valdymo platformoje turi būti fiksuojamos naudotojų registracijos užklausos, prisijungimo sesijos, jų pradžia, pabaiga, naudotojų veiksmai, teisių naudotis sistema pakeitimai, veiksmai su sistemos objektais, audito funkcijos įjungimas ar išjungimas, audito įrašų trynimas, kūrimas ar keitimas, laiko ir (ar) datos pakeitimai ir kiti veiksmai.

R76 Turi būti sudaryta galimybė tokių auditų žurnalų eksportavimui už platformos ribų.

R77 Kiekviename audito duomenų įraše turi būti fiksuojama įvykio data ir tikslus laikas, įvykio rūšis, naudotojo duomenys, įvykio rezultatas.

R78 Priemonės, naudojamos sistemos sąsajoje su viešųjų elektroninių ryšių tinklu, turi būti nustatytos taip, kad fiksuotų visus įvykius, susijusius su įeinančiais ir išeinančiais duomenų srautais.

R79 Sistemoje fiksuojami įvykiai turi būti saugomi techninėje ar programinėje įrangoje, pritaikytoje audito duomenims saugoti.

R80 Dėl įvairių trikdžių nustojus fiksuoti auditui skirtus duomenis, apie tai nedelsiant turi būti informuojamas sistemos administratorius.

R81 Audito duomenys turi būti saugomi ne trumpiau kaip šešiasdešimt dienų, užtikrinant visas prasmingas jų turinio reikšmes (pavyzdžiui, sistemos naudotojo, su kuriuo nutraukti darbo santykiai ir kuris pašalintas iš sistemos, atpažinties duomenys turi būti išsaugoti visą būtiną audito duomenų saugojimo laiką).

R82 Draudžiama audito duomenis trinti, keisti, kol nesibaigęs audito duomenų saugojimo terminas.

R83 Audito duomenų kopijos turi būti apsaugotos nuo pažeidimo, praradimo, nesankcionuoto pakeitimo ar sunaikinimo.

R84 Turi būti naudojami mažiausiai du laiko sinchronizavimo šaltiniai.

R85 Naudotojų darbo sesija turi būti automatiškai užbaigiama, jei neveikimo laikas viršija nustatytą trukmę.

R69 Correctness validation of the data entered by the user must be used in the website of the system.

R70 The server in which the website of the system resides should not display error messages about the website source code or server to the user of the website.

R71 The security measures of the website of the system must be able to deny access to the server from IP addresses that have performed threatening activities (unauthorized attempts to connect, insert SQL inserts, etc.).

R72 The server in which the website of the system resides must allow only those protocol methods that are required to ensure the functionality of the website.

R73 Directory browsing in the website of the system must be prohibited.

R74 A monitoring system for unauthorized changes to the content (defacement) of the website of the system must be installed.

R75 DMP must record user registration requests, login sessions, their start and end, user actions, changes to access rights, actions with system objects, turning auditing on or off, deletion, creation, or modification of audit records, time and (or) date changes, and other actions.

R76 There must be an ability to export such audit logs out of the system.

R77 Every audit log record must capture event date and precise time, event type, user data, the result of the event.

R78 The means used in the system interface with the public electronic communications network have to be configured to record all events related to incoming and outgoing data flows.

R79 Events recorded in the system must be stored in hardware or software which is adapted for the storage of audit data.

R80 The administrator has to be immediately informed when the recording of audit data is interrupted due to various disturbances.

R81 Audit data has to be retained for a minimum of sixty days, ensuring all meaningful meanings of its content (for example, the identity of the user of the system with whom the employment relationship has been terminated and who has been removed from the system must be retained during the term of necessary storage of audit data).

R82 It is prohibited to delete or change audit data until the term of storage of audit data has expired.

R83 Copies of audit data should be protected from tampering, loss, unauthorized alteration, or destruction.

R84 At least two time synchronization sources must be used.

R85 Users' work session must end automatically if the idle time exceeds the set duration.

R86 Platformos prieigos teisių modelio ir saugumo funkcionalumų visuma turi suteikti galimybę platformoje saugomiems duomenims atitikti Europos Sąjungos Bendrąjį duomenų apsaugos reglamentą (BDAR).

Esant reikalavimų nesuderinamumui, prioritetas teikiamas labiausiai ribojančiam reikalavimui.

R86 The combination of platform access rights model and the set of security functionalities must provide the possibility for the data stored on the platform to comply with the General Data Protection Regulation (GDPR) of the European Union.

In case of incompatibility of requirements, the most restrictive requirement shall prevail.

UŽSAKOVAS
Lietuvos statistikos departamentas
Gedimino pr. 29, LT-01500 Vilnius
Įmonės kodas: 188600177
PVM mokėtojo kodas: nėra
A. s. Nr. LT51 7044 0600 0111 1285
AB SEB BANKAS
Banko kodas 70440
Tel. +370 5 236 4822
El. p. info@stat.gov.lt
http://www.stat.gov.lt

Generalinė direktorė Jūratė Petrauskienė

CUSTOMER
The Lithuanian Department of Statistics (Statistics Lithuania)
Gedimino ave. 29, LT-01500 Vilnius
Company Number: 188600177
VAT Number: None
Account Number: LT51 7044 0600 0111 1285
Bank Name: AB SEB BANKAS
Bank Code: 70440
Phone No. +370 5 236 4822
E-mail: info@stat.gov.lt
http://www.stat.gov.lt

Jūratė Petrauskienė, Director General

TIEKĖJAS
Palantir Technologies UK, Ltd.
New Penderel House
283-288 High Holborn
London, WC1V 7HP
Įmonės kodas: 7042994
PVM mokėtojo kodas: GB 101 2291 78
Bankas: JP Morgan Chase
Sąskaitos savininkas: Palantir Technologies UK, Ltd.
A. s. Nr.: 41036031
IBAN: GB36CHAS60924241036031
SWIFT: CHASGB2L
Tel. +44 7408 886228
El. p. legalnotices@palantir.com

Matt Long, įgaliotasis asmuo

SUPPLIER
Palantir Technologies UK, Ltd.
New Penderel House
283-288 High Holborn
London, WC1V 7HP
Company Number: 7042994
VAT Number: GB 101 2291 78
Bank Name: JP Morgan Chase
Account Holder: Palantir Technologies UK, Ltd.
Account Number: 41036031
IBAN: GB36CHAS60924241036031
SWIFT: CHASGB2L
Phone No. +44 7408 886228
E-mail: legalnotices@palantir.com

Matt Long, Authorised Signatory

Duomenų valdymo platformos, reikalingos Valstybės duomenų valdysenos informacinei sistemai įgalinti ir veikti, licencija, įskaitant platformos diegimą, pirkimo sutarties Nr. STAT-(2020)49 (2020)
2 priedas

License (accompanied by system deployment service) for the data management platform necessary for setting up and operation of the State Data Governance Information System, purchase Contract No STAT-(2020)49 (2020)
Annex 2

ASMENS DUOMENŲ IR INFORMACIJOS TVARKYMAS

Atsižvelgdamos į tai, kad vykdydamas pirkimo sutartį Tiekėjas gali matyti asmens duomenis, šalys siekia užtikrinti asmens duomenų apsaugą ir atitiktį 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamento (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) reikalavimams (toliau – Bendrasis duomenų apsaugos reglamentas) ir susitaria dėl tokio asmens duomenų tvarkymo sąlygų:

1. SĄVOKOS

1.1. Šiame Sutarties priede (toliau – Priedas), išskyrus jeigu kontekstas reikalautų kitos reikšmės, toliau nurodytos sąvokos turi tokias reikšmes:

1.1.1. **Duomenų subjektas** – fizinis asmuo, kurio duomenis gali matyti Tiekėjo grupė (kaip apibrėžta toliau);

1.1.2. **Duomenų tvarkymo tikslas** – pirkimo sutarties vykdymo tikslas ir atitinkamos Šalies iš pirkimo sutarties kylančių teisių įgyvendinimo bei pareigų vykdymo tikslas;

1.1.3. **Paslaugos** – bet kokios ir visos paslaugos bei darbai, kuriuos Tiekėjo grupė (kaip apibrėžta toliau) pagal pirkimo sutartį atlieka, suteikia ar perduoda Užsakovui, ir šių paslaugų bei darbų rezultatai.

1.1.4. **Sistema** – Valstybės duomenų valdysenos informacinė sistema.

1.2. Priedo 1.1 papunktyje neapibrėžtos naudojamos sąvokos turi tokią reikšmę, kokią jos turi duomenų apsaugos teisės aktuose ir Sutartyje.

2. ASMENS DUOMENŲ TVARKYMO SĄLYGOS

2.1. Šalys susitaria, kad Sutarties įgyvendinimo tikslu Tiekėjo grupei, savo vardu ir retkarčiais kaip savo dukterinių bendrovių ir filialų atstovei ("Tiekėjo grupė"), gali būti reikalinga automatizuotomis priemonėmis atlikti šio Priedo 2.7 papunktyje nurodytus duomenų tvarkymo veiksmus su nurodytais asmens duomenimis ir (ar) jų rinkiniais. Šiame Priedo punkte nurodytas asmens duomenų tvarkymo tikslo realizavimas laikomas šalių susitartu asmens duomenų tvarkymo dalyku.

2.2. Šalys pažymi, jog Tiekėjo grupė išimtinai nesiekia tvarkyti asmens duomenų, tačiau asmens duomenų tvarkymo veiksmai gali būti neatskiriamai reikalingi, siekiant tinkamai (į)vykdyti Sutartį.

2.3. Šalys susitaria, kad Sutarties įgyvendinimo tikslu Tiekėjo grupė veikia kaip Duomenų tvarkytojas, o Užsakovas – kaip Duomenų valdytojas.

2.4. Šalys susitaria, jog Užsakovas savo nuožiūra ir atsakomybe nustato, kokių duomenų subjektų kategorijų asmens duomenys bei kokių kategorijų asmens duomenys yra suteikiami Tiekėjo grupei kiekvienu konkrečiu atveju. Užsakovas teiks Tiekėjo grupei tik tokius asmens duomenis, kokių būtinai reikia Tiekėjo grupei siekiant įgyvendinti Priedo 2.1 papunktyje numatytą tikslą bei prisiima visą su tuo susijusią riziką (įskaitant riziką tais atvejais, kai Tiekėjo grupei suteikiama daugiau asmens duomenų, nei yra būtina). Siekdamas užtikrinti tinkamą asmens duomenų perdavimo Tiekėjo grupei apimtį, Užsakovas savo lėšomis ir jėgomis gali imtis papildomų priemonių, pvz., tvarkomų asmens duomenų šifravimas, pseudonimų suteikimas ir pan.

PROCESSING OF PERSONAL DATA AND INFORMATION

Whereas, in implementation of the Contract, the Supplier can see personal data, the Parties seek to ensure the protection of personal data and compliance with the requirements of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (hereinafter referred to as the "General Data Protection Regulation"), and hereby agrees on the terms and conditions for the processing of personal data as follows:

1. DEFINITIONS

1.1. For the purposes of this Annex to the Contract (hereinafter referred to as the "Annex"), the following terms and concepts shall have the meanings hereby ascribed to them, unless the context otherwise requires:

1.1.1. **Data subject** refers to a natural person whose data can be seen by the Supplier Group (as defined below).

1.1.2. **Data processing purpose** refers to the purpose of the implementation of the Contract and the purpose of the implementation of the rights and obligations of the respective Party arising from the Contract.

1.1.3. **Services** refers to all services and works carried out, provided and transferred to the Customer by the Supplier Group (as defined below) under the Contract, as well as the results of these services and works.

1.1.4. **System** refers to the State Data Governance Information System.

1.2. The terms and concepts that are not defined in Point 1.1 of the Annex shall have the meanings given to them in the data protection legislation and in the Contract.

2. TERMS AND CONDITIONS FOR PERSONAL DATA PROCESSING

2.1. The Parties agree that in the implementation of the Contract, the Supplier Group, on behalf of itself and as an agent for its subsidiaries and affiliates from time to time (the "Supplier Group"), may be required to perform the data processing operations specified in Point 2.7 of this Annex with the specified personal data and/or sets thereof through application of automated tools. The implementation of the data processing purpose specified in this Point of the Annex shall be considered as a subject of personal data processing agreed by the Parties.

2.2. The Parties note that the Supplier Group does not exclusively seek to process personal data; however, the personal data processing operations may constitute an integral part of the proper implementation of the Contract.

2.3. The Parties agree that for the purposes of the Contract, the Supplier Group operates as a Processor and the Customer operates as a Controller.

2.4. The Parties agree that the Customer shall, at the Customer's own discretion and responsibility, determine the categories of data subjects and the categories of personal data for the provision of personal data to the Supplier Group in each specific case. The Customer shall provide the Supplier Group only with such personal data that is necessary for the Supplier Group to achieve the purpose provided in Point 2.1 of the Annex and assumes all related risks (including the risk in case when the Supplier Group is provided with more personal data than necessary). In order to ensure the appropriate volume of personal data transfer to the Supplier Group, the Customer may, at the Customer's own expense and effort, take additional measures, e.g. encryption of personal data, provision of pseudonyms, etc.

2.5. Jeigu, Tiekėjo grupės vertinimu ir vadovaujantis Priedo 2.4 papunkčiu, Užsakovo jam suteikti asmens duomenys konkrečiu atveju yra nepakankami siekiant tinkamai įvykdyti Priedo 2.1 papunktyje nurodytą tikslą, Tiekėjo grupė apie tai praneša Užsakovui, prašydamas pateikti papildomus asmens duomenis, kurių tvarkymas konkrečiu atveju yra būtinas. Gavęs atitinkamą Tiekėjo grupės pranešimą, Užsakovas priima galutinį sprendimą suteikti papildomus asmens duomenis arba ne bei prisiima visą su tokiu sprendimu susijusią riziką (įskaitant riziką, jog nepateikus papildomų asmens duomenų, Tiekėjo grupė negalės tinkamai įvykdyti Sutartimi prisiimtų įsipareigojimų).

2.6. Vykdydamas Sutartį, Tiekėjas gali rinkti metriką, analizę, statistiką ar kitus duomenis, susijusius su Užsakovo vykdomu programinės įrangos naudojimu: (a) siekdamas Užsakovui ir jo naudai teikti programinę įrangą bei paslaugas ir jas apsaugoti; ir (b) statistikos tikslais, taip pat siekdamas analizuoti, palaikyti ir tobulinti programinę įrangą ir paslaugas (su sąlyga, kad šie duomenys yra nuasmeninti).

2.7. Šalys susitaria, jog visos asmens duomenų kategorijos ir duomenų subjektų kategorijos, kurias pagal šį Priedą Užsakovas gali perduoti tvarkyti Tiekėjo grupei, yra nurodytos 1 lentelėje išdėstytuose išplėstiniuose asmens duomenų kategorijų ir duomenų subjektų kategorijų sąrašuose. Užsakovas įsipareigoja perduoti Tiekėjo grupei tvarkyti tik tokius asmens duomenis, kurie nurodyti šiuose sąrašuose. Užsakovas yra atsakingas už šių sąrašų parengimą ir atnaujinimą.

1 lentelė

Duomenų tvarkymo dalykas ir tikslas	Sutarčiai įgyvendinti ir VDV IS veiklai užtikrinti
Asmens duomenų kategorijos	Lietuvos gyventojų asmens duomenys gauti iš administracinių duomenų šaltinių. Užsakovo, Tiekėjo grupės darbuotojų vardas pavardė, padalinys, pareigos, telefonas, el. paštas, naudotojo kodas, kita informacija, skirta darbuotojui identifikuoti ir teisėms darbui su sistema suteikti.
Duomenų subjektų kategorijos	Lietuvos gyventojai, Užsakovo, Tiekėjo grupės darbuotojai
Su duomenų tvarkymu susijusi veikla	Susipažinimas su asmens duomenimis, atliekant šiuos veiksmus: o Asmens duomenų iš administracinių duomenų šaltinių ir Užsakovo duomenų bazių išgavimas ir integravimas; o sugadintų programinės įrangos duomenų (įskaitant asmens duomenis) atstatymas; o sistemos veiklos atkūrimas, visiško ar dalinio funkcionavimo sutrikimo atvejais; o sistemos įvykių žurnalo analizė.

2.8. Šalys susitaria, jog Tiekėjo grupė asmens duomenis pradeda tvarkyti, kai Užsakovas Tiekėjui juos pateikia ar sudaro prieigą prie jų, ir baigia tvarkyti, kai Tiekėjo grupė įvykdo Priedo 2.1 papunktyje nurodytą tikslą ir (ar) ištrina pasibaigus jų saugojimo terminui (jei toks nustatytas) arba, Užsakovui pareikalavus, juos grąžina Užsakovui ir (ar) ištrina.

3. ASMENS DUOMENŲ TVARKYMO REIKALAVIMAI

3.1. Tiekėjo grupė įsipareigoja atlikti asmens duomenų tvarkymo veiksmus tik Priedo 2.1 papunktyje nurodytu tikslu, laikydamasis asmens duomenų apsaugos teisės aktų bei Užsakovo raštiškais dokumentais įformintų nurodymų (jei tokie pateikiami).

2.5. If, based on the Supplier Group's estimation and in accordance with Point 2.4 of the Annex, the data provided by the Customer in particular case are insufficient for proper implementation of the purpose provided in Point 2.1 of the Annex, the Supplier Group shall inform the Customer by asking to provide additional personal data which is necessary in this specific case. Upon receipt of the relevant notice from the Supplier Group, the Customer makes the final decision whether additional personal data should be provided or not and assumes all risks related to such decision (including the risk that in case of non-provision of additional data, the Supplier Group will not be able to properly fulfil the obligations under the Contract).

2.6. While fulfilling the Contract, Supplier may collect metrics, analytics, statistics or other data related to Customer's use of the Software: (a) in order to provide and secure the Software and Services to and for the benefit of the Customer; and (b) for statistical use as well as to analyse, maintain and improve the Software and Services (provided that it makes such data not personally identifiable).

2.7. The Parties agree that all categories of personal data and categories of data subjects that the Customer can transfer to the Supplier Group for processing in accordance with this Annex are specified in the extended lists of categories of personal data and categories of data subjects provided in Table 1. The Customer undertakes to transfer to the Supplier Group for processing only such personal data that are specified in these lists. The Customer is responsible for compiling and updating of these lists.

Table 1

Subject and purpose of data processing	For the implementation of the Contract and ensuring of the operation of SDM IS
Categories of personal data	Personal data of the residents of Lithuania received from the administrative data sources. The Customer's and the Supplier Group's employee's name and surname, division, position, telephone, e-mail, user code, other information to identify the employee and grant rights to work with the system.
Categories of data subjects	Residents of Lithuania, employees of the Customer, employees of the Supplier Group
Activity related to data processing	Familiarization with personal data by performing the following actions: o Extraction of personal data from administrative data sources and the Customer's databases and integration. o Recovery of corrupted software data (including personal data). o System recovery in cases of complete or partial malfunction. o System event log analysis.

2.8. The Parties agree that the Supplier Group shall start processing personal data when the Customer provides this data or access to this data, and shall finish the processing when the Supplier Group fulfils the purpose specified in Point 2.1 of the Annex and/or deletes the data upon expiry of their storage period (if any) or, at the Customer's request, returns them to the Customer and/or deletes them.

3. REQUIREMENTS FOR PERSONAL DATA PROCESSING

3.1. The Supplier Group undertakes to perform personal data processing actions only for the purpose specified in Point 2.1 of the Annex in compliance with the personal data protection legislation and the instructions (if any) documented in written form by the Customer.

3.2. Jei tai yra numatyta Sutartimi, Užsakovas suteikia Tiekėjo grupei bendrą sutikimą pasitelkti subtiekėjus (subteikėjus) asmens duomenims tvarkyti. Jeigu pirkimo sutartyje nenustatytos kitos sąlygos, prieš pasitelkdamas naują arba pakeisdamas esamą subtiekėją (subteikėją), Tiekėjo grupė iš anksto apie tai raštu turi informuoti Užsakovą, pateikdamas planuojamo pasitelkti subtiekėjo (subteikėjo) rekvizitus ir kitą informaciją, susijusią su duomenų tvarkymo veikla, kurios pareikalaus Užsakovas. Kai Tiekėjo grupė konkrečiai asmens duomenų tvarkymo veiklai atlikti pasitelkia subtiekėją (subteikėją), Sutartimi (Priedu) tam kitam subtiekėjui (subteikėjui) nustatomos tos pačios duomenų apsaugos prievolės, kaip ir prievolės, nustatytos Tiekėjo grupei Sutartyje ir šiame Priede, visų pirma prievolė pakankamai užtikrinti, kad tinkamos techninės ir organizacinės priemonės bus įgyvendintos taip, kad asmens duomenų tvarkymas atitiktų asmens duomenų apsaugos teisės aktų reikalavimus. Kai tas subtiekėjas (subteikėjas) nevykdo duomenų apsaugos prievolių, Tiekėjo grupė išlieka visiškai atsakinga Užsakovui už to subtiekėjo (subteikėjo) prievolių vykdymą.

3.3. Užsakovas suteikia Tiekėjo grupei bendrą sutikimą pasitelkti kitus duomenų tvarkytojus („Pagalbiniai duomenų tvarkytojai") asmens duomenims, įskaitant, bet neapsiribojant, nurodytus 2 lentelėje, tvarkyti. Tiekėjo grupė turi informuoti Užsakovą apie numatomus pakeitimus, susijusius su papildomų Pagalbinių duomenų tvarkytojų pasitelkimu ar esamų pakeitimu, taip suteikiant Užsakovui galimybę prieštarauti tokiems pakeitimams. Kai Tiekėjo grupė konkrečiai asmens duomenų tvarkymo veiklai atlikti pasitelkia Pagalbinį duomenų tvarkytoją, Sutartimi (Priedu) tam kitam Pagalbiniam duomenų tvarkytojui nustatomos tos pačios duomenų apsaugos prievolės, kaip ir prievolės, nustatytos Tiekėjo grupei Sutartyje ir šiame Priede, visų pirma prievolė pakankamai užtikrinti, kad tinkamos techninės ir organizacinės priemonės bus įgyvendintos taip, kad asmens duomenų tvarkymas atitiktų asmens duomenų apsaugos teisės aktų reikalavimus. Kai Pagalbinis duomenų tvarkytojas nevykdo duomenų apsaugos prievolių, Tiekėjo grupė išlieka visiškai atsakinga Užsakovui už to Pagalbinio duomenų tvarkytojo prievolių vykdymą.

3.4. Tiekėjo grupė įsipareigoja, Užsakovui pareikalavus, nepagrįstai nedelsdamas liautis atlikti bet kokius asmens duomenų tvarkymo veiksmus, išskyrus saugojimą, ir atnaujinti veiksmus tik gavęs Užsakovo nurodymą.

3.5. Tiekėjo grupė įsipareigoja, gavusi rašytinį Užsakovo motyvuotą reikalavimą, ištrinti (arba grąžinti) asmens duomenis (jeigu tai padaryti techniškai įmanoma ir proporcinga) ir jų kopijas, kuriuos tvarko pirkimo sutarties ir šio Priedo pagrindu.

3.6. Tiekėjo grupė įsipareigoja, Užsakovui pareikalavus, pateikti visą informaciją, įrodančią su duomenų tvarkymu susijusių pareigų laikymąsi, ir padėti Užsakovui ir (ar) tretiesiems asmenims atlikti tvarkomų asmens duomenų auditą.

3.7. Šalys susitaria, jog asmens duomenys gali būti tvarkomi tik laikantis asmens duomenų apsaugos teisės aktų reikalavimų, nepažeidžiant duomenų subjektų teisių ir užtikrinant iš asmens duomenų apsaugos teisės aktų kylančių duomenų subjektų teisių tinkamą įgyvendinimą bei apsaugą.

2 lentelė

Pagalbinis duomenų tvarkytojas	Registruotas adresas	Duomenų tvarkymo apibūdinimas
Amazon Web Services, Inc. (AWS)	410 Terry Avenue North, Sietlas, Vašingtono valstija, 98109, JAV	AWS teikia debesų infrastruktūrą *Palantir* produktams.
Proofpoint, Inc.	892 Ross Drive, Saniveilas, Kalifornija, 94089, JAV	*Proofpoint* teikia įspėjimų ir užšifruotų pranešimų *Palantir Foundry* platformoje palaikymą.
Microsoft Corporation	One Microsoft Way, Redmondas, Vašingtono valstija, JAV, 98052	Teikia debesų infrastruktūrą, skirtą *Active Directory* tarnybai, reikalingai *CentralAuth* sistemai, patalpinti.

3.2. If provided by the Contract, the Customer gives the Supplier Group a general consent for engagement of subcontractors for personal data processing. Unless otherwise specified in the Contract, prior to engagement of a new subcontractor or replacement of current subcontractor, the Supplier Group shall inform the Customer in writing in advance by providing the details of the planned subcontractor as well as other information related to data processing activities requested by the Customer. Where the Supplier Group involves a subcontractor for a specific personal data processing activity, the Contract (Annex) imposes on that other subcontractor the same data protection obligations as those imposed on the Supplier Group by this Contract and Annex, in particular the obligation to ensure that proper technical and organisational measures will be implemented in such a way that the personal data processing complies with the requirements of the personal data protection legislation. Where the subcontractor fails to fulfil the data protection obligations, the Supplier Group shall remain fully liable to the Customer for the fulfilment of obligations of that subcontractor.

3.3. The Customer gives the Supplier Group a general consent for engagement of other processors ("Subprocessor(s)") for personal data processing, including but not limited to those referenced in Table 2. The Supplier Group shall inform Customer of any intended changes concerning the addition or replacement of Subprocessors, thereby giving Customer the opportunity to object to such changes. Where the Supplier Group involves a Subprocessor for a specific personal data processing activity, the Contract (Annex) imposes on that other Subprocessor the same data protection obligations as those imposed on the Supplier Group by this Contract and Annex, in particular the obligation to ensure that proper technical and organisational measures will be implemented in such a way that the personal data processing complies with the requirements of the personal data protection legislation. Where the Subprocessor fails to fulfil the data protection obligations, the Supplier Group shall remain fully liable to the Customer for the fulfilment of obligations of that Subprocessor.

3.4. The Supplier Group undertakes, at the Customer's request, to stop without undue delay any processing of personal data, except for storage, and to resume the operations only upon receipt of the Customer's instruction.

3.5. The Supplier Group undertakes, upon receipt of a written reasoned request of the Customer, to delete (or return) personal data (if technically possible and proportionate) and copies thereof which are processed based on this Contract and Annex.

3.6. The Supplier Group undertakes, at the Customer's request, to provide all information proving compliance with the obligations related to data processing and to assist the Customer and/or the third parties in auditing the processed personal data.

3.7. The Parties agree that personal data can be processed only in accordance with the requirements of the personal data protection legislation, without prejudice to the rights of data subjects and ensuring the proper implementation and protection of the rights of data subjects arising from personal data protection legislation.

Table 2

Subprocessor	Registered Address	Description of processing
Amazon Web Services, Inc. (AWS)	410 Terry Avenue North, Seattle, WA, 98109, USA	AWS provides the cloud infrastructure for Palantir products.
Proofpoint, Inc.	892 Ross Drive, Sunnyvale, CA, 94089, USA	Proofpoint supports the alerting and encrypted notification service in Palantir Foundry.
Microsoft Corporation	One Microsoft Way, Redmond WA, USA 98052	Provision of cloud infrastructure to host Active Directory for CentralAuth.

4. ASMENS DUOMENŲ SAUGUMAS IR TECHNINĖS BEI ORGANIZACINĖS PRIEMONĖS

4.1. Atsižvelgdamas į techninių galimybių išsivystymo lygį bei asmens duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus, taip pat į asmens duomenų tvarkymo keliamus įvairios tikimybės ir rimtumo pavojus duomenų subjektų teisėms ir laisvėms, Tiekėjo grupė įsipareigoja įgyvendinti tinkamas technines ir organizacines priemones, skirtas apsaugoti asmens duomenis nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, taip pat nuo bet kokio kito neteisėto tvarkymo ir užtikrinti duomenų subjekto teisių apsaugą. Tiekėjo grupė taip pat įsipareigoja imtis visų asmens duomenų saugumo priemonių, kurių reikalauja galiojantys teisės aktai.

4.2. Kadangi Tiekėjo grupė yra savo verslo srities profesionalė, turinti žinių ir patirties informacinių technologijų srityje, Tiekėjo grupė pati pasirinks ir nustatys technines ir organizacines priemones, reikalingas Priedo 2.1 papunktyje nurodytam tikslui bei tinkamam saugumui pasiekti, tačiau tokios priemonės bet kokiu atveju turi nepažeisti asmens duomenų apsaugos teisės aktų reikalavimų. Nepaisant to, Užsakovas turi teisę pateikti pasiūlymus / nurodymus Tiekėjo grupei dėl techninių ir organizacinių apsaugos priemonių taikymo. Tiekėjo grupė atsižvelgs į tokius Užsakovo pasiūlymus, juos išnagrinės ir pateiks Užsakovui motyvuotą atsisakymą įgyvendinti Užsakovo nurodymus arba nedelsdamas imsis šių veiksmų įgyvendinimo.

4.3. Nepaisant Priedo 4.1 ir 4.2 papunkčių nuostatų, tais atvejais, kai Užsakovas paveda Tiekėjo grupei tvarkyti asmens duomenis, Paslaugų teikėjui nuotoliniu būdu prisijungiant prie Sistemos ir (ar) kitų Užsakovo naudojamų informacinių sistemų, Užsakovas savo jėgomis ir lėšomis užtikrins maksimalų tokiam prisijungimui reikalingo ryšio saugumą ir taikys reikalingus bei tinkamus duomenų, jų srauto ir ryšio apsaugos įrankius bei priemones (pvz., šifravimą ar kt.).

4.4. Tiekėjo grupė užtikrina, kad asmens duomenis tvarkys tik įgalioti asmenys, įsipareigoję užtikrinti duomenų konfidencialumą.

4.5. Tiekėjo grupė, atsižvelgdama į saugomų asmens duomenų tvarkymo pobūdį ir turimą informaciją, įsipareigoja bendradarbiauti Užsakovui užtikrinant Bendrojo duomenų apsaugos reglamento 32–36 straipsniuose nustatytų prievolių laikymąsi.

4.6. Užsakovo prašymu, Tiekėjo grupė, atsižvelgdama į asmens duomenų tvarkymo pobūdį ir į technines galimybes, įsipareigoja suteikti turimą informaciją, reikalingą Užsakovui atsakyti į duomenų subjekto prašymus pasinaudoti duomenų subjekto teisėmis bei vykdyti kitus asmens duomenų apsaugos teisės aktų nustatytus reikalavimus.

5. KITI REIKALAVIMAI ASMENS IR KITŲ DUOMENŲ AR INFORMACIJOS TVARKYMUI

5.1. Teikdamas Sutartyje numatytas reikiamas infrastruktūros paslaugas, Tiekėjo grupė užtikrina, kad teikiamos paslaugos atitinka Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 5 d. nutarimu Nr. 818, VI skyriuje Reikalavimai elektroninės informacijos prieglobos paslaugų teikėjams ir skaitmeninių paslaugų teikėjams įvardytus reikalavimus:

5.1.1. ne rečiau kaip kartą per dvejus metus arba po esminių organizacinių ar sisteminių pokyčių organizuoja ir atlieka rizikos vertinimą. Šį rizikos vertinimą elektroninės informacijos prieglobos paslaugų teikėjai ir skaitmeninių paslaugų teikėjai turi teisę atlikti kartu su veiklos rizikos ir (arba) informacinių technologijų saugos atitikties vertinimu;

5.1.2. kartu su viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjais imasi reikiamų priemonių kibernetiniam saugumui užtikrinti;

5.1.3. įgyvendina organizacines ir technines priemones, užtikrinančias jų elektroninės informacijos prieglobos ar skaitmeninėms paslaugoms teikti naudojamų sistemų ir įrangos kibernetinį saugumą;

4. PERSONAL DATA SECURITY, TECHNICAL AND ORGANIZATIONAL MEASURES

4.1. Taking into account the level of technical development and the nature, scope, context and objectives of the personal data processing as well as the personal data processing risks of various probabilities and seriousness to the rights and freedoms of data subjects, the Supplier Group undertakes to implement appropriate technical and organizational measures to protect personal data from accidental or unlawful destruction, alteration, disclosure as well as any other unlawful processing and to ensure the protection of the rights of the data subject. The Supplier Group also undertakes to take all personal data security measures required by applicable laws.

4.2. Whereas the Supplier Group is a professional in its field of business having knowledge and experience in the field of information and technologies, the Supplier Group will choose and determine the technical and organizational measures necessary to achieve the purpose specified in Point 2.1 of the Annex and to ensure proper security; however, in any case, such measures must not violate the requirements of the personal data protection legislation. Nevertheless, the Customer has the right to submit offers/instructions to the Supplier Group regarding the application of technical and organizational security measures. The Supplier Group will consider such offers of the Customer, examine them and provide the Customer with a reasoned refusal to implement the instructions of the Customer or will immediately start the implementation of these actions.

4.3. Notwithstanding the provisions of Points 4.1 and 4.2 of the Annex, in cases when the Customer has delegated the personal data processing to the Supplier Group, when the Service Provider remotely connects to the System and/or other information systems used by the Customer, the Customer, at the Customer's own effort and expense, shall ensure the maximum security of the connection required and apply the necessary and proper tools and measures (e.g. encryption, etc.) to protect the data, their flow and connection.

4.4. The Supplier Group shall ensure that personal data are processed only by authorized persons committed to ensure the confidentiality of the data.

4.5. By taking into account the nature of the processing of the stored personal data and the available information, the Supplier Group undertakes to cooperate with the Customer in ensuring compliance with the obligations set out in Articles 32–36 of the General Data Protection Regulation.

4.6. At the request of the Customer, the Supplier Group, taking into account the nature of personal data processing and technical possibilities, undertakes to provide available information necessary for the Customer to respond to the data subject's requests to exercise the data subject's rights and fulfil other requirements of personal data protection legislation.

5. OTHER REQUIREMENTS FOR PERSONAL AND OTHER DATA OR INFORMATION PROCESSING

5.1. In providing the necessary infrastructure services under the Contract, the Supplier Group shall ensure that the services provided comply with the requirements set in Chapter VI "Requirements for Electronic Information Hosting Service Providers and Digital Service Providers" of the Description of Organizational and Technical Cyber Security Requirements Applicable to Cyber Security Entities, approved by Resolution No 818 of 5 August 2018 of the Government of the Republic of Lithuania:

5.1.1. To organize and perform the risk assessment at least once every two years or following major organizational or systemic changes. The electronic information hosting providers and digital service providers are entitled to carry out this risk assessment together with activity risk assessment and/or assessment of the compliance of information technologies security.

5.1.2. In cooperation with the providers of public communications networks and/or public electronic communications services, to take necessary measures to ensure cyber security.

5.1.3. To implement organizational and technical measures that ensure cyber security of the systems and equipment used for provision of digital services or electronic information hosting.

5.1.4. tvirtina ir po esminių organizacinių ar sisteminių pokyčių atnaujina savo paslaugų kibernetinio saugumo valdymo taisykles, o Nacionalinio kibernetinio saugumo centro reikalavimu jas pateikia Nacionaliniam kibernetinio saugumo centrui. Elektroninės informacijos prieglobos paslaugų ar skaitmeninių paslaugų kibernetinio saugumo valdymo taisyklėse nurodoma:

5.1.4.1. kibernetiniams incidentams valdyti reikalingų priemonių aprašymai;

5.1.4.2. elektroninės informacijos prieglobos paslaugų ar skaitmeninių paslaugų nepertraukiamo teikimo užtikrinimo planas ir jo taikymo sąlygos bei maksimalus leistinas paslaugos neveikimo laikas;

5.1.4.3. už kibernetinių incidentų valdymą atsakingų asmenų funkcijos ir atsakomybė;

5.1.4.4. viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugoms teikti naudojamų sistemų ir įrangos stebėsenos, patikrinimo, testavimo bei auditavimo tvarka ir sąlygos;

5.1.4.5. atitiktis Lietuvos ir tarptautiniams standartams, apibūdinantiems kibernetinį saugumą ar saugų elektroninės informacijos tvarkymą;

5.1.5. neatlygintinai informuoja elektroninės informacijos prieglobos ar skaitmeninių paslaugų gavėjus apie nustatytus kibernetinius incidentus, susijusius su elektroninės informacijos prieglobos ar skaitmeninėmis paslaugomis, priskirtus prie turinčių didelį poveikį, nustatytą Nacionaliniame kibernetinių incidentų valdymo plane;

5.1.6. ne vėliau kaip prieš penkias darbo dienas informuoja elektroninės informacijos prieglobos paslaugų ar skaitmeninių paslaugų gavėjus ir Nacionalinį kibernetinio saugumo centrą apie numatomus planinius darbus, kuriuos atliekant yra tikimybė sutrikdyti elektroninės informacijos prieglobos ar skaitmeninių paslaugų kibernetinį saugumą;

5.1.7. informuoja elektroninės informacijos prieglobos ar skaitmeninių paslaugų gavėjus, kuriose šalyse gali būti saugoma jų elektroninė informacija, kuri kuriama, tvarkoma ar pateikta saugoti naudojantis elektroninės informacijos prieglobos ar skaitmeninėmis paslaugomis, ir kokiais atvejais tokia informacija perkeliama į kitas šalis;

5.1.8. nustato elektroninės informacijos prieglobos ar skaitmeninių paslaugų gavėjų įspėjimo apie elektroninės informacijos prieglobos ar skaitmeninių paslaugų kibernetinio saugumo pažeidimus tvarką ir kokių veiksmų tokiu atveju privalo imtis elektroninės informacijos prieglobos ar skaitmeninių paslaugų gavėjai ir (ar) teikėjai;

5.1.9. viešai skelbia rekomendacijas elektroninės informacijos prieglobos ar skaitmeninių paslaugų gavėjams apie priemones kibernetiniam saugumui užtikrinti naudojantis elektroninės informacijos prieglobos ar skaitmeninėmis paslaugomis.

5.2. Tiekėjo grupė užtikrina, kad visa Užsakovo elektroninė informacija, kuri yra kuriama, tvarkoma ar pateikta saugoti naudojantis Tiekėjo grupės paslaugomis, yra saugojama Europos Sąjungoje.

5.3. Prireikus Tiekėjo grupė gali tvarkyti asmeninius duomenis pasauliniu mastu. Tiek, kiek tokia visuotinė prieiga yra susijusi su asmens duomenų, atsiradusių Europos Sąjungoje ir (arba) Europos ekonominėje erdvėje (EEE), perdavimu Tiekėjo grupei arba jo Pagalbiniams duomenų tvarkytojams, esantiems ne Europos Sąjungoje ir (arba) Europos ekonominėje erdvėje (EEE), kurie nėra gavę privalomo Europos Komisijos sprendimo dėl tinkamumo, tokiam duomenų perdavimui taikomos ES standartinės sutartinės sąlygos, susijusios su asmeninių duomenų perdavimu trečiose šalyse įsteigtiems duomenų tvarkytojams pagal Europos Parlamento ir Tarybos direktyvą 95/46/EB, arba visos paskesnės standartinės sutartinės sąlygos, kurios gali būti priimtos vadovaujantis ES Komisijos sprendimu (EU Model Clauses), įtrauktos į šį Priedą nuorodos būdu. Įgyvendindamos ES standartinių sutartinių sąlygų (angl. EU Model Clauses) I ir II priedus, Šalys susitaria, kad (i) Užsakovas veiks kaip duomenų eksportuotojas savo ir bet kurio savo grupės subjekto vardu, (ii) Tiekėjo grupė veiks kaip duomenų importuotojas, (iii) visi trečiųjų šalių Pagalbiniai duomenų tvarkytojai (išskyrus Tiekėjo grupę) veiks kaip „subrangovai“, vadovaujantis ES standartinių sutartinių sąlygų 11 punktu, (iv) duomenų subjektai, duomenų kategorijos ir tvarkymo veikla yra nustatyta šiame Priede (ypač 2.6 punkte), ir (V) „Palantir Gruop“ ėmėsi ir toliau taikys tinkamas technines ir organizacines asmens duomenų apsaugos priemones, įskaitant Sutartyje nustatytus reikalavimus.

5.1.4. To approve the cyber security management rules, update them following the significant organizational or systemic changes and submit them to the National Cyber Security Centre, at the request of the National Cyber Security Centre. The cyber security management rules for electronic information hosting or digital services provide:

5.1.4.1. Descriptions of the measures required for cyber incidents management.

5.1.4.2. A plan for ensuring the uninterrupted provision of electronic information hosting or digital services and conditions for application thereof as well as the maximum permissible service downtime.

5.1.4.3. Functions and responsibilities of the persons responsible for managing cyber incidents.

5.1.4.4. Procedures and conditions for monitoring, checking, testing and auditing of systems and equipment used for the provision of public communications networks and/or public electronic communications services.

5.1.4.5. Compliance with Lithuanian and international standards for cyber security or secure electronic information processing.

5.1.5. To inform, free of charge, the recipients of electronic information hosting or digital services about identified cyber incidents related to electronic information hosting or digital services classified as having a significant impact, as provided in the National Cyber Incident Management Plan.

5.1.6. To notify the recipients of electronic information hosting or digital services and the National Cyber Security Centre, not later than five working days in advance, of the scheduled work which may disrupt the cyber security of electronic information hosting or digital services.

5.1.7. To inform the recipients of electronic information hosting or digital services in which countries their electronic information that is created, managed or submitted for storage by using electronic information hosting or digital services can be stored, and in which cases such information is transferred to other countries.

5.1.8. To establish the procedure for warning the recipients of electronic information hosting or digital services about breaches of cyber security of electronic information hosting or digital services and actions to be taken by the recipients and/or providers of electronic information hosting or digital services in such cases.

5.1.9. To make public recommendations for the recipients of the electronic information hosting or digital services on measures for ensuring cyber security when using electronic information hosting or digital services.

5.2. The Supplier Group shall ensure that all electronic information of the Customer that is created, processed or submitted for storage through the services of the Supplier Group is stored in the European Union.

5.3. The Supplier Group may process personal data on a global basis as necessary. To the extent such global access involves a transfer of personal data originating from the European Union and/or the European Economic Area ("EEA"), to the Supplier Group or its Subprocessors located in countries outside the European Union and/or EEA that have not received a binding adequacy decision by the European Commission, such transfers shall be subject to the terms of the EU standard contractual clauses for the Transfer of Personal Data to Processors established in Third Countries under the Directive 95/46/EC, or any successor standard contractual clauses that may be adopted pursuant to an EU Commission decision (the "EU Model Clauses") incorporated into this Annex by reference. For the purposes of Appendix I and II of the EU Model Clauses, the Parties agree that (i) the Customer will act as the data exporter on its own behalf and on behalf of any of its group entities, (ii) the Supplier Group will act as the data importers, (iii) any third party Subprocessors (excluding the Supplier Group) will act as 'subcontractors' pursuant to Clause 11 of the EU Model Clauses, (iv) the data subjects, categories of data and processing activities shall be as set out in this Annex (and in particular clause 2.6), and (v) Palantir Group has adopted and will maintain appropriate technical and organizational security measures in respect of the personal data, including such requirements set out in the Contract.

6. ASMENS DUOMENŲ SAUGUMO PAŽEIDIMAI

6.1. Asmens duomenų saugumo pažeidimo atveju ar Tiekėjo grupė pagrįstai įtariant tokį pažeidimą, Tiekėjas nedelsdamas, tačiau bet kokiu atveju ne vėliau nei per 24 val. po to, kai sužino apie tai, raštu informuoja apie tai Užsakovą ir pateikia turimą informaciją bei duomenis, susijusius su tokiu pažeidimu.

6.2. Užsakovui pareikalavus, Tiekėjo grupė, atsižvelgdamas į technines galimybes, nepagrįstai nedelsdamas pateiks Užsakovui papildomus reikalaujamus dokumentus, informaciją ir duomenis, reikalingus tam, kad Užsakovas galėtų nustatyti ir (ar) patikrinti asmens duomenų saugumo pažeidimo faktą, ištirti jo aplinkybes ir imtis neatidėliotinų priemonių pažeidimui pašalinti ar neigiamoms jo pasekmėms sumažinti.

7. TIEKĖJO GRUPĖS ATSAKOMYBĖ IR GINČŲ SPRENDIMO TVARKA

7.1. Tiekėjas įsipareigoja atlyginti visus Užsakovo patirtus nuostolius, atsiradusius dėl Tiekėjo grupės šio pirkimo sutarties priedo sąlygų pažeidimo ar netinkamo vykdymo.

7.2. Kiekvienas ginčas, nesutarimas ar reikalavimas, kylantis iš šio Sutarties priedo ar susijęs su šiuo Sutarties priedu, jo pažeidimu, turi būti sprendžiamas derybų keliu. Jeigu per 15 dienų nuo jo kilimo šalims nepavyksta susitarti, toks ginčas, nesutarimas ar reikalavimas sprendžiamas Lietuvos Respublikos teisme.

8. ŠALIŲ ADRESAI, REKVIZITAI IR PARAŠAI

UŽSAKOVAS

Lietuvos statistikos departamentas
Gedimino pr. 29, LT-01500 Vilnius
Įmonės kodas: 188600177
PVM mokėtojo kodas: nėra
A. s. Nr. LT51 7044 0600 0111 1285
AB SEB BANKAS
Banko kodas 70440
Tel. +370 5 236 4822
El. p. info@stat.gov.lt
http://www.stat.gov.lt

Generalinė direktorė Jūratė Petrauskienė

TIEKĖJAS

Palantir Technologies UK, Ltd.
New Penderel House
283-288 High Holborn
London, WC1V 7HP
Įmonės kodas: 7042994
PVM mokėtojo kodas: GB 101 2291 78
Bankas: JP Morgan Chase
Sąskaitos savininkas: Palantir Technologies UK, Ltd.
A. s. Nr.: 41036031
IBAN: GB36CHAS60924241036031
SWIFT: CHASGB2L
Tel. +44 7408 886228
El. p. legalnotices@palantir.com

Matt Long, įgaliotasis asmuo

6. PERSONAL DATA BREACH

6.1. In the event of personal data breach or if the Supplier Group reasonably suspects such a breach, the Supplier Group shall immediately, but in any case not later than within 24 hours after becoming aware thereof, inform the Customer in writing and provide the available information and data related to such breach.

6.2. At the Customer's request, the Supplier Group shall, taking into account technical possibilities and without undue delay, provide the Customer with the required additional documents, information and data necessary to enable the Customer to identify and/or verify the fact of personal data breach, investigate the circumstances and take immediate measures to eliminate the breach or reduce negative consequences thereof.

7. RESPONSIBILITY OF THE SUPPLIER GROUP AND DISPUTE RESOLUTION

7.1. The Supplier undertakes to indemnify all losses incurred by the Customer due to the Supplier Group's violation or improper implementation of the terms and conditions of the Annex to the Contract.

7.2. Any dispute, disagreement or claim arising out of or relating to this Annex to the Contract or violation thereof shall be resolved by negotiation. If the matter cannot be resolved through negotiations within 15 days of the commencement of the dispute, such dispute, disagreement or claim will be settled by the court of the Republic of Lithuania.

8. ADDRESSES, DETAILS AND SIGNATURES OF THE PARTIES

CUSTOMER

The Lithuanian Department of Statistics (Statistics Lithuania)
Gedimino ave. 29, LT-01500 Vilnius
Company Number: 188600177
VAT Number: None
Account Number: LT51 7044 0600 0111 1285
Bank Name: AB SEB BANKAS
Bank Code: 70440
Phone No. +370 5 236 4822
E-mail: info@stat.gov.lt
http://www.stat.gov.lt

Jūratė Petrauskienė, Director General

SUPPLIER

Palantir Technologies UK, Ltd.
New Penderel House
283-288 High Holborn
London, WC1V 7HP
Company number: 7042994
VAT number: GB 101 2291 78
Bank Name: JP Morgan Chase
Account Holder: Palantir Technologies UK, Ltd.
Account Number: 41036031
IBAN: GB36CHAS60924241036031
SWIFT: CHASGB2L
Phone No. +44 7408 886228
E-mail: legalnotices@palantir.com

Matt Long, Authorised Signatory