

**VALSTYBĖS DUOMENŲ VALDYSENOS  
INFORMACINĖS SISTEMOS LICENCIJOS  
(PALANTIR FOUNDRY) PRATĖSIMO  
PIRKIMO SUTARTIS**

2021 m. lapkričio 24 d., Nr. \_\_\_\_\_  
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 Tado Rudzevičiaus, 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. 571533 „Valstybės duomenų valdyosenos informacinės sistemos licencijos (Palantir Foundry) pratęsimo pirkimas“ vykdyto neskelbiamų derybų būdu (toliau – pirkimas) rezultatus, sudarė šią pirkimo sutartį (toliau – Sutartis):

**1. SUTARTIES DALYKAS**

1.1. Tiekėjas įsipareigoja pratęsti Valstybės duomenų valdyosenos informacinės sistemos tęstinumui užtikrinti reikalingos Duomenų valdymo platformos (toliau – Palantir Foundry) licenciją, įskaitant platformos palaikymą, kartu su infrastruktūros paslaugomis (toliau – prekės) tokia apimtimi ir sąlygomis, kaip detalizuota Sutarties 2 ir 3 skyriuose ir prieduose „Techninė specifikacija“ (toliau – Techninė specifikacija, arba 1 priedas) o Užsakovas įsipareigoja atsiskaityti su Tiekėju Sutarties sąlygų 4 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 platformos Palantir Foundry licencijos pratęsimas turi įsigalioti 2021 m. gruodžio 6 d. ir galioti 12 mėn., o pratęsus Sutartį Sutarties 5.1 punkte nustatyta tvarka, iki sutarties pratęsimo termino pabaigos;

2.1.1.2. duomenų valdymo platformos Palantir Foundry licencija turi šias maksimalias metines išteklių naudojimo ribas. Šios išteklių naudojimo ribos yra metinės ir negali būti perkeliamos tarp skirtingų metų:

2.1.1.2.1. **Pirmieji metai (2021–2022):**

Platformos išteklių naudojimo ribos

| Platformos išteklių tipas             | Kiekis  | Matavimo vienetas   |
|---------------------------------------|---------|---------------------|
| Paketinis skaičiavimas                | 679 487 | skaičiavimo valanda |
| Interaktyvus skaičiavimas             | 14 902  | skaičiavimo valanda |
| Vidutinė sunaudojama disko vieta      | 44 821  | GB per mėnesį       |
| Vidutinė sunaudojama indeksuota vieta | 123     | GB per mėnesį       |

Platformos įgyvendinimo paslaugų naudojimo ribos

|                        | Kiekis | Matavimo vienetas |
|------------------------|--------|-------------------|
| Įgyvendinimo paslaugos | 3 528  | valanda           |

2.1.1.2.2. **Antrieji metai (2022–2023):**

Platformos išteklių naudojimo ribos

| Platformos išteklių tipas             | Kiekis  | Matavimo vienetas   |
|---------------------------------------|---------|---------------------|
| Paketinis skaičiavimas                | 759 426 | skaičiavimo valanda |
| Interaktyvus skaičiavimas             | 16 656  | skaičiavimo valanda |
| Vidutinė sunaudojama disko vieta      | 50 094  | GB per mėnesį       |
| Vidutinė sunaudojama indeksuota vieta | 137     | GB per mėnesį       |

**RENEWAL OF THE LICENSE OF THE STATE DATA  
GOVERNANCE INFORMATION SYSTEM (PALANTIR  
FOUNDRY) PURCHASE CONTRACT**

2021 m. November 24 d., No. \_\_\_\_\_  
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 Tadas Rudzevičius, 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. 571533 “Renewal of the license of the State Data Governance Information System (Palantir Foundry)” carried out by the public authority CPO LT in the form of a private negotiation (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 (“Palantir Foundry”) necessary to ensure the continuity of the State Data Governance Information System within such scope and under such conditions as laid out in section 2 and 3 of the Contract and annexes titled “Technical Specification” (hereinafter – technical specification or Annex 1) while the Customer shall carry out the payment to the Supplier in accordance with the terms and conditions laid out in section 4 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 licence of Palantir Foundry shall come into force from 2021 December 6 and shall remain valid for no less than 12 (twelve) months and, in case of contract extension, in accordance with section 5.1 of the Contract, until the end of the Contract extension term;

2.1.1.2. the licence of Palantir Foundry shall include the following maximum annual resource usage limits. These resource usage limits are annual only and may not be carried over between contract years:

2.1.1.2.1. **First year (2021–2022):**

Platform Resource Usage Limit:

| Platform Resource Type  | Allocation | Unit       |
|-------------------------|------------|------------|
| Batch compute           | 679,487    | compute-hr |
| Interactive compute     | 14,902     | compute-hr |
| Average disk storage    | 44,821     | GB-month   |
| Average indexed storage | 123        | GB-month   |

Implementation Services Usage Limit

|                         | Allocation | Unit  |
|-------------------------|------------|-------|
| Implementation Services | 3,528      | Hours |

2.1.1.2.2. **Second year (2022–2023):**

Platform Resource Usage Limit

| Platform Resource Type  | Allocation | Unit       |
|-------------------------|------------|------------|
| Batch compute           | 759,426    | compute-hr |
| Interactive compute     | 16,656     | compute-hr |
| Average disk storage    | 50,094     | GB-month   |
| Average indexed storage | 137        | GB-month   |

## Platformos įgyvendinimo paslaugų naudojimo ribos

|                        | Kiekis | Matavimo vienetas |
|------------------------|--------|-------------------|
| Įgyvendinimo paslaugos | 2 520  | valanda           |

## 2.1.1.2.3. Tretieji metai (2023–2024):

## Platformos išteklių naudojimo ribos

| Platformos išteklių tipas             | Kiekis  | Matavimo vienetas   |
|---------------------------------------|---------|---------------------|
| Paketinis skaičiavimas                | 799 396 | skaičiavimo valanda |
| Interaktyvus skaičiavimas             | 17 532  | skaičiavimo valanda |
| Vidutinė sunaudojama disko vieta      | 52 730  | GB per mėnesį       |
| Vidutinė sunaudojama indeksuota vieta | 144     | GB per mėnesį       |

## Platformos įgyvendinimo paslaugų naudojimo ribos

|                        | Kiekis | Matavimo vienetas |
|------------------------|--------|-------------------|
| Įgyvendinimo paslaugos | 2 016  | valanda           |

2.1.1.3. **Platformos išteklių konvertavimas:** bet kuriais konkrečiais metais Užsakovas gali pakeisti bet kurios platformos išteklių rūšies paskirstymą (kaip nurodyta aukščiau Sutarties 2.1.1.2.1–2.1.1.2.3 punktuose kiekvienais atitinkamais metais), naudodamas žemiau nurodytą koeficientų lentelę. Pavyzdžiui, 100 valandų interaktyvaus skaičiavimo gali būti panaudotos kaip 1521,74 valandos paketinio skaičiavimo. Konvertavimas tarp platformos išteklių tipų atliekamas automatiškai, jei Užsakovas viršija bet kurio atskiro platformos išteklių tipo ribą. Jei Užsakovas viršys bendrą platformos išteklių ribą bet kuriais metais, papildomus platformos išteklius reikės įsigyti pagal atskirą susitarimą.

| Platformos išteklių tipas             | Koeficientas | Matavimo vienetas   |
|---------------------------------------|--------------|---------------------|
| Paketinis skaičiavimas                | 2,30         | skaičiavimo valanda |
| Interaktyvus skaičiavimas             | 35,00        | skaičiavimo valanda |
| Vidutinė sunaudojama disko vieta      | 0,07         | GB per mėnesį       |
| Vidutinė sunaudojama indeksuota vieta | 2,00         | GB per mėnesį       |

2.1.1.4. **Įgyvendinimo paslaugų konvertavimas:** Šalims susitarus, Užsakovas nuo 2 (antrų) metų gali pasirinkti įgyvendinimo paslaugas (pagal žemiau nurodytą koeficientą) konvertuoti į platformos išteklius Sutarties 2.1.1.3 punkte nurodytais koeficientais. Minimalus konvertavimo kiekis yra 504 valandos. Pavyzdžiui, 2 (antrais) metais Užsakovas nusprendžia 504 valandas įgyvendinimo paslaugų konvertuoti į 54344.35 valandas paketinio skaičiavimo.

|                        | Koeficientas | Matavimo vienetas |
|------------------------|--------------|-------------------|
| Įgyvendinimo paslaugos | 248,00       | valanda           |

2.1.1.5. duomenų valdymo platformos palaikymas ir reikiamų infrastruktūros paslaugų teikimas turi būti užtikrintas ne trumpiau nei nustatyta Sutarties 2.1.1.1 punkte;

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 priimtus įsipareigojimus;

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

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:

## Implementation Services Usage Limit

|                         | Allocation | Unit  |
|-------------------------|------------|-------|
| Implementation Services | 2,520      | Hours |

## 2.1.1.2.3. Third year (2023–2024)

## Year 3 Platform Resource Usage Limit

| Platform Resource Type  | Allocation | Unit       |
|-------------------------|------------|------------|
| Batch compute           | 799,396    | compute-hr |
| Interactive compute     | 17,532     | compute-hr |
| Average disk storage    | 52,730     | GB-month   |
| Average indexed storage | 144        | GB-month   |

## Implementation Services Usage Limit

|                         | Allocation | Unit  |
|-------------------------|------------|-------|
| Implementation Services | 2,016      | Hours |

2.1.1.3. **Platform Resource Conversion:** In any given contract year the Customer may swap between its allocation of any Platform Resource Type (as set out above at 2.1.1.2.1–2.1.1.2.3 for each respective contract year) in accordance with the table below. For example: 100 hours of Interactive Compute could instead be utilised as 1521.74 hours of Batch Compute. A conversion between Platform Resource Types shall automatically be made in the event that the Customer exceeds the limit on any individual Platform Resource Type. Should the Customer exceed the total Platform Resource limits in any contract year, additional Platform Resources will need to be purchased subject to a separate agreement.

| Platform Resource Type  | Coefficient | Unit       |
|-------------------------|-------------|------------|
| Batch compute           | 2.30        | compute-hr |
| Interactive compute     | 35.00       | compute-hr |
| Average disk storage    | 0.07        | GB-month   |
| Average indexed storage | 2.00        | GB-month   |

2.1.1.4. **Implementation Services Conversion:** Subject to agreement between the parties, the Customer may choose from Year 2 onwards to convert Implementation Services (in accordance with the table below) into Platform Resources in line with the coefficients set out in the above table in 2.1.1.3. The minimum conversion amount shall be 504 hours. For example: In Year 2 the Customer could elect to convert 504 hours of Implementation Services to 54,344.35 hours of Batch Compute.

|                         | Coefficient | Unit  |
|-------------------------|-------------|-------|
| Implementation Services | 248.00      | Hours |

2.1.1.5. the data management platform support and provision of the required infrastructure services shall be ensured for no less than the period specified in section 2.1.1.1 above;

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. The parties agree that the obligations for the Supplier set forth in section 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. 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 nustatytais 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 teikimo procesą tiek, kiek tai susiję su prekių teikimu, pareikšti Tiekėjui pastabas ir pasiūlymus dėl prekių teikimo. 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.

### 3. LICENCIJOS SĄLYGOS

- 3.1. Leidžiami naudojimo atvejai: Tiekėjas leidžia Užsakovui naudoti Palantir Foundry licenciją šiais atvejais:
- 3.1.1. oficialiajai statistikai rengti;
- 3.1.2. COVID-19 pandemijos valdyti ir stebėti;
- 3.1.3. neteisėtai migracijai valdyti ir stebėti;
- 3.1.4. pasirengimui galimai avarijai / incidentui Astravo atominėje elektrinėje stebėti; ir
- 3.1.5. teisės aktuose numatytam valstybės duomenų atvėrimui ir pakartotiniam panaudojimui užtikrinti;
- 3.2. Papildomi naudojimo atvejai: vykdydamas Sutartį, Užsakovas siekia panaudoti Palantir Foundry licenciją bet kokiems papildomiems naudojimo atvejams, neįvardytiems Sutartyje, šalys susitaria dėl šių sąlygų, taikomų kiekvienam papildomo naudojimo atvejo prašymui nagrinėti:
- 3.2.1. Šalys raštu tarpusavyje susitaria dėl bet kokio naujo naudojimo atvejo ir dokumentais pagrindžia aiškiai apibrėžtą projekto tikslą, taikymo sritį, trukmę ir norimą rezultatą.
- 3.2.2. Kiekvienos šalies atsakingi darbuotojai peržiūri kiekvieno naujo naudojimo atvejo pagrįstumą atsižvelgdami į Sutartį, Tiekėjo taikomą Elgesio kodeksą ([https://s26.q4cdn.com/381064750/files/doc\\_downloads/governance/Code-of-Conduct.pdf](https://s26.q4cdn.com/381064750/files/doc_downloads/governance/Code-of-Conduct.pdf)), galiojančius teisės aktus bei etinius, politinius ir teisėtumo aspektus.
- 3.2.3. Tiekėjas negali nepagrįstai sulaikyti / neduoti savo pritarimo Užsakovui tęsti / vykdyti naują naudojimo atvejį, o atsisakymo atveju aiškiai raštu pagrindžia tokio atsisakymo priežastis.
- 3.2.4. Užsakovas su Tiekėju raštu patvirtina aiškią projekto komandos struktūrą, įskaitant: (i) vyresnįjį projekto rėmėją; ii) projekto savininką (atsakingą už sprendimų priėmimą); iii) techninį vadovą (atsakingą už techninį įgyvendinimą); iv) duomenų valdytoją (atsakingą už prieigos prie duomenų koordinavimą ir duomenų struktūros / schemų dalyko ekspertą); ir v) duomenų apsaugos pareigūną (atsakingą už prieigos kontrolę ir duomenų apsaugą).
- 3.2.5. Užsakovas užtikrina, kad Tiekėjui būtų lengvai prieinami visi atitinkamam naudojimo atvejui reikalingi duomenys, kartu su visais reikalingais vidiniais ir išoriniais patvirtinimais.
- 3.2.6. Užsakovas neatsako už jokiais papildomas licencijos išlaidas, susijusias su bet koku nauju naudojimo atveju, patvirtintu pagal Sutartį.
- 3.3. Papildomos autorizuotos paskyros: Tiekėjas suteiks Užsakovui galimybę suteikti ir sukurti paskyras tam, kad galima būtų naudotis Produktais (toliau – paskyros), Užsakovo darbuotojams, atstovams, nepriklausomiems rangovams ir (arba) nepriklausomų organizacijų

- 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 section 2.4.2 of the Contract is an essential part of the conditions of the Contract.

### 3. LICENCE TERMS

- 3.1. Permitted Use Cases: The Supplier permits the Customer to use the Palantir Foundry licence for the following use cases:
- 3.1.1. Preparation of Official Statistics;
- 3.1.2. Management and monitoring of COVID-19 pandemic;
- 3.1.3. Management and monitoring of illegal migration;
- 3.1.4. Monitoring of preparedness for a potential accident/incident at Astravyets Nuclear Power Plant; and
- 3.1.5. Ensuring the opening and re-use of state data, to the extent provided for in legislation.
- 3.2. Additional Use Cases: Whereas, in implementation of the Contract, the Customer seeks to utilise the Palantir Foundry licence for any additional use cases, which fall outside of the scope of the Contract, the parties hereby agree on the following terms and conditions for processing each request for an additional use case:
- 3.2.1. The parties shall mutually agree in writing on any new use case and shall document the clearly defined project purpose scope, duration and desired outcome.
- 3.2.2. Each party's responsible teams shall review the validity of each new use case in line with the Contract, Supplier's Code of Conduct ([https://s26.q4cdn.com/381064750/files/doc\\_downloads/governance/Code-of-Conduct.pdf](https://s26.q4cdn.com/381064750/files/doc_downloads/governance/Code-of-Conduct.pdf)) and as may be updated from time to time), current legislation, and taking into account any ethical, political and legal concerns.
- 3.2.3. Supplier shall not unreasonably withhold its consent for the Customer to proceed with a new use case and shall provide clear explanation in writing for any refusals given.
- 3.2.4. Customer shall confirm a clear project team structure with the Supplier in writing, inclusive of: (i) senior project sponsor; (ii) project owner (responsible for decision making); (iii) technical lead (responsible for technical implementation); (iv) data steward (responsible for coordinating data access and subject matter expert on data structure / schemas); and (v) data protection officer (responsible for access controls and data protection).
- 3.2.5. Customer shall ensure that all required data for the respective use case will be readily accessible to Supplier, complete with all necessary internal and external approvals, as applicable.
- 3.2.6. Customer shall not be responsible for any additional licence costs for any new use case approved under the Contract.
- 3.3. Additional Authorised Accounts: Supplier will provide Customer with the capability to provision and establish accounts to access the Products (*as defined below*) ("Accounts") for Customer's employees, agents, independent contractors and/or representatives of independent organisations (*such organisations subject to prior written approval of*

atstovams (tokioms organizacijoms reikalingas išankstinis rašytinis Tiekėjo sutikimas), kuriems reikia turėti prieigą prie Tiekėjo informacijos, medžiagos, dokumentų ir (arba) programinės įrangos (įskaitant, bet neapsiribojant, Duomenų valdymo platformą (Palantir Foundry)) (Produktai) Užsakovo vardu tikslais, numatytais šia Sutartimi. Užsakovas turi užtikrinti, kad šie paskyrų naudotojai yra pasirašę konfidencialumo susitarimus arba kitu būdu susaistyti konfidencialumo įsipareigojimų, kurie būtų ne mažiau ribojantys nei nurodyta 3 priede. Užsakovas turi informuoti kiekvieną naudotoją apie jo įsipareigojimus ir užtikrinti, kad kiekvienas naudotojas visada laikytųsi Sutarties sąlygų. Atsakomybė už visus tokių naudotojų veiksmus, įskaitant Sutarties pažeidimus, tenka tik Užsakovui.

3.4. Nuosavybė: Tiekėjas pasilieka visas teises, nuosavybės ir turtinę teisę, įskaitant visas intelektinės nuosavybės teises, į Produktus, atnaujinimus ir bet kokią kitą susijusią Tiekėjo pateiktą dokumentaciją ar medžiagą. Užsakovas pasilieka visas teises, nuosavybės ir turtinę teisę į visus duomenis, importuotus, kaupiamus ir tvarkomus Produkte (toliau – turinys). Tiekėjas gali naudoti, perduoti, atskleisti ar atkurti turinį tik tiek, kiek tai būtina, teikiant teikti produktus, prekes ir paslaugas, Užsakovui pagal šią Sutartį.

#### 4. SUTARTIES KAINA IR ATSISKAITYMO TVARKA

4.1. 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), 10.3 punktu, Sutarčiai taikoma fiksuotos kainos su peržiūra kainodara.

4.2. Sutarties kaina už Sutarties 1.1 punkte nurodytas prekes:

| Sutarties metai     | Pirkimo objektas   | Kaina Eur be PVM | Kaina Eur su PVM |
|---------------------|--|------------------|------------------|
| 1 metai (2021–2022) | Palantir Foundry licencija (kartu su infrastruktūros, platformos palaikymo bei įgyvendinimo paslaugomis) | 3 000 000,00     | 3 630 000,00     |
| 2 metai (2022–2023) | Palantir Foundry licencija (kartu su infrastruktūros, platformos palaikymo bei įgyvendinimo paslaugomis) | 3 000 000,00     | 3 630 000,00     |
| 3 metai (2023–2024) | Palantir Foundry licencija (kartu su infrastruktūros, platformos palaikymo bei įgyvendinimo paslaugomis) | 3 000 000,00     | 3 630 000,00     |

4.3. Sutarties kainą įskaičiuoti visi Tiekėjo mokami mokesčiai ir rinkliavos bei kitos išlaidos, taip pat ir PVM, kurį turi sumokėti pats Užsakovas, tais atvejais, kai taikomas atvirkštinis apmokestinimas. Tiekėjas neturi teisės reikalauti padengti jokių išlaidų, viršijančių Sutarties kainą.

4.4. Užsakovas sumoka Tiekėjui už tinkamai ir kokybiškai pateiktas Prekes Tiekėjui Sutartyje nustatyta tvarka pateikus sąskaitą faktūrą, ne vėliau kaip per 30 (trisdešimt) kalendorinių dienų nuo sąskaitos faktūros priėmimo per Sutarties 4.5 punkte numatytos priemonės dienos, lėšas pervesdamas į Tiekėjo banko sąskaitą, nurodytą Sutarties 13 punkte. Šiame Sutarties punkte nurodyti mokėjimų terminai, susieti su finansavimu, gaunamu iš trečiųjų šalių, gali būti pratęsti atskiru raštišku Šalių susitarimu, tačiau bet koku atveju šie terminai negali viršyti 60 (šešiasdešimt) kalendorinių dienų.

4.5. Sumokėjimo diena – tai diena, kai lėšos išskaitomos iš Užsakovo sąskaitos. Vykdam Sutartį, sąskaitos faktūros teikiamos tik elektroniniu būdu. Elektroninės sąskaitos faktūros, atitinkančios Europos elektroninių sąskaitų faktūrų standartą, kurio nuoroda

*the Supplier*) with a need to access Supplier materials, documentation and/or software (including, but not limited, to the data management platform (Palantir Foundry)) (the “Products”) on behalf of Customer for the business purposes laid out under the Contract. Customer shall ensure that such users of the Accounts have signed confidentiality agreements, or are otherwise bound by confidentiality obligations at least as restrictive as those in Annex 3. Customer shall inform each user of its obligations under, and ensure that each user shall at all times abide by, the terms of the Contract. Customer shall be solely responsible and liable for all actions of such users, including any breach of the Contract by such.

3.4. Ownership: As between the parties, Supplier retains all rights, title, and interest, including all intellectual property rights, in and to the Products, updates, and any other related documentation or materials provided by Supplier. Customer retains all rights, title, and interest in and to all data that is imported, stored and managed in the Products (“Content”). Supplier may use, transmit, disclose or reproduce the Content solely as necessary to provide the Products, goods and services, to Customer under this Contract.

#### 4. CONTRACT PRICE AND PAYMENT PROCEDURES

4.1. In accordance with the Methodology for Determining of Pricing Rules, as authorised by the 28<sup>th</sup> 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 section 10.3, this Contract is subject to the rule of fixed price with revision formulation.

4.2. The contract price for the goods specified in section 1.1 of the Contract:

| Contract Year      | Subject of the procurement procedure   | Price in euros, VAT excluded | Price in euros, VAT included |
|--------------------|--|------------------------------|------------------------------|
| Year 1 (2021–2022) | Palantir Foundry licence (inclusive of infrastructure-related services, platform support services and implementation services) | 3 000 000,00                 | 3 630 000,00                 |
| Year 2 (2022–2023) | Palantir Foundry licence (inclusive of infrastructure-related services, platform support services and implementation services) | 3 000 000,00                 | 3 630 000,00                 |
| Year 3 (2023–2024) | Palantir Foundry licence (inclusive of infrastructure-related services, platform support services and implementation services) | 3 000 000,00                 | 3 630 000,00                 |

4.3. The contract price includes all taxes, fees and other expenses to be paid or incurred by the Supplier, as well as VAT, which must be paid by the Customer in case of reverse charge. The Supplier may not require a compensation for any expense that surpasses the contract price.

4.4. The Customer shall pay the Supplier for the delivered goods no later than 30 (thirty) calendar days from the date of the Supplier’s invoice. Supplier shall invoice in accordance with section 4.5 of the Contract and Customer shall make payment to Supplier’s bank account as specified at section 13 of the Contract. The payment terms specified in this section may be extended by a separate written agreement of the parties, but in any case these terms may not exceed 60 (sixty) calendar days.

4.5. 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 16<sup>th</sup> 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

paskelbta 2017 m. spalio 16 d. Komisijos įgyvendinimo sprendime (ES) 2017/1870 dėl nuorodos į Europos elektroninių sąskaitų faktūrų standartą ir sintaksį 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.

4.6. Sutarties kaina nebus perskaičiuojama pagal bendrą kainų lygio kitimą, prekių grupių kainų pokyčius bei dėl mokesčių pasikeitimų, išskyrus PVM pasikeitimą.

4.7. Jeigu Sutarties vykdymo metu pasikeičia PVM mokėjamą reglamentuojantys teisės aktai, darantys tiesioginę įtaką Tiekėjo teikiamų Sutartyje nurodytai kainai/įkainiams, Sutartyje nurodyta kaina/įkainiai perskaičiuojami ją/juos didinant arba mažinant. Perskaičiavimas įforminamas Sutarties pakeitimu, kuris tampa neatskiriama Sutarties dalimi. Perskaičiuota kaina/įkainiai taikomi už tą prekių dalį, už kurią sąskaita faktūra išrašoma galiojant naujam PVM.

4.8. Sutarčiai taikomas atvirktinis apmokestinimas, t. y. pridėtinės vertės mokesčių (PVM) į Lietuvos valstybės biudžetą sumoka Užsakovas, o Tiekėjui sumokama kaina be PVM.

## 5. SUTARTIES GALIOJIMAS

5.1. Sutartis įsigalioja ją pasirašius abiem Šalims ir galioja iki visiško Šalių įsipareigojimų įvykdymo. Prekės turi būti tiekiamos nuo 2021 m. gruodžio 6 d. ir galioti 12 mėn. Šalių susitarimu Sutartis gali būti pratęsta sutarties 2.1.1.2 punkte ir 4.2 punkte nurodytomis sąlygomis 2 (du) kartus po 12 (dvyliką) mėnesių. Jeigu likus ne mažiau kaip 30 (trisdešimt) dienų iki Sutarties galiojimo pabaigos Užsakovas neinformuoja Tiekėjo apie ketinimą nepratęsti Sutarties galiojimo, laikoma kad Šalys sutinka ir susitaria, kad Sutarties galiojimas yra pratęsiamas dar 12 (dvylikai) mėnesių.

5.2. Jei bet kuri Sutarties sąlyga tampa ar pripažįstama visiškai ar iš dalies negaliojančia, tai neturi įtakos kitų Sutarties sąlygų galiojimui.

5.3. Sutarties sąlygos Sutarties galiojimo laikotarpiu gali būti keičiamos šios Sutarties ir Viešųjų pirkimų įstatyme nustatytais atvejais.

5.4. Sutarties keitimas galioja tik tuo atveju, jeigu jis yra sudaromas rašytiniu Sutarties šalių susitarimu. Šalių susitarimai dėl Sutarties keitimo tampa neatskiriama Sutarties dalimi.

## 6. NENUGALIMOS JĖGOS APLINKYBĖS

6.1. 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*).

6.2. 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.

6.3. 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“.

## 7. ŠALIŲ ATSAKOMYBĖ

7.1. Šalys atsako už tai, kad Sutarties sąlygos būtų tinkamai vykdomos.

7.2. Užsakovui laiku nesumokėjus Tiekėjui dėl Užsakovo kaltės, Tiekėjas turi teisę reikalauti 0,02 (dviejų šimtųjų) procento dydžio

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.

4.6. 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, except for any change in VAT.

4.7. If during the performance of the Contract the legal acts regulating the payment of VAT change, which directly affect the price provided by the Supplier, the price specified in the Contract shall be recalculated with the relevant increase or decrease as applicable. The recalculation shall be formalized by an amendment to the Contract which shall become an integral part of the Contract. The recalculated price shall then apply to the proportion of goods to be invoiced under the new VAT.

4.8. The Contract is subject to reverse charge whereby the value added tax (VAT) is paid directly by the Customer to the State of Lithuania, and the Supplier is paid the Price excluding VAT.

## 5. VALIDITY OF THE CONTRACT

5.1. The Contract shall take effect when both parties sign it and remains in effect until the obligations of the parties are fully implemented. The goods shall be delivered from 2021 December 6 and shall continue for 12 (twelve) months. By agreement between the parties, the contract may be extended under the conditions described in Sections 2.1.1.2 and 4.2 of the Contract for a further 2 (two) periods of 12 (twelve) months each. If the Customer does not inform the Supplier at least 30 (thirty) days before the expiry of the relevant contract term about the intention not to extend the Contract, the parties shall be deemed to have agreed that the Contract is extended for another 12 (twelve) months.

5.2. 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.

5.3. 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.

5.4. 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.

## 6. FORCE MAJEURE

6.1. 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*).

6.2. 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.

6.3. 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 15<sup>th</sup> of July 1996 decree No. 840 titled “Concerning the approval of the regulation on circumstances enabling a release from obligations due to *force majeure*”.

## 7. RESPONSIBILITIES OF THE PARTIES

7.1. The parties shall be responsible for a proper fulfilment of the terms of this Contract.

7.2. Should the Customer fail to pay the Supplier, then the Supplier is entitled to demand a 0.02 (two hundredths) percent late fee, calculated

delspinigių už kiekvieną uždelstą kalendorinę dieną nuo vėluojamos sumokėti sumos.

7.3. Tiekėjas, neįvykęs arba netinkamai įvykęs savo sutartinius įsipareigojimus, nurodytus Sutarties 2.1.1.1 punkte, sumoka Užsakovui 0,02 (dviejų šimtųjų) procento dydžio delspinigius už kiekvieną uždelstą kalendorinę dieną nuo Sutarties 4.2 punkte nurodytos duomenų valdymo platformos licencijos kainos.

7.4. Delspinigių sumokėjimas neatleidžia Šalių nuo prievolių pagal šią Sutartį tinkamo įvykdymo.

7.5. Užsakovas turi teisę vienašališkai išskaičiuoti delspinigius iš bet kokių Tiekėjui atliekamų mokėjimų.

## 8. SUBTIEKIMAS

8.1. Tiekėjas savo pasiūlyme nurodė, kad, vykdant Sutartį bus pasitelkiami subtiekejai (*jei pasitelkiama*): –.

Nurodytus subtiekejus (*jei jie nurodyti*) galima keisti tik raštu informavus apie tai Užsakovą nurodant pagrįstas keitimo priežastis ir gavus raštišką Užsakovo sutikimą. Naujai siūlomas subtiekejasis turi atitikti pirkimo sąlygose keičiamam subtiekejui numatytus reikalavimus. Tiekėjas bet kokių atveju atsako už visus pagal Sutartį priimtus įsipareigojimus, nepaisant to, ar jiems vykdyti bus pasitelkiami subtiekejai. Pagrįstomis subtiekejimo keitimo priežastimis laikomos priežastys, kai tiekėjo pasiūlytas subtiekejasis dėl objektyvių priežasčių (subtiekejui bankrutavus ar susidarius analogiškai situacijai, nutrūkus teisiniams santykiams su Tiekėju, subtiekejui atsisakius tiktai Prekes ir pan.) nebegalį suteikti visų ar dalies Sutartyje nurodytų Prekių. Užsakovui sutikus su subtiekejimo pakeitimu, Užsakovas kartu su Tiekėju raštu sudaro susitarimą dėl subtiekejimo pakeitimo. Šis susitarimas yra neatskiriama Sutarties dalis. Subtiekejimo keitimo tvarkos pažeidimas laikomas esminiu Sutarties pažeidimu.

8.2. Sudarius Sutartį, tačiau ne vėliau negu Sutartis pradėdama vykdyti, Tiekėjas įsipareigoja Užsakovui raštu pranešti tuo metu žinomų subtiekejų 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 subtiekejus, kuriuos Tiekėjas ketina pasitelkti vėliau.

8.3. Užsakovas ne vėliau kaip per 3 (tris) darbo dienas nuo Sutarties 8.2 papunktyje nurodytos informacijos gavimo dienos informuoja subtiekejus apie tiesioginio atsiskaitymo galimybę. Subtiekejasis, norėdamas pasinaudoti tiesioginio atsiskaitymo galimybe, per 5 (penkias) darbo dienas nuo Užsakovo informavimo apie tiesioginio atsiskaitymo galimybę, Užsakovui pateikia prašymą raštu.

8.4. Subtiekejui pateikus Užsakovui prašymą pasinaudoti tiesioginio atsiskaitymo galimybe, tarp Užsakovo, Sutartį sudariusio Tiekėjo ir jo subtiekejimo yra sudaroma trišalė sutartis, kurioje aprašoma tiesioginio atsiskaitymo su subtiekejimu tvarka ir numatoma teisė Tiekėjui prieštarauti nepagrįstiems mokėjimams subtiekejui.

## 9. GINČŲ SPRENDIMO TVARKA

9.1. 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.

## 10. SUTARTIES NUTRAUKIMO TVARKA

10.1. Sutartis gali būti nutraukta:

10.1.1. rašytiniu Šalių susitarimu;

10.1.2. Sutartyje nustatytais atvejais ir tvarka;

10.1.3. kitais Civilinio kodekso nustatytais atvejais.

10.2. Užsakovas, nesikreipdamas į teismą, gali vienašališkai

from the actual arrears, for each calendar day the payment has been delayed.

7.3. The Supplier, upon failing to fulfil its contractual obligations set forth in section 2.1.1.1 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 licence price set forth in section 4.2 of the Contract, for each calendar day of the actual delay.

7.4. Paying the late fees does not release the parties from the proper fulfilling of the responsibilities set forth in this Contract.

7.5. The Customer is entitled to unilaterally withhold late fees from any payments to be made toward the Supplier.

## 8. SUBCONTRACTING

8.1. 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.

8.2. 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.

8.3. The Customer shall within 3 (three) business days from the information reception date set forth in the subsection 8.2 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.

8.4. 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.

## 9. PROCEDURE FOR RESOLUTION OF DISPUTES

9.1. 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.

## 10. PROCEDURE FOR TERMINATING THE CONTRACT

10.1. This Contract can be terminated:

10.1.1. by the parties agreeing in writing;

10.1.2. in the situations and by the procedures set forth in the Contract;

10.1.3. in other situations as provided for in the Civil Code.

nutraukti Sutartį, raštu įspėjęs Tiekėją prieš 15 (penkiolika) kalendorinių dienų, jeigu:

10.2.1. Tiekėjui iškeliami restruktūrizavimo arba bankroto byla, Tiekėjas likviduojamas, sustabdo savo ūkinę veiklą arba kai įstatymuose ar kituose teisės aktuose nustatyta tvarka susidaro analogiška situacija;

10.2.2. esant esminiam Sutarties pažeidimui;

10.2.3. Sutartis buvo pakeista pažeidžiant Lietuvos Respublikos viešųjų pirkimų įstatymo (toliau – Viešųjų pirkimų įstatymas) 89 straipsnį;

10.2.4. paaiškėjo, kad Tiekėjas, su kuriuo sudaryta Sutartis, turėjo būti pašalintas iš pirkimo procedūros pagal Viešųjų pirkimų įstatymo 46 straipsnio 1 dalį;

10.2.5. 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.

10.3. Tiekėjas, nesikreipdamas į teismą, gali vienašališkai nutraukti Sutartį, raštu įspėjęs Užsakovą prieš 15 (penkiolika) kalendorinių dienų, jeigu Užsakovas padaro esminį Sutarties pažeidimą.

## 11. KITOS SĄLYGOS

11.1. 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.

11.2. Sutartis gali būti keičiama tik Viešųjų pirkimų įstatymo 89 straipsnyje nustatyta tvarka. Sutarties sąlygų pakeitimai įforminami Šalių rašytiniais susitarimais, kurie yra neatsiejama Sutarties dalis.

11.3. 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.

11.4. 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 subtiekiųjų 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.

11.5. Tiekėjo ir Užsakovo vienas kitam siunčiami pranešimai turi būti raštiški. Pranešimai turi būti siunčiami paštu ar elektroniniu paštu Sutartyje Šalių nurodytais adresais.

11.6. Užsakovo paskirtas už Sutarties vykdymą atsakingas asmuo – Lietuvos statistikos departamento vyriausioji patarėja inovacijoms Gita Literskė (tel. +370 5 236 4826, el. paštas: [gita.literske@stat.gov.lt](mailto:gita.literske@stat.gov.lt)).

11.7. Tiekėjo paskirtas už Sutarties vykdymą asmuo Tadas Rudzevičius (tel. +44 7408 886228, el. paštas: [legalnotices@palantir.com](mailto:legalnotices@palantir.com))

11.8. Šalys įsipareigoja per 5 (penkias) kalendorines dienas pranešti viena kitai apie Sutarties 13 dalyje „Šalių adresai, rekvizitai ir

10.2. 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:

10.2.1. 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;

10.2.2. there exists a substantial violation of the Contract;

10.2.3. 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);

10.2.4. 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;

10.2.5. it has been found that a 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.

10.3. 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.

## 11. MISCELLANEOUS CONDITIONS

11.1. 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.

11.2. 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.

11.3. 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.

11.4. 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 27 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.

11.5. 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.

11.6. The Customer has designated the following person as responsible for the implementation of the Contract: Gita Literskė, Chief Adviser for Innovation of Statistics Lithuania, tel. +370 5 236 4826, e-mail: [info@stat.gov.lt](mailto:info@stat.gov.lt).

11.7. The Supplier has designated the following person as responsible for the implementation of the Contract: Tadas Rudzevičius (tel. +44 7408 886228, e-mail: [legalnotices@palantir.com](mailto:legalnotices@palantir.com)).

parašai“ nurodytų duomenų pasikeitimą. Šalis, laiku nepranešusi apie šių duomenų pakeitimus, negali reikšti pretenzijų dėl kitos Šalies veiksmų, atliktų vadovaujantis šioje Sutartyje pateiktais duomenimis.

11.9 Sutartis sudaryta dviem egzemplioriais lietuvių ir anglų kalbomis (po vieną kiekvienai šaliai), turinčiais vienodą teisinę galią, po vieną kiekvienai Šaliai. Jei yra neatitikimų ar nesutapimų tarp anglų ir lietuvių kalbos teksto, vadovaujamosi Sutarties tekstu anglų kalba.

11.10. Sutarties priedai yra neatskiriama Sutarties dalis.

## 12. SUTARTIES PRIEDAI

12.1. Sutarties 1 priedas: Duomenų valdymo platformos Palantir Foundry, reikalingos Valstybės duomenų valdysenos informacinės sistemos tęstinumui užtikrinti, licencijos, įskaitant platformos palaikymą, pirkimo techninė specifikacija.

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

12.3. Sutarties 3 priedas: Susitarimas dėl informacijos neatskleidimo.

## 13. 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. <http://www.stat.gov.lt>

DocuSigned by:

*Dr. Jūratė Petrauskienė*

865EE2A7E4AE40D...

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.: 41036032  
IBAN: GB09CHAS60924241036032  
SWIFT: CHASDEFX  
Tel. +44 7408 886228  
El. p. [legalnotices@palantir.com](mailto:legalnotices@palantir.com)

DocuSigned by:

*Tadas Rudzevičius*

57785BE12322446...

Tadas Rudzevičius, įgaliotasis asmuo

11.8. Should the details included in section 13 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.

11.9. 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.

11.10. The annexes of the Contract are an integral part of the Contract.

## 12. ANNEX

12.1. Annex 1: Technical specification for the licence of Palantir Foundry (accompanied by system deployment service) for the data management platform necessary to ensure the continuity of the State Data Governance Information System.

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

12.3. Annex 3: Non-Disclosure Agreement.

## 13. 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](mailto:info@stat.gov.lt)

<http://www.stat.gov.lt>

*Dr. Jūratė Petrauskienė*

865EE2A7E4AE40D...

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: 41036032  
IBAN: GB09CHAS60924241036032  
SWIFT: CHASDEFX  
Phone No. +44 7408 886228

E-mail: [legalnotices@palantir.com](mailto:legalnotices@palantir.com)

DocuSigned by:

*Tadas Rudzevičius*

57785BE12322446...

Tadas Rudzevičius, Authorised Signatory

Valstybės duomenų valdysenos informacinės sistemos  
licencijos (Palantir Foundry) pratęsimo pirkimo sutarties  
Nr. STAT-(2021)  
1 priedas

Renewal of the License of the State Data Governance  
Information System (Palantir Foundry) Purchase Contract  
No STAT (2021)  
Annex 1

**VALSTYBĖS DUOMENŲ VALDYSENOS  
INFORMACINĖS SISTEMOS LICENCIJOS  
(PALANTIR FOUNDRY) PRATĖSIMO PIRKIMO  
SUTARTIES TECHNINĖ SPECIFIKACIJA**

**TECHNICAL SPECIFICATION FOR THE PURCHASE  
CONTRACT OF THE RENEWAL OF THE LICENSE  
OF THE DATA GOVERNANCE SYSTEM (PALANTIR  
FOUNDRY)**

**TURINYS**

|  |    |
|--|----|
| 1. Sąvokos ir sutrumpinimai.....   | 3  |
| 2. Įvadinė informacija.....  | 3  |
| 2.1. VDV IS tikslai ir uždaviniai.....   | 3  |
| 2.2. Esama situacija.....  | 4  |
| 2.3. Planuojama plėtra.....  | 4  |
| 3. Reikalavimai duomenų valdymo platformai .....   | 4  |
| 3.1. Reikalavimai duomenų valdymo platformos architektūrai   | 5  |
| 3.2. Reikalavimai duomenų valdymo platformos funkcionalumui.....   | 6  |
| 3.2.1. Reikalavimai duomenų įsisavinimo funkcionalumui.....  | 6  |
| 3.2.2. Funkcionalumui.....   | 7  |
| 3.2.3. Reikalavimai duomenų analizės funkcionalumui.....   | 8  |
| 3.2.4. Reikalavimai duomenų vizualizavimo funkcionalumui .....   | 10 |
| 3.2.5. Reikalavimai duomenų iškėlimo funkcionalumui.....   | 11 |
| 3.2.6. Reikalavimai naudotojų ir prieigos teisių valdymo funkcionalumui.....   | 11 |
| 3.3. Reikalavimai mokymams ir mokymų medžiagai.....  | 13 |
| 3.4. Reikalavimai dokumentacijai.....  | 13 |
| 3.5. Reikalavimai licencijavimui.....  | 13 |
| 4. Reikalavimai duomenų valdymo platformos infrastruktūrai .....   | 13 |
| 5. Reikalavimai saugumui.....  | 14 |
| 6. Licencijos sąlygos: Foundry paslaugų sutartis, Foundry palaikymo politika ir Programinės įrangos valdymo politika | 16 |

**CONTENTS**

|   |    |
|---|----|
| 1. Terms and abbreviations .....  | 3  |
| 2. Introductory information.....  | 3  |
| 2.1. Goals and objectives of SDM IS.....  | 3  |
| 2.2. Current situation.....   | 4  |
| 2.3. Coming development.....  | 4  |
| 3. Requirements for Data Management Platform .....  | 4  |
| 3.1. Requirements for DMP architecture .....  | 5  |
| 3.2. Requirements for DMP functionality.....  | 6  |
| 3.2.1. Requirements for data integration functionality .....  | 6  |
| 3.2.2. Requirements for data processing functionality .....   | 7  |
| 3.2.3. Requirements for data analysis functionality.....  | 8  |
| 3.2.4. Requirements for data visualisation functionality .....  | 10 |
| 3.2.5. Requirements for data export functionality .....   | 11 |
| 3.2.6. Requirements for user and access control management functionality.....                                     | 11 |
| 3.3. Requirements for user training and training materials.....   | 13 |
| 3.4. Requirements for documentation.....  | 13 |
| 3.5. Requirements for licensing .....   | 13 |
| 4. Requirements for DMP infrastructure .....  | 13 |
| 5. Security requirements .....  | 14 |
| 6. Licence conditions: Foundry Service Level Agreement, Foundry Support Policy, and Software Management Policy... | 16 |

## 1. Sąvokos ir sutrumpinimai

| Santrumpa/<br>sąvoka                        | Paaškinimas   |
|---|---|
| <b>DVP, platforma</b>                       | Duomenų valdymo platforma Palantir Foundry, apimanti duomenų įsisavinimo, transformacijų, analizės ir vizualizavimo funkcijas   |
| <b>Perkančioji organizacija / Užsakovas</b> | Lietuvos statistikos departamentas  |
| <b>Prekės</b>                               | Valstybės duomenų valdysenos informacinę sistemą įgalinančios duomenų valdymo platformos Palantir Foundry licencija (kartu su infrastruktūros, platformos palaikymo bei įgyvendinimo paslaugomis) |
| <b>Tiekėjas</b>                             | Valstybės duomenų valdysenos informacinės sistemos tęstinumą užtikrinančios duomenų valdymo platformos Palantir Foundry licencijos pardavėjas   |
| <b>VDV IS</b>                               | Valstybės duomenų valdysenos informacinė sistema  |

## 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](mailto:info@stat.gov.lt).

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

Pirkimo objektas – Valstybės duomenų valdysenos informacinės sistemos tęstinumui užtikrinti reikalingos duomenų valdymo platformos (toliau – Palantir Foundry) licencijos, įskaitant platformos palaikymą, kartu su infrastruktūros paslaugomis, pratęsimas.

### 2.1. VDV IS tikslai ir uždaviniai

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.
- Užtikrinti efektyvų parengtos informacijos atidavimą skelbti viešai.

### 2.2. Esama situacija

Per 2021 m. VDV IS turi būti integruotas oficialiosios statistikos rengimas, įskaitant COVID-19 pandemijos ir nelegalios migracijos stebėsenos ir valdymo projektus. Susipažint su sistemos naudojamais resursais galima specialioje resursų stebėsenos aplikacijoje <https://vdv.stat.gov.lt/workspace/resource-management/>.

## 1. Terms and abbreviations

| Abbreviation/<br>Term                           | Explanation   |
|---|---|
| <b>DMP, Platform</b>                            | Data Management Platform Palantir Foundry that includes data ingress, transformations, analysis, and visualisation functions  |
| <b>Purchasing organisation / Ordering party</b> | Lithuanian Department of Statistics   |
| <b>Item</b>                                     | A license of the Data Management Platform Palantir Foundry (inclusive of infrastructure-related services, platform support services and implementation services) which will enable the State Data Governance Information System |
| <b>Supplier</b>                                 | The seller of the license of Data Management Platform Palantir Foundry which ensures the continuity of the State Data Governance Information System   |
| <b>SDM IS</b>                                   | State Data Governance Information System  |

## 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](mailto:info@stat.gov.lt).

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

The subject of the purchase – the renewal of the licence of the Data Management Platform (Palantir Foundry) which is necessary to ensure the continuity of the State Data Governance Information System, including its support services.

### 2.1. Goals and objectives of the SDM IS

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.
- To be able to ensure the efficient publication of prepared information outside the SDM IS.

### 2.2. Current situation

Over 2021 the preparation of official statistics has to be integrated to SDM IS, including COVID-19 pandemic and illegal migration monitoring and management projects. Getting acquainted with the resources used by the system is possible in a special resource monitoring application <https://vdv.stat.gov.lt/workspace/resource-management/>.

### 2.3. Planuojama plėtra

2022–2026 m. LSD kartu su IVPK įgyvendina [Ekonomikos gaivinimo ir atsparumo didinimo priemonės „Naujos kartos Lietuva“](#) reformą „Duomenų valdymo efektyvumo užtikrinimas ir atviri duomenys“. Numatyta, kad LSD per VDV IS parengs daugiau nei 300 valstybės informacinių sistemų ir registrų atvirų duomenų rinkinius publikavimui Lietuvos atvirų duomenų portale. Tai apima pirminių duomenų, reikalingų atvirų duomenų rinkiniams surinkimą, nuasmeninimą, transformavimą, sujungimą ir parengimą publikuoti patrenktus atvirų duomenų rinkinius. Taip pat projektuojamas sveikatos duomenų pakartotinio naudojimo paslaugos realizavimas VDV IS. Kiti planuojami plėtos projektai nėra tokios reikšmingos apimtys.

### 3. 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.

### 2.3. Coming development

In 2022–2026 LSD together with IVPK implements the Reform “Ensuring the effectiveness of data management and open data” of the [recovery and resilience plan for Lithuania](#). It is planned that LSD will prepare open data sets for publication on the Lithuanian Open Data Portal from more than 300 state information systems and registers through SDM IS. This includes the collection of primary data, anonymization, transformation, aggregation, and preparation for publication open data sets. The implementation of the health data reuse service in SDM IS is also being planned. Other planned development projects are not of such a significant scope.

### 3. 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.

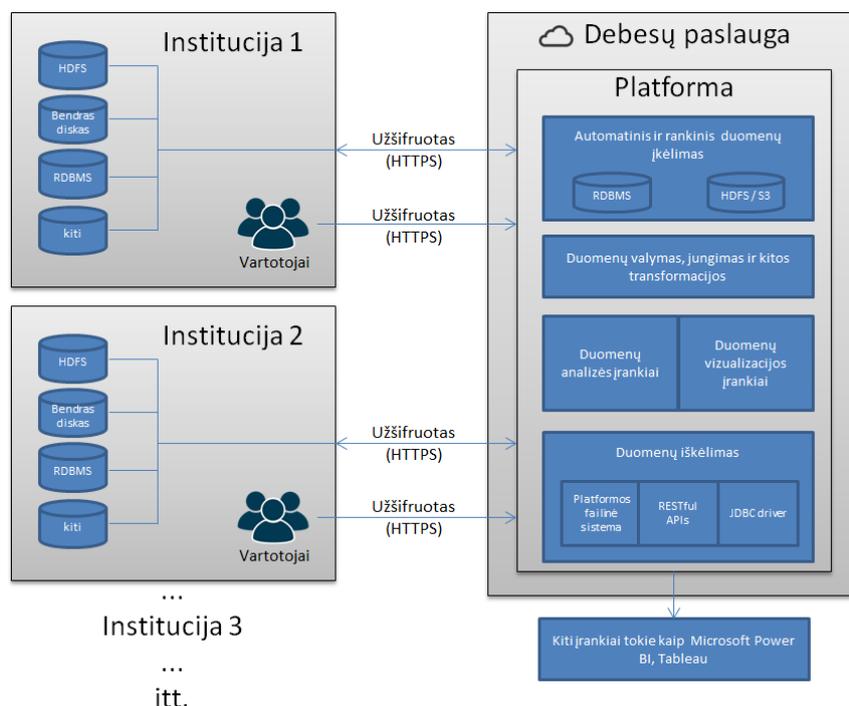
### 3.1. Reikalavimai duomenų valdymo platformos architektūrai

| 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: <ul style="list-style-type: none"> <li>- 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“);</li> <li>- valdymo sluoksnis, atsakingas už duomenų tvarkymą, apdorojimą ir transformacijas, taip pat duomenų saugumo užtikrinimą bei duomenų perdavimą kitoms aplikacijoms;</li> <li>- analizės sluoksnis, atsakingas už duomenų analizės ir vizualizavimo funkcionalumą, leidžiantį naudotojams atlikti darbą su duomenimis, siekiant išsikeltų uždavinių.</li> </ul> |
| 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 automatinių 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. |   |

### 3.1. 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: <ul style="list-style-type: none"> <li>- 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.</li> <li>- control layer which is responsible for data handling, processing, and transformations, also ensuring data security and data transfer to other applications.</li> <li>- analysis layer which is responsible for data analysis and visualisation functionality enabling users to perform work with data while achieving their goals.</li> </ul> |
| 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



### 3.2. Reikalavimai duomenų valdymo platformos funkcionalumui

#### 3.2.1. Reikalavimai duomenų įsisavinimo funkcionalumui

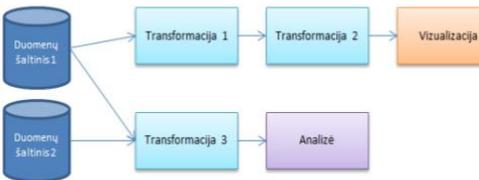
| Reikalavimo Nr.  | Reikalavimų detalizavimas   |
|--|---|
| R5 Platforma turi įgalinti vartotojus įvesti ar įkelti įvairių rūšių duomenų rinkinius ar įkelti elektronines rinkmenas. | <p>Turi būti galimybė sukurti teikiamų duomenų įvedimo formą ir suteikti kitiems vartotojams teisę ją pildyti.</p> <p>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.</p> <p>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.</p>  |
| R6 Turi būti galimybė naudojant platformos funkcionalumą sąveikauti su trečiųjų šalių informacinėmis sistemomis          | <p>Turi būti galimybė vartotojui, turinčiam atitinkamas teises, aprašyti ir sukonfigūruoti duomenų priėmimo mechanizmą, leidžiantį išoriniams vartotojams ar sistemoms įkelti duomenų rinkinius arba elektronines rinkmenas.</p> <p>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.</p> |
| R7 Platforma turi leisti automatizuoti duomenų ir elektroninių rinkmenų įkėlimo ir paėmimo procesus.                     | <p>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.</p> <p>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.</p>  |

### 3.2. Requirements for DMP functionality

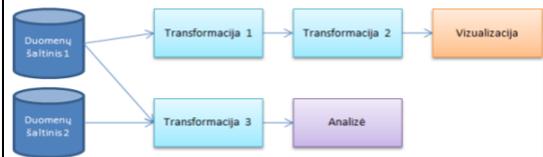
#### 3.2.1. Requirements for data integration functionality

| Requirement No.  | Requirement details  |
|--|--|
| R5 Platform has to enable users to input or upload datasets of different types or upload electronic files.   | <p>There has to be an ability to create data input form for provided data and grant other users the right to fill it out.</p> <p>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.</p> <p>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.</p>   |
| R6 There has to be an ability to interact with third party information systems using platform functionality. | <p>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.</p> <p>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.</p> |
| R7 The platform has to allow automation of data and electronic files' ingress and egress processes.          | <p>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.</p> <p>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.</p>  |

## 3.2.2. 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.  | <p>Turi būti galimybė vartotojui, turinčiam atitinkamas teises, atlikti duomenų valymą, jungimą ir transformaciją naudojant:</p> <ul style="list-style-type: none"> <li>- lengvai valdomą vartotojo sąsają duomenų įkėlimo metu leidžiančią atlikti paprastus duomenų valymo darbus, tokius kaip pasikartojančių įrašų šalinimas, reikšmių normalizacija, reikšmės pakeitimas į skaičius, išvestinių stulpelių kūrimas, stulpelių sujungimas, reikšmių pakeitimas kitomis reikšmėmis, įrašo išskaidymas į kelis stulpelius, stulpelio reikšmių užmaskavimas naudojant maišos funkcijas ir t. t.</li> <li>- 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.</li> </ul> <p>Testavimo reikmėms turi būti galimybė paleisti transformacijos kodą su mažais duomenų pavyzdžiais (angl. <i>subset</i>), sudarytais naudojant platformos filtrą prieš leidžiant juos su pilnais duomenų rinkiniais.</p> <ul style="list-style-type: none"> <li>- turi būti galimybė automatizuoti duomenų transformacijos procesus kuriant duomenų sekos planą (angl. <i>data pipeline</i>). 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.</li> <li>- naudojami duomenų šaltiniai gali ateiti iš skirtingų platformos duomenų bazių, bet jų jungimui turi būti naudojami tie patys įrankiai.</li> </ul> |
| R9 Platforma turi turėti grafinį duomenų sekos planą (angl. <i>data pipeline</i> ), kuris turi įgalinti vartotojus matyti viename lange viską, kas yra ar buvo atliekama su platformoje esančiais duomenimis: pradant nuo duomenų šaltinių pereinant prie visų transformacijų bei iš jų išplaukiančių duomenų analizių bei vizualizacijų. | <p>Paėmus bet kokią transformaciją, analizę ar vizualizaciją galima grafiškai atsekti visus žingsnius iki jos šaltinių, taip užtikrinant visų atliktų veiksmų eiliškumą, aiškumą ir suprantamumą.</p>  <pre> graph LR     S1[Duomenų šaltinis 1] --&gt; T1[Transformacija 1]     S1 --&gt; T3[Transformacija 3]     S2[Duomenų šaltinis 2] --&gt; T3     T1 --&gt; T2[Transformacija 2]     T2 --&gt; V[Vizualizacija]     T3 --&gt; A[Analizė]   </pre> <p>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.</p> <p>Pasirinkus bet kokią transformaciją ir esant poreikiui turi būti galima atnaujinti atskirai konkretų susijusį duomenų rinkinį arba kartu ir visus tokią transformacijai reikalingus įvesties (tėvinius) duomenų rinkinius iki pat pirminių duomenų šaltinių.</p> <p>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.</p>   |

## 3.2.2. 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.  | <p>There has to be an ability for a user, which has respective rights, to perform data cleaning, merging, and transformation using:</p> <ul style="list-style-type: none"> <li>- 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.</li> <li>- 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.</li> <li>- 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.</li> <li>- 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.</li> </ul> |
| 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. | <p>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.</p>  <pre> graph LR     S1[Duomenų šaltinis 1] --&gt; T1[Transformacija 1]     S1 --&gt; T3[Transformacija 3]     S2[Duomenų šaltinis 2] --&gt; T3     T1 --&gt; T2[Transformacija 2]     T2 --&gt; V[Vizualizacija]     T3 --&gt; A[Analizė]   </pre> <p>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.</p> <p>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.</p>  |

| 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.<br>Turi būti galima nustatyti bent tokius duomenų korektiškumo parametrus:<br>- eilučių skaičius<br>- ar stulpelyje visos reikšmės yra unikalios<br>- stulpelyje esančių null reikšmių skaičius<br>Vartotojas, turintis atitinkamas teises, turi galėti nustatyti kritinę ribą kiekvienam duomenų korektiškumo parametru, kuriuos platforma turi automatiškai stebėti.<br>Duomenų korektiškumo parametru pasiekus nustatytą kritinę ribą, platforma turi iškart apie tai pranešti vartotojui grafiniėje vartotojo sąsajoje. |
| R12 Platformoje turi turėti atsišakojimo (angl. <i>branching</i> ) 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.<br>It must be possible to set at least these data correctness parameters:<br>- row count<br>- whether all values in a column are unique<br>- the amount of null values in a column<br>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.<br>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.                             |

### 3.2.3. 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.<br>Turi būti užtikrintos įvairaus žinių lygio ir techninių gebėjimų vartotojų ir jų grupių (nuo duomenų analitikų iki paprastų vartotojų) galimybės atlikti įvairialypę duomenų analizę:<br>- 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;<br>- 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.  |

### 3.2.3. 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.<br>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:<br>- 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.<br>- 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 įgaliojtiems 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:<br><ul style="list-style-type: none"> <li>- nustatyti vartotojų teises peržiūrėti ir keisti išteklius;</li> <li>- priskirti išteklius vykdomoms užduotims (projektams);</li> <li>- priskirti išteklius į hierarchinę katalogų struktūrą;</li> <li>- dalytis ištekliais su kitais vartotojais</li> <li>- ieškoti prieinamų išteklių pagal raktažodžius.</li> </ul>   |
| 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.<br>Pranešimus vartotojui platforma turi pateikti grafiniėje vartotojo sąsajoje.<br>Vartotojas turi galėti nustatyti pranešimus taip, kad jie ateitų į el. pašto dėžutę, kuri yra susieta su vartotojo platformos paskyra.<br>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.<br>Vartotojas, turintis atitinkamas prieigos teises, turi galėti atlikti šiuos veiksmus:<br><ul style="list-style-type: none"> <li>- sukurti ir ištrinti skirtingus objektų tipus, pvz., organizacija, savivaldybė, įvykis ir pan.;</li> <li>- objektų tipams priskirti ir pašalinti savybes, pvz., organizacijos kodas, savivaldybės pavadinimas, įvykio data ir pan.;</li> <li>- kurti ir naikinti sąsajas tarp skirtingų objektų ir jų tipų, pvz., tam tikra organizacija yra registruota tam tikroje savivaldybėje;</li> <li>- pagal poreikį konfigūruoti objekto tipo korteles nurodant, kokia informacija jose turi atsispindėti;</li> <li>- atidaryti ir uždaryti objektų korteles, kuriose būtų matoma visa aktuali objekto informacija atsižvelgiant į objekto tipo kortelės konfigūraciją;</li> <li>- vykdyti paieškas tarp visų suintegruotų bei pagal vartotojo prieigos teises prieinamų šaltinių ir atlikti rezultatų analizę. Platformoje turi būti realizuotas:<br/> <ul style="list-style-type: none"> <li>- paieškos funkcionalumas pagal įvairius kriterijus, bet tokius kaip raktažodžiai, pakaitos ženklai (angl. wildcards), loginiai operatoriai;</li> <li>- paieškos rezultatų apžvalgos funkcionalumas, leidžiantis matyti tiek agreguotus duomenis pagal objektų tipus bei jų savybes, tiek atskirų objektų sąrašą;</li> <li>- patogus vartotojo sąsają turintis objektų ir jų tipų filtravimo bei rūšiavimo funkcionalumas.</li> </ul> </li> </ul> |

| 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:<br><ul style="list-style-type: none"> <li>- set user rights to view and change resources</li> <li>- assign resources to projects</li> <li>- assign resources to a hierarchical folder structure</li> <li>- share resources with other users</li> <li>- search accessible resources using keywords</li> </ul>   |
| 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.<br>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.<br>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.<br>The user, which has the respective access rights, must be able to perform the following actions:<br><ul style="list-style-type: none"> <li>- create and delete different object types, e.g. organisation, municipality, event, etc.</li> <li>- add and remove properties on object types, e.g. organisation code, municipality name, event date, etc.</li> <li>- create and delete links between different objects and their types, e.g. a certain organisation is registered in a certain municipality</li> <li>- configure views for object types by specifying what information has to be reflected in them</li> <li>- open and close object views which would display all up-to-date object information, by taking into account the configuration of the object type</li> <li>- search across all integrated data sources, and perform analysis of the results based on user's access rights.</li> </ul> The platform must have:<br><ul style="list-style-type: none"> <li>- search functionality by various criteria, such as keywords, wildcards, logical operators</li> <li>- search result overview functionality, which allows to see both aggregated data by object types and their properties, and a list of individual results</li> <li>- convenient UI for filtering and sorting objects and their types.</li> </ul> |

| 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.:<br>- pateikti bendrą informaciją apie duomenų lentelę: eilučių ir stulpelių skaičius, atnaujinimo datą ir pan.;<br>- išrinkti pirminių duomenų aibę bei analizuoti schemas;<br>- braižyti duomenų histogramas;<br>- braižyti duomenų pasiskirstymo grafikus;<br>- braižyti laiko eilutes;<br>- vaizduoti duomenis žemėlapiuose;<br>- filtruoti duomenis;<br>- tvarkyti duomenų rinkinio stulpelius: šalinti, pervadinti, keisti tvarką, kurti naujus stulpelius;<br>- jungti duomenų rinkinius;<br>- eksportuoti duomenų rinkinius atvirais duomenų formatais, pvz., CSV ar pan.;<br>- rūšiuoti duomenis. |
| R20 Platformoje turi būti realizuotas skaičiuoklės programinės įrangos funkcionalumas, leidžiantis atlikti operacijas su duomenimis.  | Turi būti užtikrintas toks minimalus skaičiuoklės funkcionalumas:<br>- duomenų įvedimas į skaičiuoklę;<br>- funkcijų rašymas naudojant nuorodas į langelius.<br>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 analizės 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 sąsaja 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.<br>Prieiga prie ataskaitų turi būti kontroliuojama naudojant platformos prieigos teisių modelį.   |

### 3.2.4. 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.<br>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.<br>Turi būti galimybė pasirinkti lauko reikšmę iš sistemoje egzistuojančių reikšmių.<br>Turi būti galimybė automatiškai užtikrinti duomenų korektiškumą prieš leidžiant išsaugoti formą.<br>Įvestus duomenis turi būti galima analizuoti naudojantis bet kokiais platformoje esančiais analizės įrankiais. |

| 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:<br>- provide a dataset summary: row and column count, last update date, etc.<br>- view a data subset and analyse schemas<br>- plot histograms<br>- plot distribution charts<br>- plot time series<br>- display data on maps<br>- filter data<br>- edit dataset columns: remove, rename, change order, create new columns<br>- join datasets<br>- export datasets in open data formats such as CSV or similar<br>- sort data. |
| R20 Platform must have a spreadsheet functionality which allows operations on data.   | The following minimal spreadsheet functionality must be ensured:<br>- data entry into spreadsheet<br>- writing functions by using references to cells<br><br>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.<br>Access to the reports must be controlled according to the platform's access rights model.   |

### 3.2.4. 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.<br>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.<br>There has to be an ability to automatically ensure data correctness before allowing to save the form.<br>It has to be possible to analyse the entered data using any already existing analysis tools in the platform. |

### 3.2.5. 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. |

### 3.2.6. 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: <ul style="list-style-type: none"> <li>- vartotojai ar vartotojų grupės, kuriems suteikta skaitytojo prieigos teisė, turi galėti peržiūrėti išteklius;</li> <li>- vartotojai ar vartotojų grupės, kuriems suteikta redaktoriaus prieigos teisė, turi galėti peržiūrėti ir keisti išteklius;</li> <li>- vartotojai ar vartotojų grupės, kuriems suteikta savininko prieigos teisė, turi galėti peržiūrėti ir keisti išteklius bei keisti tų išteklių prieigos teises.</li> </ul> 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 grafiniame vartotojo sąsajoje.   |
| R30 Platformos RESTful API turi palaikyti ilgalaikį prisijungimą iš išorinių sistemų.   | Platforma turi galėti išduoti ilgalaikį prisijungimo atpažinimo ženklą (angl. <i>authentication token</i> ) 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.   |

### 3.2.5. 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. |

### 3.2.6. 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: <ul style="list-style-type: none"> <li>- users or user groups, which were granted the reader access right, must be able to view the resources</li> <li>- users or user groups, which were granted the editor access right, must be able to view and change the resources</li> <li>- 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</li> </ul> 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.  | <p>Platforma turi palaikyti pagrindinių katalogų kūrimą, į kuriuos vartotojai turi galėti dėti išteklius pagal jų šaltinį, organizacijos struktūrą, projekcinę veiklą ar kitą loginę tvarką.</p> <p>Kataloguose vartotojai turi galėti dėti išteklius ar kitus (vaikinius) katalogus.</p> <p>Turi būti galimybė kiekvieną katalogą hierarchijoje apsaugoti prieigos teisėmis. Vaikiniai katalogai ir ištekliai turi paveldėti savo prieigos teises iš visų savo tėvinių katalogų.</p>  |
| R32 Vartotojų paieškos rezultatuose rodomi ištekliai turi atitikti kiekvieno iš rodomų išteklių prieigos teises. | <p>Paieškos rezultatuose turi būti rodomi tik tie ištekliai, kuriuos ieškantis vartotojas turi prieigos teises matyti.</p>   |
| R33 Platforma turi palaikyti išteklių apsaugojimą saugumo žymomis.   | <p>Papildomai prie aukščiau aprašytų prieigos teisių, turi būti galimybė ištekliais suteikti vieną ar kelias saugumo žymas.</p> <p>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.</p> <p>Ištekliai kataloguose turi paveldėti katalogams priskirtas saugumo žymas.</p> <p>Ištekliai, kurie naudoja duomenis iš kitų saugumo žymomis apribotų išteklių, turi paveldėti jų saugumo žymas.</p> <p>Saugumo žymos atsiradimas ant išteklių turi apriboti vartotojų turėtas prieigos teises prie išteklių. Pvz., vartotojas, turintis savininko prieigos teisę prie išteklių, bet neturintis visų ištekliais suteiktų saugumo žymų, turi negalėti jų pasiekti.</p> <p>Vartotojas turi turėti kiekvieną išteklių saugumo žymą tam, kad galėtų pasiekti išteklius.</p> <p>Vartotojai turi negalėti priskirti ištekliais tokios saugumo žymos, po kurios priskyrimo jie patys nebegalėtų pasiekti išteklių.</p> |

| Requirement No.  | Requirement details  |
|--|--|
| R31 The platform has to support saving of resources in a folder hierarchy.                                       | <p>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.</p> <p>The users have to be able to place resources or other (child) folders inside folders.</p> <p>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.</p>  |
| R32 The resources shown in user search results have to respect the access rights of each of the shown resources. | <p>Only those search results, for which the user that is performing the search has access rights to view, have to be shown.</p>  |
| R33 The platform has to support protecting the resources using security markings.                                | <p>In addition to the above described access rights, there has to be an ability to assign one or more security markings to resources.</p> <p>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.</p> <p>Resources that are in folders have to inherit the security markings of folders.</p> <p>Resources that use data from other resources that are restricted using security markings have to inherit the security markings of those resources.</p> <p>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.</p> <p>The user must have each security marking of the resources to be able to access such resources.</p> <p>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.</p> |

### 3.3. Reikalavimai mokymams ir mokymų medžiagai

R34 Tiekėjas įsipareigoja sutarties galiojimo metu apmokyti iki 10 Užsakovo specialistų (iki 2 sistemos ir duomenų administratorių ir iki 8 duomenų analitikų).

R35 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.

R36 Mokymams naudojamą mokymų medžiagą turi būti galima panaudoti kitų naudotojų mokymams (mokymus turi galėti prvesti anksčiau apmokinti atitinkamos valstybės institucijos naudotojai) be papildomų minėtos informacijos keitimo, koregavimo ar konfigūravimo darbų.

### 3.4. Reikalavimai dokumentacijai

R37 Duomenų valdymo platformos dokumentacija, įskaitant techninį pasiūlymą, mokymų medžiagą ir RESTful API užklausų aprašymus, turi būti pateikta lietuvių arba anglų kalba.

### 3.5. Reikalavimai licencijavimui

R38 Įsigyta licencija negali riboti duomenų valdymo platformos naudotojų skaičiaus.

R39 Įsigyta licencija turi užtikrinti platformos atnaujinimus jos galiojimo metu, be papildomų Užsakovo sąnaudų, ne rečiau kaip vieną kartą per mėnesį.

R40 Įsigyta licencija ne trumpiau kaip 1 (vienus) metus turi užtikrinti duomenų valdymo platformos palaikymą, įskaitant klaidų taisymą ir atnaujinimus.

R41 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.

## 4. Reikalavimai duomenų valdymo platformos infrastruktūrai

R42 Tiekėjas turi užtikrinti duomenų valdymo platformai reikalingą infrastruktūrą.

R43 Platformos duomenų saugojimo funkcionalumas turi palaikyti paskirstytas, saugias ir plačiai pasiekiamas duomenų saugojimo infrastruktūras, tokias kaip, pvz., Azure Blob Store, HDFS ar Amazon S3.

R44 Naudojama infrastruktūra turi galėti dinamiškai plėstis (angl. *horizontal scaling*) pagal realaus laiko resursų poreikį, taip užtikrindama reikalingus resursus turimam duomenų kiekiui ir naudotojų skaičiui.

R45 Platforma turi būti įgyvendinta „vieno langelio“ principu, t. y. turi būti patogiai vartotojo aplinka, per kurią galima lengvai pasiekti visus suintegruotus duomenų šaltinius bei platformos įrankius neišeinant už platformos ribų ir nesinaudojant papildomomis taikomosiomis programomis.

R46 Platformos tarnybinių stočių veikimas turi būti nuolatos stebimas. Į iškilusius incidentus turi būti operatyviai reaguojama ir sutrikimai turi būti šalinami pagal standartines veiklos procedūras.

R47 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.

R48 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.

R49 Turi būti užtikrintas platformos prieinamumas ne mažiau kaip 99 proc. laiko visą parą vidutiniškai per metus.

R50 Turi būti galimybė perkelti duomenų valdymo platformą į kitą nei Tiekėjo infrastruktūrą (pvz., valstybinę) Užsakovo sąnaudomis.

### 3.3. Requirements for user training and training materials

R34 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).

R35 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.

R36 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.

### 3.4. Requirements for documentation

R37 DMP documentation, including technical proposal, training materials and descriptions of RESTful API calls, must be provided in Lithuanian or English.

### 3.5. Requirements for licensing

R38 Software license cannot limit the number of DMP users.

R39 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.

R40 Software license must include operations and maintenance support, including bug fixes and upgrades for at least 1 (one) year.

R41 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.

## 4. Requirements for DMP infrastructure

R42 The Supplier must provide the necessary infrastructure for the DMP.

R43 The storage functionality of the platform must support distributed, secure, and widely available storage infrastructures such as Azure Blob Store, HDFS, or Amazon S3.

R44 The infrastructure must scale dynamically (*horizontal scaling*) 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.

R45 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.

R46 The operation of DMP servers must be constantly monitored. Incidents must be responded promptly and resolved in accordance with standard operating procedures.

R47 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.

R48 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.

R49 The availability of the platform must be at least 99% time per day on average per year.

R50 It must be possible to move DMP to an infrastructure other than the Supplier's (e.g. Government's) at the Customer's expense.

## 5. Reikalavimai saugumui

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

R51 Tarptautinio standarto ISO/IEC 27001:2013 *Information technology – Security techniques – Information security management systems – Requirements* arba lygiavėčio jam standarto.

R52 Tarptautinio standarto ISO/IEC 27002:2013 *Information technology – Security techniques – Code of practice for information security controls* arba lygiavėčio jam standarto. Duomenų valdymo platformoje saugomi duomenys turi būti apsaugoti nuo nesankcionuoto priėjimo, naudojimo, pakeitimo, atskleidimo, sunaikinimo ar praradimo.

R53 Šių tarptautinių standartų arba lygiavėčių jiems standartų: ISO/IEC 27017:2015 – *Information Security Specifically for Cloud Services*; ISO/IEC 27018:2019 – *Protecting Personally Identifiable Information in Cloud Services as a Data Processors*; SOC 2, Type 2 (Security, Confidentiality, and Availability).

R54 Siekiant užtikrinti perduodamos informacijos saugą, turi būti naudojama ne žemesnė nei TLS 1.2 kriptografijos protokolo versija šiuose komunikacijos scenarijuose: sistema–naudotojas ir pagal poreikį sistema–sistema.

R55 Duomenys platformoje turi būti šifruojami tiek tranzito metu (angl. *in transit*), tiek ramybės būsenoje (angl. *at rest*).

R56 Turi būti galimybė Užsakovui naudoti savo šifravimo raktą (angl. *bring your own key*) duomenims šifruoti platformoje ir prirėkus jį ištrinti, taip užtikrinant, kad duomenys liks užšifruoti ir nepasiekiami.

R57 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 lygiavėčiame sąraše.

R58 Sistemos slaptažodžiai negali būti saugojami programiniame kode.

R59 Sistemos svetainė turi drausti išsaugoti slaptažodžius.

R60 Atliekant sistemos svetainės administravimo darbus ryšys turi būti šifruojamas naudojant ne trumpesnę kaip 128 bitų raktą.

R61 Šifruojant naudojami skaitmeniniai sertifikatai privalo būti išduoti patikimų sertifikavimo tarnybų. Sertifikato raktas turi būti ne trumpesnis kaip 2048 bitų.

R62 Svetainės kriptografinės funkcijos turi būti įdiegtos tarnybinės stoties, kurioje yra svetainė, dalyje arba kriptografiniame saugumo modulyje (angl. *Hardware security module*).

R63 Visi kriptografiniai moduliai turi gebėti saugiai sutrikti (angl. *fail securely*).

R64 Draudžiama sistemos tarnybinėje stotyje saugoti sesijos duomenis (identifikatorių), pasibaigus susijungimo sesijai.

R65 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).

## 5. Security requirements

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

R51 International standard ISO/IEC 27001: 2013 *Information technology – Security techniques – Information security management systems – Requirements* or a suitable equivalent.

R52 International standard ISO/IEC 27002: 2013 *Information technology – Security techniques – Code of practice for information security controls* or a suitable equivalent. Data stored on the DMP must be protected from unauthorized access, use, alteration, disclosure, destruction or loss.

R53 The following international standards or a suitable equivalent: ISO/IEC 27017:2015 – *Information Security Specifically for Cloud Services*; ISO/IEC 27018:2019 – *Protecting Personally Identifiable Information in Cloud Services as a Data Processors*; SOC 2, Type 2 (Security, Confidentiality, and Availability).

R54 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.

R55 The data on the DMP must be encrypted both during transit and at rest.

R56 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.

R57 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.

R58 System passwords cannot be stored in the source code.

R59 System website must prohibit saving passwords.

R60 During site administration, the connection must be encrypted using a key of at least 128 bits.

R61 Digital certificates used for encryption must be issued by trusted certification authorities. The certificate key must be at least 2048 bits long.

R62 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.

R63 All cryptographic modules must be able to "fail securely".

R64 It is forbidden to store session data (identifier) on the server after connection session ends.

R65 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.

R66 Turi būti naudojama sistemos svetainė naudotojo įvedamų duomenų tikslumo kontrolė (angl. validation).

R67 Tarnybinė stotis, kurioje yra sistemos svetainė, neturi rodyti sistemos svetainės naudotojui klaidų pranešimų apie svetainės programinį kodą ar tarnybinę stotį.

R68 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).

R69 Tarnybinė stotis, kurioje yra sistemos svetainė, turi leisti tik svetainės funkcionalumui užtikrinti reikalingus protokolo metodus.

R70 Turi būti uždrausta naršyti sistemos svetainės aplankuose (angl. directory browsing).

R71 Turi būti įdiegta sistemos svetainė turinio nesankcionuoto pakeitimo (angl. defacement) stebėsenos sistema.

R72 Duomenų valdymo platformoje turi būti fiksuojamos naudotojų registracijos užklauskos, prisijungimo sesijos, jų pradžia, pabaiga, naudotojų veiksmai, teisių naudotis sistema pakeitimai, veiksmai su sistemos objektais, audito funkcijos įjungimas ar išjungimas, audito įrašų trynimasis, kūrimas ar keitimas, laiko ir (ar) datos pakeitimai ir kiti veiksmai.

R73 Turi būti sudaryta galimybė tokių auditų žurnalų eksportavimui už platformos ribų.

R74 Kiekviename audito duomenų įrašė turi būti fiksuojama įvykio data ir tikslus laikas, įvykio rūšis, naudotojo duomenys, įvykio rezultatas.

R75 Priemonės, naudojamos sistemos sąsajoje su viešųjų elektroninių ryšių tinklu, turi būti nustatytos taip, kad fiksuotų visus įvykius, susijusius su įeinančiais ir išeinančiais duomenų srautais.

R76 Sistemoje fiksuojami įvykiai turi būti saugomi techninėje ar programinėje įrangoje, pritaikytoje audito duomenims saugoti.

R77 Dėl įvairių trikdžių nustojus fiksuoti auditui skirtus duomenis, apie tai nedelsiant turi būti informuojamas sistemos administratorius.

R78 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).

R79 Draudžiama audito duomenis trinti, keisti, kol nesibaigęs audito duomenų saugojimo terminas.

R80 Audito duomenų kopijos turi būti apsaugotos nuo pažeidimo, praradimo, nesankcionuoto pakeitimo ar sunaikinimo.

R81 Turi būti naudojami mažiausiai du laiko sinchronizavimo šaltiniai.

R82 Naudotojų darbo sesija turi būti automatiškai užbaigiama, jei neveikimo laikas viršija nustatytą trukmę.

R83 Platformos prieigos teisių modelio ir saugumo funkcionalumų visuma turi suteikti galimybę platformoje saugomiems duomenims atitikti Europos Sąjungos Bendrąjį duomenų apsaugos reglamentą (BDAR).

R66 Correctness validation of the data entered by the user must be used in the website of the system.

R67 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.

R68 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.).

R69 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.

R70 Directory browsing in the website of the system must be prohibited.

R71 A monitoring system for unauthorized changes to the content (defacement) of the website of the system must be installed.

R72 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.

R73 There must be an ability to export such audit logs out of the system.

R74 Every audit log record must capture event date and precise time, event type, user data, the result of the event.

R75 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.

R76 Events recorded in the system must be stored in hardware or software which is adapted for the storage of audit data.

R77 The administrator has to be immediately informed when the recording of audit data is interrupted due to various disturbances.

R78 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).

R79 It is prohibited to delete or change audit data until the term of storage of audit data has expired.

R80 Copies of audit data should be protected from tampering, loss, unauthorized alteration, or destruction.

R81 At least two time synchronization sources must be used.

R82 Users' work session must end automatically if the idle time exceeds the set duration.

R83 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.

## 6. Licencijos sąlygos: Foundry paslaugų sutartis, Foundry palaikymo politika ir Programinės įrangos valdymo politika

1. Foundry paslaugų sutartis
2. Foundry palaikymo politika
3. Programinės įrangos valdymo politika

## 6. Licence conditions: Foundry Service Level Agreement, Foundry Support Policy, and Software Management Policy

1. Foundry Service Level Agreement
2. Foundry Support Policy
3. Software Management Policy

### Palantir Foundry paslaugų sutartis (toliau – PS)

*Paskutinį kartą atnaujinta: 2021 m. liepos 15 d.*

Ši PS numato Palantir Užsakovų naudojimąsi Palantir Foundry (toliau – **Foundry**). PS papildo, tačiau nekeičia Palantir Prieigos Sąlygų ar kitos sutarties, reglamentuojančios Jūsų naudojimąsi Foundry, įskaitant bet kuriuos papildymus, priedus ir pridedamus dokumentus (toliau kartu – **Sutartis**). Palantir gali laikas nuo laiko atnaujinti šią PS. Esant prieštaravimui tarp šios PS ir Sutarties sąlygų, šios PS sąlygos pakeičia ir reguliuoja, jeigu Sutartis konkrečiai nenustato pirmenybės. Jei čia nenurodyta kitaip, visi šioje PS vartojami apibrėžimai, parašyti didžiosiomis raidėmis, turi tokią reikšmę, kokia jiems suteikta Sutartyje.

#### 1. Vykdyto įsipareigojimas

- a. Taikomos Užsakymo formos Galiojimo metu Palantir deda komerciškai pagrįstas pastangas, kad užtikrintų Užsakovui **99,9 procentų** prieinamumą žemiau nurodytomis sąlygomis (toliau – **Vykdyto įsipareigojimas**). Vykdyto įsipareigojimas suprantamas kaip Darbo procesai, atitinkantys pagrindines produkto galimybes. Jei Palantir neatlieka Vykdyto įsipareigojimo, Užsakovas gali gauti žemiau nurodytus Paslaugų kreditus.
- b. Kiekvieno Darbo proceso pasiekiamumas apskaičiuojamas iš Kalendorinių minučių atėmus bendrą minučių skaičių kiekvieno 10 minučių

### Palantir Foundry Service Level Agreement (“SLA”)

*Last Updated: July 15, 2021*

This SLA concerns the use of Palantir Foundry (“**Foundry**”) by Customers of Palantir. This SLA supplements, but does not modify, the Palantir Terms and Conditions of Access or other agreement governing your use of Foundry, including any attachments, exhibits, and appendices thereto (collectively, the “**Agreement**”). This SLA may be updated by Palantir from time to time. In the event of a conflict between the terms and conditions of this SLA and the Agreement, the terms and conditions of this SLA shall supersede and control, unless the Agreement specifically establishes precedence. Unless otherwise defined herein, all capitalised terms used in this SLA will have the meanings given to them in the Agreement.

#### 1. Performance Commitment

- a. During the Term of the applicable Order Form, Palantir will make commercially reasonable efforts to provide Availability of **99.9%** to Customer on the terms set forth below (the “**Performance Commitment**”). The Performance Commitment is defined in terms of Workflows that correspond to core product capabilities. If Palantir does not meet the Performance Commitment, Customer may be eligible to received Service Credits as defined below.
- b. Availability for each Workflow is calculated as the Calendar Minutes, minus the number of cumulative

intervalo metu, kurio metu Darbo procesas yra nepasiekiamas, bent su dešimt (10) bandymų tokio intervalo metu, padalijus iš Kalendorinių minučių. Jei per tam tikrą 10 minučių intervalą nebandoma atlikti jokio Darbo proceso, laikoma, kad šis intervalas yra 100 proc. pasiekiamas.

minutes in each 10-minute interval during which the Workflow is Unavailable, with at least ten (10) execution attempts made during such interval, divided by the Calendar Minutes. If no Workflow execution attempts are made in a given 10-minute interval, that interval is assumed to be 100% Available.

| Darbo procesas       | Apibūdinimas  | Nepasiekiamas apibrėžimas   |
|----------------------|---|---|
| Autentifikavimas     | Patvirtina Įgaliotų vartotojų, galinčių valdyti prieigą prie Foundry ir visų susijusių išteklių, tapatybę.  | Įgalioto vartotojo autentifikavimo užklausa nepavyksta, nurodoma Vidaus klaida. |
| Autorystė            | Integruota kūrimo aplinka į autoriaus kodu pagrįstas duomenų transformacijas, sudarančias atskirus elementus duomenų sraute.                          | Užklausa įkelti Autorinę vartotojo sąsają nepavyksta, nurodoma Vidaus klaida.   |
| (At)statymas         | Tvarko procesus, susijusius su naujų duomenų rinkinių versijų kūrimu po jų išvalymo ar pakeitimo.   | Užklausa pradėti darbą nepavyksta, nurodoma Vidaus klaida.                      |
| Kodų žurnalas        | Foundry įdiegta atvira /neribota/ kodavimo aplinka, leidžianti atlikti pažangią analitinę analizę naudojant pramonės standarto kalbas ir bibliotekas. | Užklausa pradėti kodavimą nepavyksta, nurodoma Vidaus klaida.                   |
| Kontūras             | „Nurodykite ir spustelėkite“ įrankis, leidžiantis iš viršaus į apačią analizuoti didelio masto duomenis.  | Užklausa pradėti Kontūro darbą nepavyksta, nurodoma Vidaus klaida.              |
| Prieiga prie duomenų | Ieškojimas, naršymas ir duomenų rinkinių bei bet kurių Foundry aplankų sistemoje  | Užklausa peržiūrėti arba atidaryti duomenų rinkinį per                          |

| Workflow       | Description   | Unavailable Definition   |
|----------------|---|--|
| Authentication | Authenticates identity of Authorized Users to manage access to Foundry and all associated resources within.                                 | Authorized User authentication request fails with Internal Error returned.   |
| Authoring      | An integrated development environment to author code-based data transformations that constitute the individual elements in a data pipeline. | Request to load Authoring user interface fails with Internal Error returned. |
| Builds         | Manages the processes involved in creating new versions of datasets after they have been cleaned or transformed.                            | Request to initiate job fails with Internal Error returned.                  |
| Code Workbook  | Open-ended coding environment embedded in Foundry permitting advanced analytical analysis using industry-standard languages and libraries.  | Request to execute code fails with Internal Error returned.                  |
| Contour        | Point-and-Click tool allowing top-down analysis of large-scale data.  | Request to initiate Contour job fails with Internal Error returned.          |
| Data Access    | Navigation, browsing, and previewing of datasets and any resource created in the  | Request to preview or open dataset via the Foundry UI fails                  |

|               |  |   |                 |   |   |
|---------------|--|---|-----------------|---|---|
|               | sukurtų išteklių peržiūra.   | Foundry vartotojo sąsają nepavyksta, nurodoma Vidaus klaida.  |                 | Foundry file system.  | with Internal Error returned.   |
| Duomenų ryšys | Duomenų ištraukimas ir įtraukimas, apimantis duomenų ryšio adapterį (įdiegtą išorinėje tinklo aplinkoje) ir duomenų ryšio koordinatorių (Foundry).                             | Užklausa įtraukti duomenis nepavyksta, nurodoma Vidaus klaida.  | Data Connection | Data extraction and ingestion, comprising the data connection adapter (installed in external network environment) and data connection coordinator (within Foundry). | Request to execute data ingestion job fails with Internal Error returned.                       |
| Duomenų būklė | Pateikia informaciją apie esamą visų duomenų perdavimo ir transformacijos /apdorojimo/ srautų būklę bei įspėjimo galimybes.  | Užklausa paskaičiuoti /suplanuoti/ /įvertinti/ būklės patikrinimus nepavyksta, nurodoma Vidaus klaida.                | Data Health     | Provides information on the current health of all data connection and transformation pipelines, along with alerting capabilities.                                   | Request to calculate health check fails with Internal Error returned.                           |
| Objektai      | Leidžia peržiūrėti duomenis, pateikiamus kaip objektų tipai (pvz., žmonės, vietos ir santykiai), kurie suteikia jiems kontekstinę reikšmę lentelių formos duomenų rinkiniuose. | Visos API užklauskos nuo „Object Explorer“ vartotojo sąsajos iki Foundry paslaugų nepavyksta, nurodoma Vidaus klaida. | Objects         | Allows viewing of data represented as the object types (for example people, places, and relationships) that give them contextual meaning across tabular datasets.   | All API requests from the Object Explorer UI to Foundry services return with an Internal Error. |
| Ataskaitos    | Vaizdinis ataskaitų teikimo įrankis, leidžiantis konfigūruojamą analizių kūrimą ir bendrinimą  | Visos API užklauskos nuo Ataskaitų vartotojo sąsajos iki Foundry paslaugų nepavyksta, nurodoma Vidaus klaida.         | Reports         | Visual reporting tool, allowing highly configurable creation and sharing of analyses.   | All API requests from the Reports UI to Foundry services return with an Internal Error.         |
| Lentelė       | Konfigūruojamas prietaisų skydelio įrankis, leidžiantis konfigūruojamą interaktyvių prietaisų skydelių, rodančių duomenis Foundry, kūrimą.                                     | Visos API užklauskos nuo „Slate“ vartotojo sąsajos iki Foundry paslaugų nepavyksta, nurodoma Vidaus klaida            | Slate           | Configurable dashboarding tool allowing highly configurable creation of interactive dashboards displaying data within Foundry.                                      | All API requests from the Slate UI to Foundry services return with an Internal Error.           |

## 2. Paslaugų kreditai

- a. Jeigu galimybė pasiekti / atlikti Darbo procesą, kuriam taikomas Vykdyto įsipareigojimas, nukrenta žemiau taikomos ribos, nustatytos šios PS 1 skirsnyje, (toliau – „Paslaugų neatlikimas“), Užsakovas gali pateikti prašymą Paslaugų kreditams gauti.
- b. Paslaugų kreditai yra apskaičiuojami procentais nuo Foundry Cloud prenumeratos mokesčių, kuriuos Užsakovas sumoka Palantir už tam tikro kalendorinio mėnesio Paslaugų neatlikimą Darbo procesų metu. Kiekvienas Darbo procesas sudaro vienodą Foundry Cloud prenumeratos mokesčių dalį. Bendras maksimalus Paslaugų kreditų, kuriuos turi išduoti Palantir, dydis dėl Paslaugų neatlikimų bet kurį kalendorinį mėnesį negali viršyti 5 procentų Foundry Cloud prenumeratos mokesčių, priskirtinų tam kalendoriniam mėnesiui (apskaičiuojami proporcingai per taikomą Užsakymo terminą).

| Pasiekiamumas<br>(galimybė /laisvai/<br>naudotis)    | Paslaugų kredito<br>procentinis dydis |
|--|---------------------------------------|
| Mažiau nei 99,9 proc., bet ne mažiau kaip 99,0 proc. | 10 proc.                              |
| Mažiau nei 99,0 proc., bet ne mažiau kaip 98,0 proc. | 20 proc.                              |
| Mažiau nei 98,0 proc. bet ne mažiau kaip 97,0 proc.  | 30 proc.                              |
| Mažiau nei 97,0 proc., bet ne mažiau kaip 96,0 proc. | 40 proc.                              |
| Mažiau kaip 96,0 proc.                               | 50 proc.                              |

- c. Norėdamas prašyti Paslaugos kredito, Užsakovas informuoja Palantir per trisdešimt (30) dienų nuo tariamo Paslaugos neatlikimo momento, pateikdamas raštišką prašymą adresu [service-credits@palantir.com](mailto:service-credits@palantir.com) ir nuroydamas bent šią

## 2. Service Credits

- a. If Availability for a Workflow within scope of the Performance Commitment falls below the applicable threshold set forth in Section 1 of this SLA (a “**Service Level Failure**”), then Customer may submit a request for Service Credits.
- b. Service Credits are calculated as a percentage of the Foundry Cloud Subscription fees paid by Customer to Palantir for a given calendar month for Workflows that suffered a Service Level Failure. Each Workflow accounts for an equal proportion of the applicable Foundry Cloud Subscription fees. The aggregate maximum magnitude of Service Credits to be issued by Palantir arising from Service Level Failures in any given calendar month shall not exceed 5% of the Foundry Cloud Subscription fees attributable to that calendar month (calculated on a pro rata basis over the applicable Order Term).

| Availability                                | Service Credit Percentage |
|---|---------------------------|
| Less than 99.9% but equal to or above 99.0% | 10%                       |
| Less than 99.0% but equal to or above 98.0% | 20%                       |
| Less than 98.0% but equal to or above 97.0% | 30%                       |
| Less than 97.0% but equal to or above 96.0% | 40%                       |
| Less than 96.0                              | 50%                       |

- c. To request a Service Credit, Customer must notify Palantir within thirty (30) days from the time the alleged Service Level Failure occurred by submitting a written request to [<service-credits@palantir.com>](mailto:service-credits@palantir.com) with, at a minimum, the

informaciją:

- i. Temos antraštėje žodžius „Prašymas Palantir paslaugų kreditui gauti“.
  - ii. Išsamų aprašymą, įskaitant datas ir laiką, paaiškinantį, kada ir kodėl, Užsakovo manymu, nurodytas Darbo procesas buvo nepasiekiamas.
  - iii. Jei yra, bet kokius patvirtinančius išteklių ID, duomenų rinkinius, objektus, žurnalus ar duomenis, arba Užsakovo pašalintą neskelbtiną ar konfidencialią informaciją.
- d. Palantir peržiūri užklausas dėl Paslaugų kreditų per 30 darbo dienų nuo gauto galiojančio prašymo. Palantir savo nuožiūra taiko bet kokius Paslaugų kreditų mokėjimus už kitą Užsakovo mokėjamą arba, jei galima, pinigų grąžinimą pasibaigus Užsakymo terminui. Paslaugų kreditai nėra perduodami arba perleidžiami. Paslaugų kreditai, jei taikomi, yra vienintelė ir išimtinė priemonė tam, kad būtų pašalintos tokio Vykdyto išipareigojimo neatlikimo pasekmės. Prašymo Paslaugų kreditui gauti nepateikimas atima teisę gauti Paslaugų kreditus.

### 3. Apibrėžimai

- a. **Pasiekiamumas / (galimybė /laisvai/ naudotis)** yra apskaičiuojamas už kiekvieną Darbo procesą, kaip nurodyta šios PS 1 skirsnyje.
- b. **Kalendorinės minutės** yra bendras minučių skaičius per tam tikrą kalendorinį mėnesį.
- c. **Vidaus klaida** yra 5XX HTTP Atsako kodas.
- d. **Planinė priežiūra** – tai iš anksto nustatytas laikotarpis, neįtrauktas į Prieinamumo skaičiavimus.
- e. **Paslaugų kreditas** yra pagal šią Sutartį apskaičiuotas kreditas doleriais, kurį Palantir gali grąžinti į Užsakovo sąskaitą būsimiems mokėjimams atlikti. Paslaugų kreditai yra neperleidžiami ir negali būti keičiami ar konvertuojami į pinigines išmokas.

following details:

- i. The words “Palantir Service Credit Request” in the subject header;
  - ii. A detailed description, including dates and times, explaining when and why the Customer believes the specified Workflow was Unavailable;
  - iii. If available, any corroborating resource IDs, datasets, objects, logs or data, with sensitive or confidential information removed by Customer.
- d. Palantir will review Service Credit requests within 30 business days upon receipt of a valid request. Palantir will apply any Service Credits owing against Customer’s next payment or, if applicable, as a refund at the end of your Order Term, in its discretion. Service Credits are not transferable or assignable. Service Credits, where applicable, are the sole and exclusive remedy for failure of the Performance Commitment. Failure to submit a Service Credit request as set forth herein will disqualify you from eligibility for receiving Service Credits.

### 3. Definitions

- a. **Availability** is calculated for each Workflow as set forth in Section 1 of this SLA.
- b. **Calendar Minutes** is the total number of minutes in a given calendar month.
- c. **Internal Error** is a 5XX HTTP Response Code.
- d. **Scheduled Maintenance** means a pre-determined period of time excluded from Availability calculations.
- e. **Service Credit** is a dollar credit, calculated as described herein, that Palantir may credit back to an eligible Customer account against future payments. Service Credits are non-transferrable and may not be exchanged or converted for monetary disbursements.

- f. **Nepasiekiamas** yra apibrėžta kiekvienai Paslaugai, kaip nurodyta šios PS 2 skirsnyje.
- f. **Unavailable** is defined for each Service as set forth in Section 2 of this SLA.
- g. **Darbo procesas** reiškia Foundry sudėtinę dalį, kurios Pasiiekiamumas / (galimybė /laisvai/ naudotis) vertinamas kaip Vykdyto įsipareigojimo dalis.
- g. **Workflow** means a component of Foundry for which Availability is measured as part of the Performance Commitment.

#### 4. Išimtys

- a. Palantir neatsako už bet kokį Vykdyto įsipareigojimo nesilaikymą tiek, kiek tai kyla dėl: (a) Užsakovo, jo filialų ir (arba) įgaliotų naudotojų naudojimosi Programine įranga, išskyrus pagal Sutartį ar Dokumentaciją įgaliotus asmenis, įskaitant pakeitimus, pataisymus ar žalą, bet neapsiribojant bet kokių aplaidumų, tyčiniu nusizengimu ar naudojimu; (b) Užsakovo turinio; (c) Užsakovo arba įgaliotų naudotojų įrangos; (d) bet kokio Programinės įrangos naudojimo, neklasifikuojamo kaip „Bendrai prieinama“ Palantir nuožiūra; (e) trečiųjų šalių veiksmų ar neveikimo, paslaugų, produktų ar sistemų, kurių neteikia Palantir; (f) bet kokios priežasties, vertinamos kaip force majeure aplinkybės, ar veiksmų, kurių Palantir negali pagrįstai kontroliuoti, įskaitant, bet neapsiribojant, bendras interneto problemas; (g) Programinės įrangos vertinimo arba koncepcinio naudojimo įrodymo pagal bet kokio pobūdžio susitarimą be išlaidų; (h) Nepasiekiamumo dėl klaidų, dėl kurių Palantir išleido produkto atnaujinimą, kuris lieka neįgyvendintas dėl Užsakovo veiksmų ar neveikimo; (i) pasirinktų scenarijų (tekstų / rašmenų) ar kodų, nepateiktų kartu su Programine įranga; j) Planinės priežiūros (žemiau nurodytos Palantir programinės įrangos valdymo politikoje).

#### 5. PS pakeitimai

- a. Palantir gali atnaujinti, papildyti, pašalinti arba keisti Darbo procesus, įskaitant Prieinamumą, Nepasiekiamas apibrėžimą, Procentinį prieinamumo skaičiavimą ir (arba) Brandos lygį pagal Programinės įrangos valdymo politiką. Tokie pakeitimai gali būti įgyvendinti Palantir nuožiūra,

#### 4. Exclusions

- a. Palantir will have no liability for any failure to meet the Performance Commitment to the extent arising from: (a) use of the Software by Customer, its Affiliates, and/or Authorizes Users other than as authorized under the Agreement or Documentation, including alterations, modifications or damage but not limited to any negligence, wilful misconduct or use; (b) Customer Content; (c) Customer or Authorized User equipment; (d) any use of Software not classified as Generally Available in Palantir's discretion; (e) third party acts or omissions, or services, products, or systems not provided by Palantir; (f) any matter constituting force majeure or factors beyond Palantir's reasonable control, including but not limited to general Internet problems; (g) evaluation or proof-of-concept use of the Software under a no-cost agreement of any kind; (h) Unavailability caused by errors for which Palantir has released a Product Update that remains unimplemented due to Customer's action or inaction; (i) custom scripts or code not provided with the Software; (j) Scheduled Maintenance (as further described in the Palantir Foundry Software Management Policy).

#### 5. SLA Changes

- a. Palantir may update, add, remove, or modify Workflows, including Availability, Unavailable Definition, Percentage Availability Calculation, and/or Maturation Level pursuant to the Software Management Policy. Such modifications may be implemented at Palantir's discretion, provided that

jei jie nesumažina Darbo procesų funkcionalumo, atlikimo, Prieinamumo ar saugumo. Palantir iš anksto raštu dokumentais informuoja apie tokius pakeitimus ir ne vėliau kaip prieš 90 dienų raštu įspėja Užsakovo techninį kontaktą dėl esminių neigiamų pakeitimų. Svarbūs neigiami PS pakeitimai įsigalioja praėjus 90 dienų įspėjimo terminui.

- b. Jei Užsakovas mano, kad PS pakeitimas daro jam esminį neigiamą poveikį, o pakeitimas įvyko ne dėl to, kad Palantir laikėsi galiojančių įstatymų, teisės aktų ar galiojančio teismo nurodymo, tada Užsakovas gali informuoti Palantir apie savo prieštaravimą dėl pakeitimo per 30 dienų po to, kai Palantir pateikia pranešimą, ir Užsakovas toliau vadovaujasi tuometinėmis PS sąlygomis iki anksčiausios iš šių datų (i) tuo metu galiojančios Užsakymo formos galiojimo pabaigos arba nutraukimo, arba (ii) keturis (4) mėnesius po to, kai Palantir pateikė pranešimą apie pakeitimą. Jeigu Užsakovas neinformuoja Palantir apie savo prieštaravimą, taikomos atnaujintos PS sąlygos.

they do not result in a material reduction in functionality, performance, Availability, or security of the Workflows. Palantir will provide advance written notice via the Documentation of such modifications with at least 90 days' advance written notice to the Customer Technical Contact for materially adverse modifications. Material adverse changes to the SLA will become effective after the 90 day notice period.

- b. If Customer believes that a change to the SLA has a material adverse impact on Customer, and the change is not a result of Palantir complying with applicable law, regulation, or a valid court order, then Customer may notify Palantir of its objection to the change within 30 days after Palantir provides notice and Customer will then remain governed by the then-current SLA terms until the earlier of (i) the expiration or termination of the then-current Order Form, or (ii) four (4) months after the notice of change was provided by Palantir. If Customer does not notify Palantir of its objection, then the updated SLA terms will apply.

[LIKUSI PUSLAPIO DALIS SPECIALIAI YRA PALIKTA TUŠČIA] [REST OF PAGE LEFT INTENTIONALLY BLANK]

## Duomenų valdymo platformos Palantir Foundry palaikymo politika („Palaikymo politika“)

## Palantir Foundry Support Policy (“Support Policy”)

*Paskutinį kartą atnaujinta: 2021 m. liepos 15 d.*

*Last Updated: July 15, 2021*

Ši Palaikymo politika apima Palantir palaikymą, susijusį su Palantir Foundry naudojimo klaidomis. Palantir palaikymas teikiamas, jei tai numatyta Palantir prieigos sąlygose, taikomoje Užsakymo formoje ar kitoje sutartyje, reglamentuojančioje Duomenų valdymo platformos Palantir Foundry naudojimą, įskaitant visus jos priedus (bendrai vadinama „Sutartimi“). Kilus prieštaravimui tarp šios Palaikymo politikos ir Sutarties sąlygų, pirmenybė teikiama šios Palaikymo politikos sąlygoms, nebent Sutartyje yra konkrečiai nustatyta pirmenybė. Jei šiame Priede nenurodyta kitaip, visi šioje Palaikymo politikoje vartojami terminai didžiosiomis raidėmis turės tokią reikšmę, kokia jiems suteikta Sutartyje ir (arba) Palantir darbo proceso lygio sutartyje.

This Support Policy concerns Palantir’s support offering (“**Palantir Support**”) in connection with Errors in the use of Palantir Foundry (“**Foundry**”). Palantir Support shall be provided if specified in the Palantir Terms and Conditions of Access, the applicable Order Form, or other agreement governing your use of Foundry, including any attachments, exhibits, and appendices thereto (collectively, the “**Agreement**”). In the event of a conflict between the terms and conditions of this Support Policy and the Agreement, the terms and conditions of this Support Policy shall supersede and control, unless the Agreement specifically establishes precedence. Unless otherwise defined in this Addendum, all capitalised terms used in this Support Policy will have the meanings given to them in the Agreement and/or the Palantir Workflow Level Agreement, as applicable.

### 1. Palantir palaikymas

- a. Taikomo Užsakymo termino metu Palantir teikia nuotolinę techninę pagalbą Užsakovo techninio skyriaus darbuotojams anglų kalba (arba kita kalba, jei tai konkrečiai nurodyta taikomoje Užsakymo formoje), siekiant reaguoti ir atsakyti į su klaidomis susijusius klausimus, įskaitant tyrimus, analizę, trikčių šalinimą, ir problemų sprendimus.
- b. Palantir palaikymas apima plataus masto mokymo išteklius ir dokumentus, prieinamus visiems įgaliotiems vartotojams.

### 2. Pranešimas apie klaidas

- a. Esant klaidai, Užsakovo techninio skyriaus darbuotojai pateikia pranešimą apie Klaidą, kuriame pateikiama bent jau ši informacija:
- b. klaidos sunkumo lygis pagal 1 lentelę;

### 1. Palantir Support

- a. During the applicable Order Term, Palantir shall provide English language (or other language where specifically set forth in an applicable Order Form) remote Technical Support to Customer Technical Contacts to respond to and answer questions arising from any Error, including triage, analysis, troubleshooting, and workarounds.
- b. Palantir Support includes extensive training resources and Documentation available to all Authorized Users.

### 2. Reporting Errors

- a. In the event of an Error, Customer’s Technical Contacts shall submit an Error report including, at a minimum:
- b. the Severity level of the Error, in accordance with Table 1;

- c. pakankamai informacijos, kad Palantir Palaikymo darbuotojai galėtų atkartoti klaidą (įskaitant, kai taikoma, klaidų pranešimus); ir
- d. Užsakovo techninio skyriaus darbuotojų, paskirtų bendrauti su Palantir šiuo klausimu, kontaktinė informacija (telefono numeris ir el. paštas).
- e. **P0 klaidos:** Kliento techninio skyriaus darbuotojai gali pateikti pranešimą apie P0 klaidą, siųsdami el. laišką Palantir nurodytu el. pašto adresu, skirtu pranešimams apie P0 klaidą teikti.
- f. **P1 - P3 klaidos:** Kliento techninio skyriaus darbuotojai gali teikti pranešimą apie P1-P3 klaidas per programos teikiamą Foundry Issues klaidų ataskaitų paslaugą (arba vėlesnę Palantir teikiamą paslaugą). Jei Foundry Issues nepasiekiamas, Kliento techninio skyriaus darbuotojai gali pateikti pranešimą apie P1-P3 klaidą, siųsdami el. laišką Palantir nurodytu el. pašto adresu, skirtu pranešimams apie P1-P3 klaidą teikti.
- g. Pranešimai apie klaidą, kuriuose pateikiama funkcijų užklausa, laikomi uždarytais, kai tik jie yra perduodami viduje atitinkamoms vidaus komandoms.
- c. information sufficient to enable Palantir Support personnel to replicate the Error (including, where applicable, error messages); and
- d. the contact details (phone number and email) of the Customer Technical Contact assigned to liaise with Palantir on the issue.
- e. **P0 Errors:** Customer Technical Contacts may file a P0 Error report by sending an email to the P0 reporting email address provided by Palantir.
- f. **P1 - P3 Errors:** Customer Technical Contacts may submit P1 - P3 Error reports through Foundry Issues, the in-application Error reporting service (or a successor service made available by Palantir). In the event Foundry Issues is not accessible, Customer Technical Contacts may file a P1-P3 Error report by sending an email to the P1-P3 reporting email address provided by Palantir.
- g. Error reports containing feature requests shall be considered closed once forwarded internally to applicable internal teams.

### 3. Klaidos sunkumo lygiai

### 3. Error Severity Levels

| 1 lentelė: Klaidos sunkumo lygio apibrėžimai |   |
|--|---|
| P0   | Klaida, kuri daro rimtą poveikį veiklai arba sutrikdo Kliento veiklą, dėl kurios: (a) darbo procesas tampa iš esmės neveiksmingas arba nepasiekiamas, (b) iš esmės pabloginamas darbo proceso efektyvumas, tarsi jis būtų iš esmės neveiksmingas arba nepasiekiamas, arba (c) iš esmės apribojama Užsakovo galimybė visiškai arba dalinai naudotis darbo procesu. |
| P1   | Klaida, iš esmės apribojanti Užsakovo galimybę naudoti darbo procesą įprastai veiklai, kuri: (a) iš esmės pablogina darbo proceso efektyvumą, kai yra veiklą įgalinantis  |

| Table 1: Error Severity Level Definitions |  |
|---|--|
| P0  | Error which causes serious business impact or disruption to Customer's business activities by (a) rendering a Workflow materially inoperative or unavailable, (b) substantially degrading the performance of a Workflow as if it were materially inoperative or unavailable, or (c) materially limiting Customer's use of all or part of a Workflow. |
| P1  | Error which materially limits or restricts Customer's use of a Workflow for normal business purposes by (a) substantially degrading the performance of a Workflow  |

|    |  |
|----|--|
|    | sprendimas, arba (b) gali turėti rimtą poveikį Užsakovo veiklai arba ją sutrikdyti, jei yra laiku neišspręsta.   |
| P2 | Klaida, kuri (a) daro tik nedidelį poveikį Užsakovo galimybei naudotis darbo procesu, arba (b) daro nedidelį poveikį įprastai Užsakovo veiklai.                        |
| P3 | Klaida, kuri (a) daro tik labai nedidelį poveikį Užsakovo galimybei naudotis darbo procesu, arba (b) turi ribotos arba neturi jokios įtakos įprastai Užsakovo veiklai. |

|    |  |
|----|--|
|    | where a business-enabling workaround exists, or (b) potentially having serious business impact or disruption to the Customer's business activities if not resolved in timely manner. |
| P2 | Error which (a) causes only a minor impact to the Customer's use of Workflow, or (b) marginally affects normal business activities of the Customer.                                  |
| P3 | Error which (a) causes only a very minor impact on the Customer's use of Workflow, or (b) has limited to no effect on the normal business activities of the Customer.                |

#### 4. Atsakas dėl klaidų

a. Gavęs pranešimą apie klaidą, Palantir peržiūrės ir pagrįstai savo nuožiūra patvirtins sunkumo lygį pagal 1 lentelėje pateiktas apibrėžtis, ir dės komerciškai pagrįstas pastangas laikytis 2 lentelėje nurodyto pradinio atsakymo termino, atsižvelgiant į sunkumo lygį, pagal 3 lentelėje nurodytas vietas (regiono) darbo valandas. Esant neatitikimui tarp klaidos sunkumo lygio, apie kurį pranešė Užsakovas, ir to, kurį pagrįstai nustatė Palantir, pirmenybė teikiama Palantir nustatytam sunkumo lygiui, ir Palantir nedelsdamas apie jį praneša Užsakovui. Jei Užsakovas pateiks Palantir pagrįstą pagrindą nesutikti su Palantir nustatytu klaidos sunkumo lygiu, tiek Užsakovas, tiek Palantir praneš apie nesutarimą atitinkamiems savo organizacijos darbuotojams, kurie dės sąžiningas pastangas pasiekti abipusį sutarimą dėl atitinkamo klaidos sunkumo lygio. Po pirminės analizės ir atsakymo Palantir pradeda klaidų taisymą ir periodiškai teikia Užsakovui ataskaitas ir atnaujinimus per Status Utility arba, jei Status Utility nėra, el. paštu Užsakovo techninio skyriaus darbuotojams. Jei Užsakovo techninio skyriaus darbuotojai neatsako arba yra nepasiekiami, Palantir gali sumažinti sunkumo lygį vienu lygiu.

#### 4. Error Response

a. Upon receipt of an Error report, Palantir will review and confirm in its reasonable discretion the Severity Level based on the definitions provided in Table 1 and use commercially reasonable efforts to meet the Initial Response Time for the applicable Severity Level set forth in Table 2, as defined for the applicable Regional Business Hours set forth in Table 3. In the event of a conflict between the Customer reported Severity Level and Palantir's reasonable designation, Palantir's designation shall prevail and Palantir will promptly notify Customer of such designation. If Customer provides Palantir a reasonable basis for disagreeing with Palantir's assigned Error Severity Level, each of Customer and Palantir will escalate the disagreement within their respective organizations to personnel positioned to undertake good faith efforts to mutually agree on an appropriate Error Severity Level. Following initial triage and response, Palantir shall begin Error Correction and provide Customer with periodic reports and updates via the Status Utility or, if the Status Utility is not available, to the Customer Technical Contact via email. If the Customer Technical Contact is unresponsive or unreachable, Palantir may downgrade the Severity Level by one level.

| <b>2 lentelė: Atsakymas dėl klaidos sunkumo lygio</b> |                                 |  |   |
|---|---------------------------------|--|---|
| <b>Sunkumo lygis</b>                                  | <b>Pradinis atsakymo laikas</b> | <b>Aprėptis</b>                          | <b>Tikslinio sprendimo palaikymas</b>   |
| P0  | 30 minutės                      | 24x7x365                                 | Klaidos taisymas pradedamas per 1 valandą nuo atsakymo laiko, kol klaida pašalinama arba sumažinamas jos sunkumo lygis. |
| P1  | 8 darbo valandos                | Taikomos vietos (regiono) darbo valandos | Klaidos taisymas pradedamas nuo pirminio atsakymo laiko, kol klaida pašalinama arba sumažinamas jos sunkumo lygis.      |
| P2  | 24 darbo valandos               | Taikomos vietos (regiono) darbo valandos | Klaidų taisymas Palantir nuožiūra atnaujinant produktą  |
| P3  | 60 darbo valandų                | Taikomos vietos (regiono) darbo valandos | Klaidų taisymas Palantir nuožiūra atnaujinant produktą  |

| <b>Table 2: Error Severity Level Response</b> |                              |                                    |  |
|---|------------------------------|------------------------------------|--|
| <b>Severity Level</b>                         | <b>Initial Response Time</b> | <b>Coverage</b>                    | <b>Targeted Resolution Support</b>   |
| P0  | 30 Minutes                   | 24x7x365                           | Error Correction commencing within 1 clock hour of Response Time until Error is resolved or downgraded |
| P1  | 8 Business Hours             | Applicable Regional Business Hours | Error Correction commencing from Initial Response Time until Error is resolved or downgraded.          |
| P2  | 24 Business Hours            | Applicable Regional Business Hours | Error Correction at Palantir's discretion in a Product Update  |
| P3  | 60 Business Hours            | Applicable Regional Business Hours | Error Correction at Palantir's discretion in a Product Update  |

## 5. Palaikymo valandos

- a. P1 - P3 klaidų atveju Užsakovai gali pasirinkti vieną numatytąjį palaikymo regioną, apibrėžtą kaip „Siųsti į“ („Ship to“) vietos Palaikymo regionas (arba geografiškai arčiausiai esantis regionas), nurodytas Užsakymo formoje, arba kaip Šalys yra sutarusios. Jei regionas nėra

## 5. Support Hours

- a. For P1 - P3 Errors, Customers may select one Default Support Region, defined as the Support Region of (or geographically closest to) the “Ship To” location contained in the applicable Order Form, or as otherwise agreed between the Parties. In the absence of a selection, US East shall be the

pasirinktas, „US East“ yra numatytasis Palaikymo regionas. Palaikymo valandos daugiau nei viename Palaikymo regione gali būti perkamos atskirai.

Default Support Region. Support Hours in more than one Support Region may be purchased separately.

| <b>3 lentelė: Palantir palaikymo valandos – P1-P3 klaidos</b> |                                      |  |  |
|---|--------------------------------------|--|--|
| <b>Palaikymo regionas</b>                                     | <b>Vietos (regiono) darbo dienos</b> | <b>Vietos (regiono) darbo valandos</b> | <b>Neįskaitant švenčių</b>                                       |
| GMT   | Pirmadienis–penktadienis             | 09:00–17:00                            | JK nedarbo dienos („bank holidays“); kasmetinis žiemos uždarymas |
| Vidurio Europos laikas<br>( <i>Central European Time</i> )    | Pirmadienis–penktadienis             | 09:00–17:00                            | JK nedarbo dienos („bank holidays“); kasmetinis žiemos uždarymas |
| JAV Rytų laiko juosta<br>( <i>US Eastern Time Zone</i> )      | Pirmadienis–penktadienis             | 09:00–17:00                            | JAV valstybinės šventės; kasmetinis žiemos uždarymas             |
| JAV Vakarų laiko juosta<br>( <i>US Western Time Zone</i> )    | Pirmadienis–penktadienis             | 09:00–17:00                            | JAV valstybinės šventės; kasmetinis žiemos uždarymas             |

| <b>Table 3: Palantir Support Hours P1 - P3 Errors</b> |                               |                                |   |
|---|-------------------------------|--------------------------------|---|
| <b>Support Region</b>                                 | <b>Regional Business Days</b> | <b>Regional Business Hours</b> | <b>Excluded Holidays</b>                    |
| GMT   | Monday - Friday               | 09h00 - 17h00                  | UK Bank Holidays; Annual Winter Closure     |
| Central European Time                                 | Monday - Friday               | 09h00 - 17h00                  | UK Bank Holidays; Annual Winter Closure     |
| US Eastern Time Zone                                  | Monday - Friday               | 09h00 - 17h00                  | US National Holidays; Annual Winter Closure |
| US Western Time Zone                                  | Monday - Friday               | 09h00 - 17h00                  | US National Holidays; Annual Winter Closure |

## 6. Apibrėžtys

- a. **Kasmetinis žiemos uždarymas** – darbo dienos, esančios gruodžio 20 d. ir sausio 10 d. arba tarp šių datų, kuriomis Palantir P1-P3 Palaikymo valandos

## 6. Definitions

- a. **Annual Winter Closure** means the Business Days on or between December 20<sup>th</sup> and January 10<sup>th</sup> on an annual basis in which Palantir offers reduced

yra sutrumpintos. Tikslios datos pranešamos kasmet, ne vėliau kaip prieš du (2) mėnesius ir iš viso negali viršyti dešimties (10) darbo dienų.

- b. **Darbo valandos** – paros valandos tam tikrame Palaikymo regione, kuriomis teikiamas Palantir Palaikymas.
- c. **Darbo dienos** – savaitės dienos tam tikrame Palaikymo regione, kuriomis teikiamas Palantir Palaikymas.
- d. **Užsakovo techninio skyriaus darbuotojai** – iki penkių (5) darbuotojų, kuriuos Užsakovas paskyrė pagrindiniais techniniais Palantir kolegomis, o jų el. pašto adresai įtraukti į Baltąjį sąrašą dėl išplėstų privilegijų, tokių kaip galimybė pateikti pranešimus apie klaidas. Šie darbuotojai turi būti pakankamai gerai susipažinę su Palantir Foundry ir dėti komerciškai pagrįstas pastangas tam, kad užtikrintų, kad klaidos, apie kurias buvo pranešta, neatsirastų dėl jokios taikomos išimties.
- e. **Klaida** – programinės klaidos, defektai ar klaidos Palantir Foundry platformoje, apie kurias pranešė Užsakovo techninio skyriaus darbuotojai.
- f. **Klaidų taisymas** – komerciškai pagrįstos pastangos ištaisyti klaidas, išspręsti problemas arba leisti atnaujinimus tam, kad būtų ištaisytos klaidos.
- g. **Status Utility** – Užsakovui prieinamas tinklalapis, kuriame Palantir gali paskelbti apie esminį darbo proceso efektyvumo sumažėjimą.
- h. **Techninis palaikymas** – techninė pagalba, kurią Palantir teikia Užsakovui asmeniškai, el. paštu, telefonu, patvirtinta nuotoline prieiga ar kitomis techninėmis priemonėmis.

## 7. Išimtys

- a. Palantir neprisiima jokių išipareigojimų ir neatsako už bet kokią nesugebėjimą teikti Palantir palaikymo, skirtą (i) klaidoms, apie kurias pranešta kitaip, nei nurodyta šioje Politikoje, (ii) programinei įrangai,

P1-P3 Support Hours. Exact dates are communicated on an annual basis with no less than two (2) months' notice and shall not exceed ten (10) Business Days in total.

- b. **Business Hours** means hours of the day in a particular Support Region during which Palantir Support is available.
- c. **Business Days** means days of the week in a particular Support Region during which Palantir Support is available.
- d. **Customer Technical Contacts** means up to five (5) personnel designated by Customer as the primary technical counterparts for Palantir, with email addresses whitelisted for escalated privileges, such as filing of Error reports. Customer Technical Contacts must be reasonably familiar with Foundry and shall use commercially reasonable efforts to ensure any reported Errors do not arise from any applicable Exclusion.
- e. **Error** means bugs, defects, or errors in Foundry reported by a Customer Technical Contact.
- f. **Error Correction** means the use of commercially reasonable efforts to correct Errors, provide a workaround, or make available an Update to correct Errors.
- g. **Status Utility** means a Customer accessible web page where material degradations to the performance status of Workflows may be published by Palantir.
- h. **Technical Support** means technical support assistance via in-person, email, telephone, approved remote access or other technical means provided by Palantir to the Customer.

## 7. Exclusions

- a. Palantir will have no obligations to provide, and shall bear no liability for any failure to provide, Palantir Support for (i) Errors reported other than as set forth in this Policy, (ii) Software not

kuri Palantir nuožiūra nėra klasifikuojama kaip visuotinai prieinama, (iii) trečiosios šalies programinei įrangai ar paslaugoms, (iv) Užsakovams, kurie nustato geografinius ar techninius prieigos apribojimus Palantir darbuotojams, v) Užsakovo ar įgalioto vartotojo įrangai; ir (arba) vi) pasirinktiniams scenarijams ar kodui, nepateiktiems Palantir Foundry. Palantir teikiamoms profesionalioms paslaugoms, įskaitant, bet neapsiribojant, duomenų modeliavimą, integravimą, ontologijos konfigūravimą ir mokymą, taikomos Sutarties sąlygos ir nėra įtrauktos į Palantir palaikymą.

classified as Generally Available in Palantir's discretion, (iii) third party software or services, (iv) Customers that impose geographic or technical restrictions on access by Palantir personnel, (v) Customer or Authorized User equipment; and/or (vi) custom scripts or code not provided with Foundry. Professional Services provided by Palantir, including but not limited to data modelling, integration, ontology configuration, and training, are subject to the terms of the Agreement and are excluded from Palantir Support.

## 8. Palantir palaikymo pakeitimai

- a. Palantir retkarčiais gali atnaujinti šią Palaikymo politiką. Tokie pakeitimai gali būti įgyvendinti Palantir nuožiūra, su sąlyga, kad jie nesumažins Palantir palaikymo. Palantir iš anksto raštu praneša apie tokius pakeitimus pasitelkęs dokumentus ir ne vėliau kaip prieš 90 dienų raštu informuoja Užsakovo techninio skyriaus darbuotojus dėl esminių nepalankių pakeitimų. Esminiai nepalankūs Palaikymo politikos pakeitimai įsigalios po 90 dienų pranešimo laikotarpio.
- b. Jei Užsakovas mano, kad pakeitimas daro esminį neigiamą poveikį Užsakovui, ir pakeitimas įvyko ne dėl to, kad Palantir laikėsi galiojančių įstatymų, teisės aktų ar galiojančio teismo įsakymo, Užsakovas gali pranešti Palantir apie savo prieštaravimą dėl tokio pakeitimo per 30 dienų po Palantir pranešimo, ir Užsakovui toliau taikomos tuo metu galiojančios Palaikymo politikos sąlygos, kol (i) baigia galioti arba nutraukiama tuometinė Užsakymo forma arba (ii) keturis (4) mėnesius po to, kai Palantir pateikė pranešimą apie pakeitimą. Užsakovui nepranešus Palantir apie savo prieštaravimą, bus taikoma atnaujinta Palaikymo politika.

[LIKUSI PUSLAPIO DALIS TYČIA PALIKTA TUŠČIAS]

## 8. Palantir Support Changes

- a. Palantir may update this Support Policy from time to time. Such modifications may be implemented at Palantir's discretion, provided that they do not result in a material reduction in Palantir Support. Palantir will provide advance written notice via the Documentation of such modifications with at least 90 days' advance written notice to the Customer Technical Contact for materially adverse modifications. Material adverse changes to the Support Policy will become effective after the 90 day notice period.
- b. If Customer believes that a modification has a material adverse impact on Customer, and the change is not a result of Palantir complying with applicable law, regulation, or a valid court order, then Customer may notify Palantir of its objection to the change within 30 days after Palantir provides notice and Customer will then remain governed by the then-current Support Policy terms until the earlier of (i) the expiration or termination of the then-current Order Form, or (ii) four (4) months after the notice of change was provided by Palantir. If Customer does not notify Palantir of its objection, then the updated Support Policy will apply.

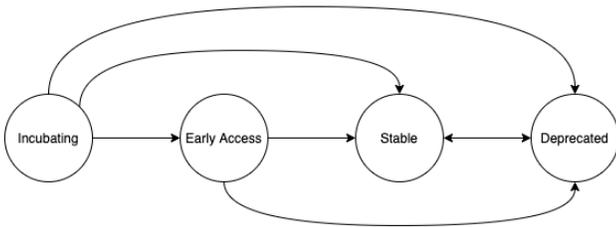
[REST OF PAGE LEFT INTENTIONALLY BLANK]

## Programinės įrangos valdymo politika

*Paskutinį kartą atnaujinta: 2021 m. liepos 15 d.*

### Darbo proceso būsenos perėjimas ir brandumas

Foundry Darbo procesams taikomas žemiau pavaizduotas būsenos perėjimo ir brandumo procesas. Rodyklės (strėlės) rodo leistinus Darbo procesų perėjimus kiekviename brandumo etape. Pavyzdžiui, Inkubavimo Darbo procesai gali būti pakelti iki Išankstinės prieigos arba Bendrai prieinamų, ar Nebenaudojamų. Bendrai prieinami Darbo procesai yra labiau riboti ir gali pereiti tik į Nebenaudojamą būseną.



**Inkubavimo** Darbo procesai – tai tokie procesai, dėl kurių Palantir darbuotojai glaudžiai bendradarbiauja su pasirinktais Užsakovais, kad sukurtų naujo produkto ar koncepcijos prototipą. Netaikomos jokios vykdymo, stabilumo ar palaikymo garantijos. Būsena gali būti pereinama Palantir nuožiūra apie tai pranešus arba nepranešus.

**Išankstinės prieigos** Darbo procesai yra prieinami pasirinktiems Užsakovams per IPP (išsamesnės informacijos ieškokite žemiau) su ribotomis vykdymo, stabilumo ir palaikymo garantijomis. Klaidos gali atsirasti dėl Užsakovo techninių kontaktų, bet netaikomi Palantir Atsakymo į klaidas įsipareigojimai. Būsena gali būti pereinama Palantir nuožiūra apie tai pranešus arba nepranešus.

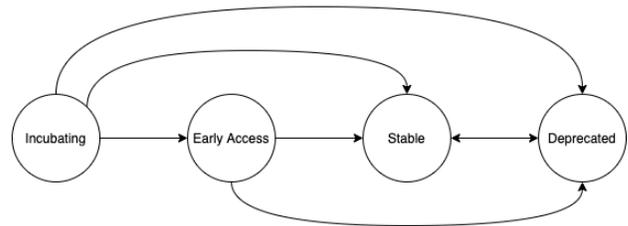
**Bendrai prieinami** Darbo procesai prieinami visiems Užsakovams, turintiems dabartinę prieigą prie Foundry. Taikomos Foundry paslaugų sutartys ir Foundry palaikymo politika. Apie bet kokio Bendrai prieinamo Darbo proceso perėjimą prie

## Palantir Foundry Software Management Policy

*Last Updated: July 15, 2021*

### Workflow State Transition and Maturation

Foundry Workflows are subject to a defined state transition and maturation process as shown below. The arrows indicate the permitted transitions for Workflows in each maturation phase. For example, Incubating Workflows may be elevated to Early Access or Generally Available, or Deprecated. Generally Available Workflows are more restricted and can only transition to Deprecated status.



**Incubating** Workflows are those for which Palantir personnel are partnering closely with select clients to prototype a novel product or concept. No performance, stability, or support guarantees apply. State may be transition in Palantir's discretion with or without notice.

**Early Access** Workflows are made available to select Customers through the EAP (see below for further details) with limited performance, stability, and support guarantees. Errors may be raised by Customer Technical Contacts but Palantir's Error Response obligations do not apply. State may be transition in Palantir's discretion with or without notice.

**Generally Available** Workflows are available to all Customers with current access to Foundry. Foundry SLAs and the Foundry Support Policy apply. A transition of any Generally Available Workflow to Deprecated shall be communicated by Palantir with at least 6 months' prior written notice to Customers. Foundry SLAs and the Foundry Support Policy shall continue to apply until the conclusion of the applicable

Nebenaudojamo Palantir informuoja Užsakovus ne vėliau kaip prieš 6 mėnesius raštu. Foundry paslaugų sutartys ir Foundry palaikymo politika ir toliau taikomos iki galiojančio įspėjimo laikotarpio pabaigos.

**Nebenaudojami** Darbo procesai yra tie procesai, kuriuos Palantir mažina arba pašalina iš Foundry. Pabrėžtinai rekomenduojama jų vengti. Jei Darbo procesai iš Inkubavimo ar Išankstinės prieigos perjungti tiesiai į Nebenaudojamus, netaikomos jokios vykdymo, stabilumo ar palaikymo garantijos. Bendrai prieinamiems Darbo procesams ir toliau 6 mėnesius nuo perėjimo prie Nebenaudojamų taikomos Foundry paslaugų sutartys bei Foundry palaikymo politika. Pavyzdžiui, jei Palantir 2021 m. sausio 1 d. praneša apie A Darbo proceso perėjimą iš Bendrai prieinamo prie Nebenaudojamo, toks perėjimas įvyks 2021 m. liepos 1 d. ar maždaug tuo metu, ir toliau, iki 2021 m. gruodžio 31 d., bus taikomos Paslaugų sutartys ir Palaikymo politika. Nuo 2022 m. sausio 1 d. A Darbo procesui nebus taikomos jokios vykdymo, stabilumo ar palaikymo garantijos.

### **Išankstinės prieigos programa (IPP)**

Palantir siūlo IPP, skirtą Išankstinės prieigos Darbo procesams Užsakovams pasirinkti, žinant, kad tokiems Darbo procesams taikomos ribotos vykdymo, stabilumo ir palaikymo garantijos ir kad jie niekada nebus prieinami kaip Bendrai prieinami Darbo procesai. Darbo procesai, prieinami per IPP, gali keistis Palantir nuožiūra be įspėjimo.

### **Produkto perkėlimai ir nusidėvėjimai**

Jei Visuotinai prieinamam Darbo procesui reikalingas Užsakovo atliekamas perkėlimas į naują versiją, pavyzdžiui, dėl sugadintų IPP pakeitimų, Palantir pateikia Užsakovui išteklių ir artefaktų, kuriuos reikia toliau naudoti, sąrašą. Prireikrus Palantir pateiks tokią pranešimą apie šiuos minimalius informavimo laikotarpius:

notice period.

**Deprecated** Workflows are those for which Palantir is reducing or removing from Foundry. Use is strongly discouraged. For Workflows transitioned directly to Deprecated from Incubating or Early Access, no performance, stability, or support guarantees apply. For Generally Available Workflows, Foundry SLAs and Foundry Support Policy shall continue to apply for a period of 6 months following transition to Deprecated. By way of example, if Palantir provides notice of a transition of Workflow A from Generally Available to Deprecated on January 1, 2021, such transition would occur on or around July 1, 2021, with continued applicability of SLAs and Support Policy until December 31, 2021. From January 1, 2022, no performance, stability, or support guarantees would apply to Workflow A.

### **Early Access Program (“EAP”)**

Palantir offers an EAP for Early Access Workflows to select Customers with understanding that such Workflows are subject to limited performance, stability, and support guarantees and may never be made available as Generally Available Workflows. Workflows made available through the EAP may change in Palantir’s discretion without notice.

### **Product Migrations and Deprecations**

Where a Generally Available Workflow requires Customer-actioned migration to a new version, for example because of breaking API changes, Palantir shall provide Customer with a list of Customer-created resources and artifacts that require action for continued use. Where applicable, Palantir will provide such notice on the following minimum notification periods:

| Inkubavimas | Išankstinė prieiga | GA           | Nebenaudojamas |
|-------------|--------------------|--------------|----------------|
| Nėra        | Nėra               | > 6 mėnesiai | > 2 mėnesiai   |

| Incubation | Early Access | GA         | Deprecated |
|------------|--------------|------------|------------|
| None       | None         | > 6 months | > 2 months |

Palantir pasilieka teisę pranešti Užsakovui apie pagreitintą perkėlimo laiką, jei iškyla kritinių saugumo, platformos stabilumo ar su veikla susijusių problemų, kiekvienas pagrįstai nustatomas Palantir nuožiūra.

### Planinė priežiūra

Siekdami užtikrinti Palantir galimybę pristatyti saugiausią, efektyviausią Foundry versiją, pasilikame teisę atlikti Planinę priežiūrą pagal nustatytą dažnį arba *ad hoc*, kai taikomos tam tikros sąlygos.

**Planinė priežiūra** atliekama kiekvieno kalendorinio mėnesio pirmąjį šeštadienį 10 val. GMT ir tęsiasi (2) valandas. Planinės priežiūros laikas ir diena gali būti pakeisti Palantir nuožiūra, apie tai įspėjus ne vėliau kaip prieš (2) mėnesius. Tuo atveju, jei Palantir reikia daugiau nei (2) valandų prastovos individualiam priežiūros laikotarpiui, Palantir informuoja apie tai Užsakovą prieš (2) mėnesius.

**Planinė avarinė priežiūra** įvyksta su informacijos saugumu susijusio įvykio atveju arba privalomo avarinio atkūrimo iš atsarginės kopijos atveju. Palantir pasilieka teisę skelbti skubią prastovą situacijai ištaisyti, tačiau apie tai kiek įmanoma anksčiau informuoja Užsakovą.

Palantir reserves the right to provide Customer notice of accelerated migration timelines in the event of critical security, platform stability, or operational issues, each as reasonably determined in Palantir's discretion.

### Scheduled Maintenance

To ensure Palantir's ability to deliver the most secure, performant version of Foundry, we reserve the right to conduct Scheduled Maintenance on a defined cadence or on an ad hoc basis, where certain conditions apply.

**Scheduled Maintenance** shall occur during each calendar month on the first Saturday of such month at 10h00 GMT for a duration of (2) hours. The time and day of the Scheduled Maintenance may be changed in Palantir's discretion with no less than (2) months' advance notice. In the event that Palantir needs more than (2) hours of downtime for an individual maintenance window, Palantir will provide the client with (2) months' advance notice.

**Emergency Scheduled Maintenance** shall occur event of an information security-related event or in the event of a mandatory emergency restore from backup. Palantir reserves the right to take immediate downtime to remedy the situation but will notify the Client as far in advance as possible.

Esant reikalavimų nesuderinamumui, prioritetas teikiamas labiausiai ribojančiam reikalavimui.

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](mailto:info@stat.gov.lt)  
<http://www.stat.gov.lt>

DocuSigned by:



865EE2A7E4AE40D...

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](mailto:info@stat.gov.lt)  
<http://www.stat.gov.lt>

DocuSigned by:



865EE2A7E4AE40D...

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.: 41036032  
IBAN: GB09CHAS60924241036032  
SWIFT: CHASDEFX  
Tel. +44 7408 886228  
El. p. [legalnotices@palantir.com](mailto:legalnotices@palantir.com)

DocuSigned by:



57785BE12322446...

Tadas Rudzevicius, 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: 41036032  
IBAN: GB09CHAS60924241036032  
SWIFT: CHASDEFX  
Phone No. +44 7408 886228  
E-mail: [legalnotices@palantir.com](mailto:legalnotices@palantir.com)

DocuSigned by:



57785BE12322446...

Tadas Rudzevicius, Authorised Signatory

Valstybės duomenų valdysenos informacinės sistemos licencijos (Palantir Foundry) pratęsimo pirkimo sutarties Nr. STAT-(2021) 2 priedas

Renewal of the License of the State Data Governance Information System (Palantir Foundry) Purchase Contract No STAT (2021) Annex 2

## ASMENS DUOMENŲ IR INFORMACIJOS TVARKYMAS

Atsižvelgdamos į tai, kad vykdydamas pirkimo sutartį Tiekėjas gali matyti asmens duomenis, šalis siekia užtikrinti asmens duomenų apsaugą ir atitikti 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. Šalis 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. Šalis pažymi, jog Tiekėjo grupė išimtinai nesiekia tvarkyti asmens duomenų, tačiau asmens duomenų tvarkymo veiksmams gali būti neatskiriamai reikalingi, siekiant tinkamai (į)vykdyti Sutartį.

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

2.4. Šalis 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 section 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, 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 section 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 section 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 section 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 išdėstytose 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 ir užsieniečių asmens duomenys, gauti iš administracinių duomenų šaltinių.<br>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: <ul style="list-style-type: none"> <li>○ Asmens duomenų iš administracinių duomenų šaltinių ir Užsakovo duomenų bazių išgavimas ir integravimas;</li> <li>○ sugadintų programinės įrangos duomenų (įskaitant asmens duomenis) atstatymas;</li> <li>○ sistemos veiklos atkūrimas, visiško ar dalinio funkcionavimo sutrikimo atvejais;</li> <li>○ sistemos įvykių žurnalo analizė.</li> </ul> |

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 section 2.4 of the Annex, the data provided by the Customer in particular case are insufficient for proper implementation of the purpose provided in section 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 and non-residents received from the administrative data sources.<br>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: <ul style="list-style-type: none"> <li>○ Extraction of personal data from administrative data sources and the Customer's databases and integration.</li> <li>○ Recovery of corrupted software data (including personal data).</li> <li>○ System recovery in cases of complete or partial malfunction.</li> <li>○ System event log analysis.</li> </ul> |

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 section 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 section 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 subtiekiejus (subteikėjus) asmens duomenims tvarkyti. Jeigu pirkimo sutartyje nenustatytos kitos sąlygos, prieš pasitelkdamas naują arba pakeisdamas esamą subtiekieją (subteikėją), Tiekėjo grupė iš anksto apie tai raštu turi informuoti Užsakovą, pateikdamas planuojamo pasitelkti subtiekiejo (subteikėjo) rekvizitus ir kitą informaciją, susijusią su duomenų tvarkymo veikla, kurios pareikalavus Užsakovas. Kai Tiekėjo grupė konkrečiai asmens duomenų tvarkymo veiklai atlikti pasitelkia subtiekieją (subteikėją), Sutartimi (Priedu) tam kitam subtiekiejui (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 subteikėjas (subteikėjas) nevykdo duomenų apsaugos prievolių, Tiekėjo grupė išlieka visiškai atsakinga Užsakovui už to subtiekiejo (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   |
|--|--|---|
| <i>Amazon Web Services, Inc. (AWS)</i> | 410 Terry Avenue North, Sietlas, Vašingtono valstija, 98109, JAV | AWS teikia debesų infrastruktūrą <i>Palantir</i> produktams.  |
| <i>Proofpoint, Inc.</i>                | 892 Ross Drive, Saniveilas, Kalifornija, 94089, JAV              | <i>Proofpoint</i> teikia įspėjimų ir užšifruotų pranešimų <i>Palantir Foundry</i> platformoje palaikymą.                    |
| <i>Microsoft Corporation</i>           | One Microsoft Way, Redmondas, Vašingtono valstija, JAV, 98052    | Teikia debesų infrastruktūrą, skirtą <i>Active Directory</i> tarnybai, reikalingai <i>CentralAuth</i> 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 and 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. Atsižvelgdama 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 pasirinktą ir nustatytas technines ir organizacines priemones, reikalingas Priedo 2.1 papunktyje nurodytam tikslui bei tinkamam saugumui pasiekti, tačiau tokios priemonės bet kokių 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 nustatytą 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 TVARKYMOUI

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 skaitmeninės 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 section 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 sections 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 išpėjimo 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 Pagalbiniam 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 Group“ 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 (5) 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) Supplier 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 kokių 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, atsižvelgdama 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, iširti 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](mailto:info@stat.gov.lt)  
<http://www.stat.gov.lt>

DocuSigned by:

*Dr. Jūratė Petrauskienė*

865EE2A7E4AE40D...

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.: 41036032  
IBAN: GB09CHAS60924241036032  
SWIFT: CHASDEFX  
Tel. +44 7408 886228  
El. p. [legalnotices@palantir.com](mailto:legalnotices@palantir.com)

DocuSigned by:

*Tadas Rudzevičius*

57785BE12322446...

Tadas Rudzevičius, 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](mailto:info@stat.gov.lt)  
<http://www.stat.gov.lt>

DocuSigned by:

*Dr. Jūratė Petrauskienė*

865EE2A7E4AE40D...

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: 41036032  
IBAN: GB09CHAS60924241036032  
SWIFT: CHASDEFX  
Phone No. +44 7408 886228  
E-mail: [legalnotices@palantir.com](mailto:legalnotices@palantir.com)

DocuSigned by:

*Tadas Rudzevičius*

57785BE12322446...

Tadas Rudzevičius, Authorised Signatory

Valstybės duomenų valdysenos  
informacinės sistemos licencijos (Palantir  
Foundry) pratęsimo pirkimo sutarties  
Nr. STAT-117 (2021)  
3 priedas

Renewal of the License of the State Data  
Governance Information System (Palantir  
Foundry) Purchase Contract  
No STAT-117 (2021)  
Annex 3

## SUSITARIMAS DĖL INFORMACIJOS NEATSKLEIDIMO

Šis Susitarimas dėl informacijos neatskleidimo (toliau – Susitarimas) sudaromas tarp i) Palantir Technologies UK, Ltd. (toliau – Tiekėjas) ir ii) šalies, šio Susitarimo pasirašymo puslapyje nurodytos kaip Užsakovas (toliau – Užsakovas), nuo šio Susitarimo pasirašymo puslapyje nurodytos dienos (toliau – Įsigaliojimo diena), siekiant apsaugoti tam tikrą konfidencialią informaciją, kuri Užsakovo su Tiekėju sudaryta Sutartimi patvirtinta tvarka atskleidžiama išimtinai Užsakovo prijungimo prie duomenų valdymo platformos (toliau – Platforma) bei vėlesnės jos prieigos prie šios Platformos ir naudojimosi ja tikslais (toliau – Leistinas naudojimas).

Kiekviena žemiau pasirašiusi šalis (toliau – Informaciją gaunanti šalis) supranta, kad kita šalis (toliau – Informaciją atskleidžianti šalis) atskleidė arba gali atskleisti informaciją, susijusią su Informaciją atskleidžiančios šalies veikla, o tokia anksčiau, dabar ar vėliau Informaciją gaunančiai šaliai atskleista informacija toliau šiame Susitarime vadinama Informaciją atskleidžiančios šalies „Nuosavybės teise saugoma informacija“. Informaciją atskleidžiančios šalies atskleidžiama Nuosavybės teise saugoma informacija gali apimti (be apribojimų): a) patentus ir patentų paraiškas; b) komercines paslaptis; c) nuosavybės teise saugomą ir konfidencialią informaciją, pavyzdžiui, informaciją apie programines įrangos programas, eskizus, brėžinius, algoritmus, praktinę patirtį (angl. *knowhow*), formules, procesus, idėjas, metodus, išradimus (tiek patentuojamus, tiek nepatentuojamus), schemas, modelius, prietaisus, įrangą, autorinius kūrinius ir kitus techninius, verslo, finansinius, investavimo, teisinius, klientų ir produktų kūrimo planus, prognozes, santykius, strategijas ir informaciją, informaciją, gaunamą iš Informaciją atskleidžiančios šalies klientų ar susijusių su jais; taip pat d) visą kitą informaciją, kurią Informaciją gaunanti šalis žinojo ar pagrįstai turėjo žinoti esant Informaciją atskleidžiančios šalies Nuosavybės teise saugoma informacija.

Atsižvelgdamos į Informaciją gaunančios šalies galimybę susipažinti su Informaciją atskleidžiančios šalies Nuosavybės teise saugoma informacija, Šalys susitaria:

1. Informaciją gaunanti šalis sutinka: a) visais atvejais, nepaisant šio susitarimo nutraukimo ar galiojimo pabaigos, laikyti Informaciją atskleidžiančios šalies Nuosavybės teise saugomą informaciją konfidencialia; b) neatskleisti tokios Nuosavybės teise saugomos informacijos ar bet kokios su ja susijusios informacijos jokiems tretiesiems asmenims; c) imtis pagrįstų atsargumo priemonių, kad apsaugotų tokią Nuosavybės teise saugomą informaciją (įskaitant visas atsargumo priemones, kurias Informaciją gaunanti šalis taiko savo konfidencialiai medžiagai, tačiau jomis neapsiribojant); d) jokiais atvejais nenaudoti Nuosavybės teise saugomos informacijos jokiais kitais nei Leistino naudojimo tikslais; e) nekopijuoti ir apgrąžos inžinerijos būdu neanalizuoti (angl. *reverse engineer*) tokios Nuosavybės teise saugomos informacijos; f) neeksportuoti ir nereeksportuoti (kaip apibrėžta galiojančiuose Lietuvos Respublikos ar kituose eksporto kontrolės įstatymuose ar kituose teisės aktuose (toliau – Eksporto įstatymai)) tokios Nuosavybės teise saugomos informacijos ar jos produktų pažeidžiant Eksporto įstatymus; ir g) suteikti prieigą prie Nuosavybės teise saugomos informacijos tik tiems pareigūnams, direktoriams, darbuotojams, konsultantams ar atstovams, kuriems ji yra būtina ir kurie yra pasirašę

## MUTUAL NON-DISCLOSURE AGREEMENT

This Non-Disclosure Agreement (the “Agreement”) is entered into by and between (i) Palantir Technologies UK, Ltd. (the “Supplier”) and (ii) the party set forth on the signature page to this Agreement under the heading “Customer” (the “Customer”) as of the effective date set forth on the signature page to this Agreement (the “Effective Date”), to protect the confidentiality of certain information disclosed solely in relation to the onboarding of the Customer to the data management platform (the “Platform”) and the Customer’s subsequent access to and use of that Platform, as provided by the Supplier and endorsed by Customer under its Contract with Supplier (the “Permitted Use”).

Each undersigned party (the “Receiving Party”) understands that the other party (the “Disclosing Party”) has disclosed or may disclose information relating to the Disclosing Party’s business, which to the extent previously, presently or subsequently disclosed to the Receiving Party is hereinafter referred to as “Proprietary Information” of the Disclosing Party. Proprietary Information disclosed by the Disclosing Party may include, without limitation: (a) patents and patent applications; (b) trade secrets; (c) proprietary and confidential information, such as software programs, sketches, drawings, algorithms, know-how, formulas, processes, ideas, techniques, inventions (whether patentable or not), schematics, models, apparatuses, equipment, works of authorship, and other technical, business, financial, investor, legal, customer and product development plans, forecasts, relationships, strategies and information, information from or pertaining to the Disclosing Party’s customers; and (d) all other information that the Receiving Party knew, or reasonably should have known, was the Proprietary Information of the Disclosing Party.

In consideration of any access of the Receiving Party to Proprietary Information of the Disclosing Party, the Parties hereby agree as follows:

1. The Receiving Party agrees: (a) to hold the Disclosing Party’s Proprietary Information in confidence at all times and notwithstanding any termination or expiration of this agreement; (b) not to divulge any such Proprietary Information or any information derived therefrom to any third person; (c) to take reasonable precautions to protect such Proprietary Information (including, without limitation, all precautions the Receiving Party employs with respect to its own confidential materials); (d) not to make any use whatsoever at any time of such Proprietary Information other than the Permitted Use; (e) not to copy or reverse engineer any such Proprietary Information; (f) not to export or reexport (within the meaning of any applicable Republic of Lithuania or other export control laws or regulations (the “Export Laws”)) any such Proprietary Information or product thereof in violation of any Export Laws; and (g) to limit access to the Proprietary Information to only those officers, directors, employees, consultants or agents having a need to know and who have signed confidentiality agreements containing, or are otherwise bound by, confidentiality obligations at least as restrictive as those in this (the “Authorised Representatives”). The Receiving Party shall be responsible and liable for any improper use of the Proprietary Information or any breach of this Agreement by any Authorised Representative.

konfidencialumo susitarimus, nustatančius konfidencialumo įsipareigojimus (ar yra kitaip įsipareigoję jų laikytis), numatančius ne mažesnius nei šiame Susitarime nurodyti apribojimai (toliau – Įgalioji atstovai). Informaciją gaunanti šalis prisiima atsakomybę tuo atveju, jei bet kuris Įgaliojtas asmuo netinkamai naudoja Nuosavybės teise saugomą informaciją ar pažeidžia šį Susitarimą.

2. Informaciją atskleidžianti šalis, nesuteikdama jokių teisių ar leidimų, sutinka, kad aukščiau išdėstytos nuostatos netaikomos informacijai, kuri: a) yra arba tampa (ne dėl Informaciją gaunančios šalies ar su ja susijusių asmenų, jos atstovų, konsultantų ar darbuotojų netinkamų veiksmų ar neveikimo) viešai prieinama; b) kuria Informaciją gaunanti šalis be apribojimų disponavo ar kurią ji žinojo prieš gaudama šią informaciją iš Informaciją atskleidžiančios šalies; c) kurią Informaciją gaunančiai šaliai teisėtai ir be apribojimų atskleidė trečiasis asmuo; arba d) kurią savarankiškai sukūrė Informaciją gaunančios šalies darbuotojai, neturintys galimybės susipažinti su Informaciją atskleidžiančios šalies Nuosavybės teise saugoma informacija, nesinaudodami tokia Nuosavybės teise saugoma informacija.

3. Informaciją gaunanti šalis, nepažeisdama Susitarime nustatytų įsipareigojimų, gali atskleisti Nuosavybės teise saugomą informaciją, kurią atskleisti reikalauja galiojantis teismo ar kitos jurisdikciją turinčios vyriausybės institucijos sprendimas, su sąlyga, kad Informaciją gaunanti šalis a) Informaciją atskleidžiančiai šaliai pateikia pagrįstą išankstinį rašytinį pranešimą apie tokios informacijos atskleidimą; ir b) kruopščiai ir pagrįstai stengiasi apriboti informacijos atskleidimą bei užtikrinti arba padėti Informaciją atskleidžiančiai šaliai užtikrinti atskleidžiamos informacijos konfidencialumą ar gauti teismo nutartį dėl apsaugos priemonių, užkertančių kelią ar apribojančių informacijos atskleidimą, kiek tai netrukdo Informaciją atskleidžiančiai šaliai dalyvauti procese.

4. Informaciją gaunanti šalis nedelsdama praneša Informaciją atskleidžiančiai šaliai apie bet kokį Nuosavybės teise saugomos Informacijos praradimą ar neteisėtą atskleidimą.

5. Informaciją atskleidžiančiai šaliai bet kuriuo metu pateikus rašytinį prašymą, Informaciją gaunanti šalis nedelsdama perduoda Informaciją atskleidžiančiai šaliai visą Informaciją atskleidžiančios šalies Nuosavybės teise saugomą informaciją ir visus dokumentus ar laikmenas, kuriuose yra tokios Nuosavybės teise saugomos informacijos, bei visas jų kopijas ar išrašus.

6. Informaciją gaunanti šalis supranta, kad jokia šio Susitarimo nuostata a) nereikalauja atskleisti jokios Informaciją atskleidžiančios šalies Nuosavybės teise saugomos informacijos; b) neįpareigoja Informaciją atskleidžiančios šalies sudaryti kokius nors sandorius ar santykius; c) neįpareigoja nė vienos iš šalių sudaryti papildomą susitarimą su kita šalimi (išskyrus atvejus, kiek tai reglamentuoja šis Susitarimas). Jokia šio Susitarimo nuostata nesukuria ir nebus laikoma sukuriančia šalių darbo santykius, jungtinę veiklą ar atstovavimo santykius.

7. Bet kokios Nuosavybės teise saugomos informacijos kopijos bus Informaciją atskleidžiančios šalies nuosavybė ir joms taikomi visi originaluose esantys nurodymai bei informacija apie konfidencialumą ar nuosavybės teisę, nebent Informaciją atskleidžianti šalis raštu nurodytų kitaip.

8. INFORMACIJĄ ATSKLEIDŽIANTI ŠALIS NUOSAVYBĖS TEISE SAUGOMĄ INFORMACIJĄ PATEIKIA TOKIĄ, KOKIA JI YRA, IR INFORMACIJĄ GAUNANTI ŠALIS NAUDOJA JĄ SAVO RIZIKA. INFORMACIJĄ ATSKLEIDŽIANTI ŠALIS NETEIKIA JOKIŲ TIESIOGINIŲ, NETIESIOGINIŲ AR ĮSTATYMUOSE NUMATYTŲ GARANTIJŲ.

2. Without granting any right or licence, the Disclosing Party agrees that the foregoing shall not apply with respect to any information that: (a) is or becomes (through no improper action or inaction by the Receiving Party or any affiliate, agent, consultant or employee of the Receiving Party) generally available to the public; (b) was in the Receiving Party's possession or known by it without restriction prior to receipt from the Disclosing Party; (c) was rightfully disclosed to the Receiving Party by a third party without restriction; or (d) was independently developed without use of any Proprietary Information of the Disclosing Party by employees of the Receiving Party who have had no access to any such Proprietary Information.

3. The Receiving Party may, without violating the obligations of the Agreement, disclose Proprietary Information to the extent required by a valid order by a court or other governmental body having jurisdiction, provided that the Receiving Party: (a) provides the Disclosing Party with reasonable prior written notice of such disclosure; and (b) uses diligent reasonable efforts to limit disclosure and to obtain, or to assist the Disclosing Party in obtaining, confidential treatment or a protective order preventing or limiting the disclosure, while allowing the Disclosing Party to participate in the proceeding.

4. The Receiving Party will immediately notify the Disclosing Party in the event of any loss or unauthorised disclosure of any Proprietary Information.

5. Upon written request by the Disclosing Party at any time, the Receiving Party will promptly turn over to the Disclosing Party all Proprietary Information of the Disclosing Party and all documents or media containing any such Proprietary Information and any and all copies or extracts thereof.

6. The Receiving Party understands that nothing herein: (a) requires the disclosure of any Proprietary Information of the Disclosing Party; (b) requires the Disclosing Party to proceed with any transaction or relationship; or (c) shall result in any obligation on the part of either party to enter into any further agreement with the other (except the cases which are regulated by this Agreement). Nothing in this Agreement creates or shall be deemed to create any employment, joint venture, or agency between the parties.

7. Any reproduction of any Proprietary Information will remain the property of the Disclosing Party and will contain any and all confidential or proprietary notices or legends that appear on the original, unless otherwise authorised in writing by the Disclosing Party.

8. THE DISCLOSING PARTY IS PROVIDING PROPRIETARY INFORMATION ON AN "AS IS" BASIS FOR USE BY THE RECEIVING PARTY AT ITS OWN RISK. THE PARTY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS, IMPLIED OR STATUTORY.

9. Nė viena šalis nesinaudos kitos šalies vardu naujoje verslo veikloje, neleis ir neplatins jokių skelbimų, pareiškimų, pranešimų spaudai ar kitos reklaminės ar rinkodaros medžiagos, susijusios su šiuo Susitarimu, bei kitaip nenaudos kitos šalies prekių ženklų, paslaugų ženklų, prekių pavadinimų, logotipų, domenų vardų ar kitos informacijos apie šaltinį, sąsajas ar rėmimą, kiekvienu atveju negavusi išankstinio aiškaus rašytinio kitos šalies sutikimo.

10. Šis Susitarimas galioja 3 (trejus) metus nuo Įsigaliojimo dienos (toliau – Galiojimo laikotarpis). Be to, bet kuri šalis gali bet kada nutraukti šį Susitarimą, raštu įspėjusi kitą šalį apie tai prieš 30 (trisdešimt) dienų. Informaciją gaunančios šalies įsipareigojimai saugoti Galiojimo laikotarpiu gautą Nuosavybės teise saugomą informaciją galioja 5 (penkerius) metus nuo šio Susitarimo nutraukimo ar galiojimo pabaigos. Informaciją gaunančios šalies įsipareigojimai pagal šį Susitarimą bus privalomi jos įpėdiniais, veiklos tęsėjams ir teisėtiems teisių perėmėjams. Nepaisant jokių priešingų šio Susitarimo nuostatų, Informaciją gaunančios šalies įsipareigojimai dėl visos Nuosavybės teise saugomos informacijos, kuri sudaro Informaciją atskleidžiančios šalies komercinę paslaptį, liks galioti ir po šio Susitarimo nutraukimo ar galiojimo pabaigos tol, kol tokia informacija bus komercine paslaptimi.

11. Šio Susitarimo atsisakymas ar pakeitimas yra privalomas šaliai tik tuo atveju, jei jis sudaromas raštu ir jį pasirašo tinkamai įgaliotas tos šalies atstovas, o nepasinaudojimas teise ar delsimas ją pasinaudoti nebus laikomas teisės atsisakymu.

12. Informaciją gaunanti šalis pripažįsta ir sutinka, kad dėl Informaciją atskleidžiančios šalies Nuosavybės teise saugomos informacijos unikalumo gali nebūti tinkamų teisių gynimo priemonių jos įsipareigojimų pagal šį Susitarimą pažeidimo atveju, dėl kurio Informaciją atskleidžiančiai šaliai gali būti padaryta nepataisoma žala, todėl, įvykus tokiam pažeidimui ar iškilus tokio pažeidimo grėsmei, be įstatymuose numatytų teisių gynimo priemonių, Informaciją atskleidžianti šalis turi teisę teismo reikalauti įpareigoti Informaciją gaunančią šalį atlikti tam tikrus pažeidimą užkertančius veiksmus ar sustabdyt pažeidimo veiksmus, netaikant nuostolių, galinčių atsirasti dėl šio įpareigojimo, atlyginimo užtikrinimo instituto.

13. Tuo atveju, jei bet kurios iš šio Susitarimo nuostatų teismo ar kitos kompetentingos jurisdikcijos institucijos būtų pripažintos neteisėtomis, negaliojančiomis ar neįgyvendinamomis, tokios nuostatos apribojamos ar pašalinamos tiek, kiek yra būtina, kad šis Susitarimas toliau galėtų visa apimtimi. Visi pranešimai, kuriuos leidžiama arba reikalaujama pateikti pagal šį Susitarimą, turi būti parengti raštu ir pateikti įteikiant asmeniškai, elektroniniu paštu, faksu arba užsakomuoju ar registruotu laišku su gavimo patvirtinimu, ir bus laikomi pateiktais įteikus asmeniškai, praėjus 5 (penkioms) dienoms nuo išsiuntimo paštu arba patvirtinus jų gavimą elektroniniu būdu. Pranešimai siunčiami šio Susitarimo pabaigoje nurodytais adresais arba kitu bet kurios šalies raštu nurodytu adresu. Šį Susitarimą reglamentuoja Lietuvos Respublikos įstatymai, neatsižvelgiant į jų nuostatas dėl teisės normų kolizijos.

14. Šis Susitarimas sudarytas dviem vienodą juridinę galią turinčiais egzemplioriais anglų ir lietuvių kalbomis. Esant prieštaravimų ar neatitikimų tarp šio Susitarimo teksto anglų ir lietuvių kalbomis, vadovaujamosi tekstu anglų kalba.

Šis Susitarimas sudaro visą šalių susitarimą dėl šio Susitarimo dalyko.

Tai patvirtindamos šalys įformino šį Susitarimą toliau nurodytą Įsigaliojimo dieną.

9. Neither party shall use the other party as a reference for new business, or issue or release any announcement, statement, press release or other publicity or marketing materials relating to this Agreement or otherwise use the other party's trademarks, service marks, trade names, logos, domain names or other indicia of source, affiliation or sponsorship, in each case, without obtaining the prior express written consent of the other party.

10. This Agreement will terminate 3 (three) years after the Effective Date (the "Term"). Furthermore, this Agreement may be terminated by either party at any time upon 30 (thirty) days' written notice to the other party. The Receiving Party's obligations to protect Proprietary Information received during the Term shall continue for 5 (five) years after termination or expiration of this Agreement. The Receiving Party's obligations under this Agreement will be binding upon its heirs, successors, and permitted assigns. Notwithstanding anything to the contrary herein, the Receiving Party's obligations with respect to all Proprietary Information which is a trade secret of the Disclosing Party will survive any termination or expiration of this Agreement for so long as such information remains a trade secret.

11. No waiver or modification of this Agreement will be binding upon a party unless made in writing and signed by a duly authorised representative of such party and no failure or delay in enforcing any right will be deemed a waiver.

12. The Receiving Party acknowledges and agrees that due to the unique nature of the Disclosing Party's Proprietary Information, there can be no adequate remedy at law for any breach of its obligations hereunder, which breach may result in irreparable harm to the Disclosing Party, and therefore, that upon any such breach or any threat thereof, the Disclosing Party shall be entitled to appropriate equitable relief, without the requirement of posting a bond, in addition to whatever remedies it might have at law.

13. In the event that any of the provisions of this Agreement shall be held by a court or other tribunal of competent jurisdiction to be illegal, invalid or unenforceable, such provisions shall be limited or eliminated to the minimum extent necessary so that this Agreement shall otherwise remain in full force and effect. All notices permitted or required under this Agreement shall be in writing and shall be delivered by personal delivery, electronic mail, facsimile transmission or by certified or registered mail, return receipt requested, and will be deemed given upon personal delivery, 5 (five) days after deposit in the mail, or upon acknowledgment of receipt of electronic transmission. Notices will be sent to the addresses set forth at the end of this Agreement or such other address as either party may specify in writing. This Agreement shall be governed by the laws of the Republic of Lithuania without regard to the conflicts of law provisions thereof.

14. This agreement is drawn up in duplicate in English and Lithuanian language, each having equal legal force. In the event of inconsistency or discrepancy between the English version and Lithuanian version of this Agreement, the English version shall prevail.

This Agreement constitutes the entire agreement between the parties with respect to the subject matter hereof.

In Witness Whereof, the parties have caused this Agreement to be executed as of the Effective Date set forth below.

**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](mailto:info@stat.gov.lt)  
<http://www.stat.gov.lt>

DocuSigned by:

*Dr. Jūratė Petrauskienė*

865EE2A7E4AE40D...

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.: 41036032  
 IBAN: GB09CHAS60924241036032  
 SWIFT: CHASDEFX  
 Tel. +44 7408 886228  
 El. p. [legalnotices@palantir.com](mailto:legalnotices@palantir.com)

DocuSigned by:

*Tadas Rudzevicius*

57785BE12322446...

Tadas Rudzevicius, įgaliotasis asmuo

**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](mailto:info@stat.gov.lt)  
<http://www.stat.gov.lt>

DocuSigned by:

*Dr. Jūratė Petrauskienė*

865EE2A7E4AE40D...

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: 41036032  
 IBAN: GB09CHAS60924241036032  
 SWIFT: CHASDEFX  
 Phone No. +44 7408 886228  
 E-mail: [legalnotices@palantir.com](mailto:legalnotices@palantir.com)

DocuSigned by:

*Tadas Rudzevicius*

57785BE12322446...

Tadas Rudzevicius, Authorised Signatory