DocuSign Envelope ID: 5A45EFF2-9542-436F-B64A-A4C98DF04360

Palantir Foundry licencijos išplėtimo
papildomais infrastruktūros ištekliais pirkimo
sutarties Nr. STAT (2023)
1 priedas

The Extension of the Palantir Foundry license
with additional infrastructure resources
purchase contract No STAT (2023)
Annex 1

PALANTIR FOUNDRY LICENCIJOS IŠPLĖTIMO PAPILDOMAIS INFRASTRUKTŪROS IŠTEKLIAIS TECHNINĖ SPECIFIKACIJA

TECHNICAL SPECIFICATION FOR THE EXTENSION OF THE PALANTIR FOUNDRY LICENSE WITH ADDITIONAL INFRASTRUCTURE RESOURCES

DocuSign Envelope ID: 5A45EFF2-9542-436F-B64A-A4C98DF04360

TURINYS

1. Sąvokos ir santrumpos.....3

2. Įvadinė informacija.....4

3. Reikalavimai skaičiavimo ištekliams.....10

4. Reikalavimai papildomai duomenų valdymo platformos (DVP) infrastruktūrai.....10

5. Reikalavimai saugumui.....13

CONTENT

1. Terms and abbreviations……..3

2. Introductory information……..4

3. Requirements for computing resources….……10

4. Requirements for additional Data Management Platform (DMP) infrastructure……..……10

5. Security requirements……13

DocuSign Envelope ID: 5A45EFF2-9542-436F-B64A-A4C98DF04360

1. Sąvokos ir santrumpos

Santrumpa/ sąvoka	Paaiškinimas
Administ-raciniai duomenys	Viešajam administravimui naudojami duomenys, įskaitant asmens duomenis, tarp jų ir specialių kategorijų asmens duomenis, iš jų ir duomenys, esantys registruose, valstybės ir kitose informacinėse sistemose ir dokumentuose.
Administ-racinių duomenų šaltiniai	Registrų ir valstybės informacinių sistemų registre registruoti valstybės registrai ir informacinės sistemos.
ADP	Atvirų duomenų portalas (nuostatai: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/6e0d9154391911eabd71c05e81f09716?jfwid=4t02btuvx) (žr. https://data.gov.lt/)
Agentūra	Valstybės duomenų agentūra (iki 2023 m. sausio 1 d. – Lietuvos statistikos departamentas)
API	Integracinė sąsaja / aplikacijų programavimo sąsaja (angl. *Aplication Programming Interface*)
Duomenų ežeras (angl. *data lake*)	Centralizuota duomenų saugykla, leidžianti kaupti bet kokios struktūros ar nestrukturuotus duomenis dideliu mastu ir atlikti duomenų pseudoniminimo, anoniminimo ar nuasmeninimo procedūras, transformacijas, jungimą, analizes, vizualizacijas ir (ar) kitus veiksmus.
Duomenų valdymo ciklas	Duomenų valdymo procesas, apimantis pagrindines su duomenimis atliekamas procedūras: duomenų įsisavinimą, duomenų transformacijas ir validavimą, konfidencialumo užtikrinimą, analizę ir sklaidą.
ES	Europos Sąjunga
IP	Investicijų projektas
IVPK	Informacinės visuomenės plėtros komitetas
IS	Informacinė sistema
IT	Informacinės technologijos
OSVDV įstatymas	Lietuvos Respublikos oficialiosios statistikos ir valstybės duomenų valdysenos įstatymas
Pirminiai duomenys	Pradiniai neapdoroti valstybės ir kitų informacinių sistemų ir registrų objektams registruoti pateikti duomenys, įskaitant asmens duomenis, tarp jų ir specialių kategorijų asmens duomenis.
projektas	Lietuvos Respublikos ekonomikos ir inovacijų ministerijos valstybės skaitmeninimo plėtros programos pažangos priemonės Nr. 05-002-01-07-07 „Skatinti duomenų prieinamumą ir pakartotinį naudojimą“ veiklos „Valstybės informacinių išteklių integracija į duomenų ežerą“ projektas Nr. 02-008-P-0001
Valstybės duomenys	OSVDV įstatymo 21 straipsnio 1 dalyje nustatytais tikslais Valstybės duomenų valdysenos informacinėje sistemoje ir Duomenų valdymo platformoje kaupiamos pirminių duomenų, administracinių duomenų kopijos, informacija, dokumentai ir (arba) jų kopijos ir kiti duomenys, išskyrus statistinius duomenis.
Valstybės informaci-niai ištekliai	Informacijos, kurią valdo institucijos, atlikdamos teisės aktų nustatytas funkcijas, apdorojamos informacinių technologijų priemonėmis, ir ją apdorojančių informacinių technologijų priemonių visuma.
VDVIS	Valstybės duomenų valdysenos informacinė sistema
DVP, platforma	Duomenų valdymo platforma – VDVIS posistemis, skirtas valstybės duomenų įsisavinimo, transformacijų, analizės ir vizualizavimo funkcijoms atlikti, paremtas Palantir Foundry technologija.

1. Terms and abbreviations

Abbreviation/ term	Explanation
Administra-tive data	The data, including personal data, among them also special categories of personal data, contained in registers, the state and other information systems and documents which are used for public administration.
Administra-tive data sources	State registers and information systems registered in the Register of Registers and State Information Systems.
ODP	Open Data Portal (Regulations: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/6e0d9154391911eabd71c05e81f09716?jfwid=4t02btuvx) (see https://data.gov.lt/)
Agency	State Data Agency (until 1 January 2023 – Lithuanian Department of Statistics)
API	Application Programming Interface
Data lake	Centralised data repository that allows large-scale storage of structured or unstructured data of any kind as well as data pseudonymisation, anonymisation or depersonalisation procedures, transformation, merging, analysis, visualisation and/or other actions.
Data management cycle	Data management process that covers the main procedures performed on data: data ingestion, data transformation and validation, confidentiality, analysis and dissemination.
EU	European Union
IP	Investment project
ISDC	Information Society Development Committee
IS	Information system
IT	Information technologies
Law on OSSDG	Law on Official Statistics and State Data Governance of the Republic of Lithuania
Primary data	Initial raw data submitted for registration of objects in state and other information systems and registers, including personal data, among them also special categories of personal data.
The Project	The project No 02-008-P-0001 of the activity “Integration of State information resources into the data lake” under Progress Measure No 05-002-01-07-07 “Promoting data accessibility and re-use” of the State Digitisation Development Programme of the Ministry of the Economy and Innovation of the Republic of Lithuania
State data	Copies of primary data and administrative data as well as information, documents and/or copies thereof and other data, excluding statistical data, stored in the State Data Governance Information System and the Data Management Platform for the purposes set in Article 21(1) of the Law on OSSDG.
State information resources	Information managed by the institutions in the exercise of their statutory functions, processed by information technology tools, together with the information technology tools used for processing thereof.
SDGIS	State Data Governance Information System
DMP, the Platform	Data Management Platform – SDGIS subsystem designed to perform the functions of state data ingestion, transformation, analysis and visualisation , based on Palantir Foundry technology.

DocuSign Envelope ID: 5A45EFF2-9542-436F-B64A-A4C98DF04360

2. Įvadinė informacija

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

Prekių pateikimo vieta – Valstybės duomenų agentūra, Gedimino pr. 29, LT-01500 Vilnius.

Pirkimo objektas – Palantir Foundry licencijos išplėtimas papildomais infrastruktūros ištekliais. Pirkimo tikslas yra įsigyti agentūros turimos Palantir Foundry licencijos papildomus infrastruktūros išteklius iki 2024 m. gruodžio 5 d (toliau – paslauga), kurie leistų laiku ir kokybiškai įgyvendinti Lietuvos Respublikos ekonomikos ir inovacijų ministerijos valstybės skaitmeninimo plėtros programos pažangos priemonės Nr. 05-002-01-07-07 „Skatinti duomenų prieinamumą ir pakartotinį naudojimą“ veiklos „Valstybės informacinių išteklių integracija į duomenų ežerą“ projektą Nr. 02-008-P-0001 (toliau – projektas).

Siūlomos paslaugos tiekėjas turi būti gamintojas arba turėti gamintojo arba gamintojo atstovo leidimą prekiauti siūlomos programinės įrangos licencijomis Lietuvos Respublikoje ar/ir Europos Sąjungoje.

2.1. Projekto kontekstas

Duomenys labai svarbūs visiems ekonomikos ir visuomenės sektoriams, tačiau kiekviena sritis turi ypatumų ir ne visuose sektoriuose pažanga vyksta vienodu tempu. Todėl svarbu kurti sektorines duomenų erdves tokiose strateginėse srityse kaip gamyba, žemės ūkis, sveikatos priežiūra, judumas ir kt. Šių erdvių tikslas – šalinti teisines ir technines kliūtis dalytis duomenimis, derinant reikiamas priemones ir infrastruktūrą bei rengiant konkrečios erdvės taisykles.

Duomenų valdymo ciklas ir duomenų atvėrimas yra efektyviausias, kai naudojamos techninės priemonės – tai padeda sumažinti duomenų kokybės riziką, kylančią dėl duomenų fragmentacijos, padidinti administracinių šaltinių duomenų kokybę, atverti administracinių šaltinių duomenis, pakartotinai naudoti didelės vertės duomenų rinkinius, kuriais disponuoja viešasis sektorius, sukurti standartizuotus duomenų nuasmeninimo, atvėrimo ir konfidencialumo užtikrinimo metodus, įgyvendinti efektyvius duomenų mainų sprendimus. Pandemijos valdymas reikalavo duomenų operatyvumo ir kokybės, todėl Lietuva 2020 m. įsigijo standartinę duomenų valdymo platformą, kurios valdytojas-ūkvedys yra agentūra.

VDVIS yra bendra erdvė valstybės valdymo, mokslo ir verslo informacijos poreikiams tenkinti, analizėms ir tyrimams atlikti, efektyviems mainams vykdyti ir dalytis vieša, kokybiška bei aktualia informacija. Svarbūs valstybės duomenys detaliausiu lygmeniu patenka į duomenų ežerą, po to duomenų bandomojoje aplinkoje 85 valstybės tarnautojai, mokslininkai ar verslo atstovai juos jungia, analizuoja ir dalijasi ar parengia produktus viešam atvėrimui ar pakartotiniam panaudojimui. Naudojimasis VDVIS užtikrina operatyvumą, lankstumą ir skaidrumą valdant valstybės duomenis, svarbių valstybės duomenų konsolidaciją, kokybės valdymą ir patikimumą. Šiuo metu VDVIS integruota apie 40 valstybės informacinių išteklių ir yra naudojama įvairiems valstybės analitikos uždaviniams spręsti, keistis duomenimis tarp institucijų, taip pat vykdant centralizuotą viešojo sektoriaus duomenų atvėrimą IVPK projekte.

Didelės vertės duomenų rinkinių pakartotinis naudojimas turi ypatingą socioekonominės naudos potencialą, todėl prieiga prie duomenų rinkinių bus kiek įmanoma mažiau teisiškai ribojama ir nemokama. Tokie duomenys bus automatizuotai nuskaitomi ir skelbiami per API. Projekto įgyvendinimas užtikrina efektyvų duomenų valdymą, leidžiantį išvengti sprendimų dubliavimo. Tokiu būdu racionaliai naudojami finansiniai ištekliai, gerinama duomenų kokybė, efektyviai valdomos asmens duomenų pažeidžiamumo rizikos, inventorizuojami duomenys, užtikrinamos duomenų pakartotinio naudojimo galimybės per API.

Pakartotinai naudojant duomenis, kuriais disponuoja viešojo sektoriaus įstaigos, kuriama pridėtinė vertė pakartotinių naudotojų, galutinių naudotojų ir visuomenės plačiąja prasme naudai, kartu daugeliu atvejų – ir pačios viešojo sektoriaus įstaigos naudai, nes skatinamas skaidrumas bei atskaitomybė ir gaunama atsiliepimų iš naudotojų ir galutinių naudotojų, todėl viešojo sektoriaus įstaigos skatinamos užtikrinti surinktos informacijos kokybę ir savo viešųjų užduočių atlikimą.

2. Introductory information

Purchasing organisation – State Data Agency (Statistics Lithuania) (hereinafter referred to as the “Agency”), legal person number – 188600177, address – Gedimino Ave. 29, LT-01500, Vilnius, Tel. (+370 5) 236 4800, Email: info@stat.gov.lt.

Place of delivery of goods – State Data Agency, Gedimino Ave. 29, LT-01500, Vilnius.

Purchase object – the extension of the Palantir Foundry license with additional infrastructure resources. The purpose of the purchase is to purchase additional infrastructure resources for the agency's owned Palantir Foundry license by 5 December 2024 (hereinafter referred to as the “service”), which will enable timely and high-quality implementation of the project No 02-008-P-0001 of the activity “Integration of State information resources into the data lake” under Progress Measure No 05-002-01-07-07 “Promoting data accessibility and re-use” of the State Digitisation Development Programme of the Ministry of the Economy and Innovation of the Republic of Lithuania (hereinafter referred to as the “project”).

The provider of the offered service must be a manufacturer or have permission from the manufacturer or the manufacturer's representative to sell licenses of the offered software in the Republic of Lithuania and/or the European Union.

2.1. Project context

Data are essential for all sectors of the economy and society, but each area has its own particularities and not all sectors progress at the same pace. Therefore, it is important to create sectoral data spaces in strategic areas such as manufacturing, agriculture, healthcare, mobility, etc. The purpose of these spaces is to remove legal and technical barriers to data sharing by harmonising the necessary tools and infrastructure and by developing rules for a specific space.

The data management cycle and data opening are most effective when technical tools are used – this helps to reduce data quality risks due to data fragmentation, to increase the quality of data from administrative sources, to open data from administrative sources, to reuse high-value datasets held by the public sector, to develop standardised methods for depersonalisation, opening and securing the confidentiality of the data, and to implement efficient data sharing solutions. Pandemic management required speed and quality of data, which is why in 2020 Lithuania purchased a standard data management platform managed by the Agency.

SDGIS is a common space for meeting the public administration, science and business information needs, for analysis and research, for efficient exchange and sharing of public, quality and relevant information. Important state data at the most detailed level enter the data lake, then 85 civil servants, scientists or business representatives aggregate and analyse them in data pilot environment and share or prepare them into products for public opening or re-use. The use of SDGIS ensures efficiency, flexibility and transparency in state data management, consolidation of important state data, quality management and reliability. Currently, SDGIS integrates around 40 public information resources and is used for a wide range of public analytical tasks, for the exchange of data between institutions, as well as for the centralised opening of public sector data in the ISDC project.

The re-use of high-value datasets has a particular potential for socio-economic benefits and therefore access to datasets will be free of charge and the least legally restricted possible. Such data will be automatically read and published via API. The project ensures efficient data management, avoiding duplication of solutions. In this way, financial resources are used rationally, data quality is improved, risks of personal data vulnerabilities are effectively managed, data are inventoried, data reuse possibilities through API are ensured.

The re-use of data held by public sector bodies generates value added for the benefit of re-users, end-users and society at large, and in many cases also for the benefit of the public sector body itself, by promoting transparency and accountability, and by obtaining feedback from users and end-users, and thus public sector bodies are encouraged to ensure the quality of collected information and the performance of their public tasks.

DocuSign Envelope ID: 5A45EFF2-9542-436F-B64A-A4C98DF04360

Projektui įgyvendinti būtinos tiesioginės viešosios investicijos, siekiant padidinti į VDVIS integruotų duomenų apimtį panaudojant 376 informacinius išteklius, sukuriant prielaidas pakartotinai panaudoti duomenis.

Siekiant integruoti informacinius išteklius į nacionalinį duomenų ežerą reikia:

1. sukurti sąsają su duomenų tiekėju per duomenų dalijimosi jungtį
2. aprašyti semantinę struktūrą, parengti metaduomenis
3. sutvarkyti gautus duomenų rinkinius (transformavimas, valymas, nuasmeninimas / šifravimas, jungimas, agregavimas ir kiti darbai atsižvelgiant į duomenų specifiką ir vartotojų poreikius dėl atvėrimo)
4. sukurti nacionalinio duomenų ežero (VDVIS) sąsają su Atvirų duomenų portalo (data.gov.lt) duomenų saugykla per REST (angl. *Representational state transfer*) aplikacijų programavimo sąsają (API)
6. sukurti atvirų duomenų rinkinių ir jų metaduomenų automatinio atnaujinimo mechanizmą.

Projektas tiesiogiai susijęs su europinėmis duomenų atvėrimo ir pakartotinio panaudojimo iniciatyvomis. Numatytos investicijos leis sklandžiai technologiškai įgyvendinti duomenų atvėrimą, integraliai panaudojant viešojo sektoriaus duomenų panaudojimą įvairialypiams tikslams. Reforma siekiama išspręsti viešojo sektoriaus duomenų decentralizacijos ir fragmentacijos sąlygotas problemas, kurios lemia brangų ir lėtą duomenų atvėrimą ir pakartotinį panaudojimą, nepasinaudojus siūlomu technologiniu sprendimu – nacionaliniu duomenų ežeru. Nacionalinis duomenų ežeras įgyvendinamas naudojantis jau įgyvendintais technologiniais sprendimais. Ši infrastruktūra apims ir didelės vertės sveikatos duomenų pakartotinį panaudojimą. Šiuo metu jau atverti duomenys, susiję su pandemija, ir sudarytos sąlygos pakartotinai juos panaudoti.

2.2. projektu sprendžiama problema ir jos priežastys

Esamos duomenų atvėrimo iniciatyvos nesprendžia viešojo sektoriaus duomenų fragmentacijos problemos, nedidina jų prieinamumo visuomenei, mokslui ir verslui ir neužtikrina atveriamų duomenų kokybės (vertės) bei nesudaro galimybių šiuos duomenis efektyviai jungti ir analizuoti ar kitaip pakartotinai panaudoti. Be to, duomenų atvėrimas dar labiau padidina duomenų valdytojų sąnaudas rengiant ir teikiant atvertus duomenis, o tuo pat metu šių atvertų duomenų vertė dėl kokybės trūkumų išlieka abejotina. Fragmentuotai kaupiami ir atveriami duomenys sudaro kliūtis mokslui ir verslui pasinaudoti šiais valstybės informacijos ištekliais, kuriant didelę ekonominę ir socialinę vertę turinčius produktus.

Pagrindinė problemos priežastis yra bendros erdvės, kurioje būtų realizuotas visas duomenų valdymo ciklas (operatyvus duomenų paėmimas, transformacija, kokybės užtikrinimas, duomenų jungimas ir analizė, tuo pat metu užtikrinant duomenų saugumą ir lanksčiai paskirstant naudotojų teises) nebuvimas.

Nesant bendros duomenų valdymo platformos, viešojo sektoriaus duomenų atvėrimas tampa brangi, bet ilgalaikio efekto nekurianti ir išsklaidyta investicija: esamos duomenų atvėrimo iniciatyvos nesprendžia duomenų šaltinių fragmentacijos problemos, nedidina duomenų prieinamumo visuomenei, mokslui ir verslui ir neužtikrina atveriamų duomenų kokybės (vertės) bei nesudaro galimybių šiuos duomenis efektyviai jungti ir analizuoti ar kitaip pakartotinai panaudoti. Be to, fragmentuotas duomenų atvėrimas sudaro prielaidas dubliuoti duomenis, savo ruožtu, nesant bendro duomenų kokybės užtikrinimo, keliama klaidingos interpretacijos rizika, mažinamas viešojo sektoriaus, kaip duomenų šaltinio, patikimumas.

Fragmentuotai kaupiami ir atveriami duomenys sudaro kliūtis mokslui ir verslui pasinaudoti šiais valstybės informacijos ištekliais, kuriant didelę ekonominę ir socialinę vertę turinčius produktus.

The implementation of the project requires direct public investment to increase the volume of data integrated into the SDGIS through the use of 376 information resources, by creating the preconditions for data re-use.

In order to integrate information resources into the national data lake, it is necessary:

1. To create an interface with the data provider via a data sharing connector (agent).
2. To describe the semantic structure, prepare metadata.
3. To organise the received datasets (transformation, cleansing, depersonalisation/encryption, merging, aggregation and other work based on the specificity of the data and the user needs for opening).
4. To create an interface between the national data lake (SDGIS) and the data repository of the Open Data Portal (data.gov.lt) via Representational State Transfer (REST) application programming interface (API).
6. To create a mechanism for automatic updating of open datasets and metadata thereof.

The project is directly linked to European initiatives on data opening and re-use. The planned investments will allow the smooth technological implementation of data opening, by integrally using the public sector data for various purposes. The reform aims to address the problems caused by the decentralisation and fragmentation of public sector data, which leads to costly and slow data opening and re-use, without taking advantage of the proposed technological solution – the national data lake. The national data lake is implemented using already implemented technological solutions. This infrastructure will also include the re-use of high-value health data. The pandemic-related data have now been opened and made available for re-use.

2.2. The problem and causes thereof addressed by the project

Existing data opening initiatives do not address the fragmentation of public sector data, do not make such data more accessible to the public, science and business, and do not ensure the quality (value) of the data opened, nor do they provide opportunities for the data to be efficiently aggregated and analysed or otherwise re-used. Moreover, data opening further increases the costs for data controllers on producing and providing open data, while at the same time the value of these open data remains questionable due to quality deficiencies. Fragmented storage and opening of data create obstacles for science and business to take advantage of these state information resources in creating products with high economic and social value.

The main cause of the problem is the lack of common space in which the entire data management cycle (prompt data extraction, transformation, quality assurance, data merging and analysis, while ensuring data security and flexible distribution of user rights) is realised.

In the absence of a common data management platform, opening of public sector data becomes a costly and dispersed investment having no long-term effect: existing data opening initiatives do not address the fragmentation of data sources, do not increase the availability of data to the public, science and business, and do not ensure the quality (value) of the data opened, nor do they allow for the data to be efficiently aggregated and analysed or otherwise re-used. In addition, fragmented data opening leads to data duplication and, in turn, in the absence of general data quality assurance, risks misinterpretation and undermines the credibility of the public sector as a data source.

Fragmented storage and opening of data create obstacles for science and business to take advantage of these state information resources in creating products with high economic and social value.

DocuSign Envelope ID: 5A45EFF2-9542-436F-B64A-A4C98DF04360

2.3. Projekto turinys

Projekto tikslas – reikšmingai išplėsti VDVIS apimtį ir panaudojimą valstybės analitikos uždaviniams spręsti ir viešojo sektoriaus duomenims atverti.

Projekto metu siekiama sudaryti sąlygas vienoje erdvėje teikti valstybės duomenų, reikalingų valstybės informacijos reikmėms, integravimo, konsolidavimo ir atvėrimo užtikrinimo paslaugą, įskaitant valstybės duomenų inventorinimą ir viešo duomenų katalogo sukūrimą.

Projekto tikslai ir uždaviniai susiję su kitomis viešojo sektoriaus iniciatyvomis (pvz., IVPK sukurtu ADP), tačiau jų nedubliuoja, priešingai, tęsia viešojo sektoriaus duomenų atvėrimo iniciatyvą, sudarant galimybes centralizuoti šį procesą. Projekto metu bus konsoliduoti valstybės informacinėms reikmėms būtini administracinių šaltinių kaupiami duomenys, tai leis užtikrinti efektyvų duomenų pakartotinį panaudojimą, tuo pat metu – bus sudarytos sąlygos mokslui ir verslui prieiti prie šių konsoliduotų valstybės duomenų išteklių, atveriant juos viešai arba teikiant eksperimentines erdves (angl. *sandbox*‘us) jų uždaviniams įgyvendinti.

Projektą agentūra įgyvendina be partnerių, tačiau priimdamas sprendimus dėl VDVIS paslaugų teikimo, integruojamų administracinių duomenų šaltinių ir jų duomenų apimties ir tikslingumo ir kitais klausimais tarsis su susijusiomis valstybės institucijomis, taip pat Ekonomikos ir inovacijų ministerija bei IVPK.

Šiuo metu Registrų ir valstybės informacinių sistemų registre yra registruoti 95 registrai ir 312 valstybės informacinių sistemų. Šiuos registrus ir informacines sistemas valdo 134 skirtingi valdytojai ir tvarko 166 pagrindiniai tvarkytojai. Didžioji dalis registrų ir informacinių sistemų yra uždaro pobūdžio ir orientuotos į žinybinio informacijos poreikio tenkinimą. Paslaugos valdymas nėra centralizuotas, kilus poreikiui prieiti prie minėtų duomenų išteklių, reikia kreiptis į atskirus jų valdytojus ar tvarkytojus, pagal atskiras pačių institucijų nusistatytas paslaugų teikimo tvarkas.

Projekto kontekste paslaugos pasiūlą reikėtų analizuoti trimis aspektais: viešojo sektoriaus duomenų, reikalingų valstybės informacijos reikmėms, konsolidavimo, atvėrimo ir mainų užtikrinimo. Kaip atskirą pasiūlos komponentą būtina įvertinti ir duomenų kokybės užtikrinimą, nes bet koks duomenų panaudojimas neįmanomas be kokybės konteksto.

Viešojo sektoriaus duomenų, reikalingų valstybės informacinėms reikmėms, konsolidavimo paslaugos neteikia nė viena valstybės institucija. Su išlyga kaip tam tikra konsoliduotos informacijos erdvė galėtų būti Oficialiosios statistikos portalas, kuriame oficialiąją statistiką teikia ne tik agentūra, bet ir kitos oficialiąją statistiką tvarkančios institucijos pagal Oficialiosios statistikos programos I dalį.

2.4. Projekto vykdymo planas

Planuojama projekto trukmė – iki 2026 m. birželio mėn. projekto veiklas numatoma vykdyti lygiagretinant duomenų valdymo ciklo procesus, tačiau pirmiausia pradedant nuo valstybės išteklių inventorizacijos.

2.5. Projekto tikslinės grupės

Tikslinės grupės yra viešojo valdymo įstaigos, mokslo institucijos, verslas ir visuomenė plačiąja prasme. Projektu užtikrinamas duomenų prieinamumo didinimas, jų atvėrimas, integralumas.

2.6. Teisinės projekto prielaidos ir aplinka

Pagrindiniai projekto veiklas reglamentuojantys arba su jomis susiję teisės aktai:

1. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 2016 m. balandžio 27 d. dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas)
2. Lietuvos Respublikos teisės gauti informaciją ir duomenų pakartotinio naudojimo įstatymas
3. Lietuvos Respublikos oficialiosios statistikos ir valstybės duomenų valdysenos įstatymas

2.3. Project content

The aim of the project is to significantly expand the scope and use of the SDGIS to solve state analytics tasks and to open public sector data.

The project is aimed at creating the conditions for integration, consolidation and opening of data required for state information needs in one space, including the state data inventory and the creation of public data catalogue.

The objectives and tasks of the project are related to, but not duplicative of, other public sector initiatives (e.g. ODP developed by ISDC) and, on the contrary, continue the public sector data opening initiative by enabling the centralisation of this process. The project will consolidate data from administrative sources that are essential for the information needs of the State, thus ensuring efficient re-use of the data, while at the same time enabling science and business to have access to these consolidated State data resources, either by opening them publicly or by providing sandboxes for the implementation of their tasks.

The Agency has been implementing the project without partners but will consult the relevant public authorities, the Ministry of the Economy and Innovation and ISDC when making decisions regarding the SDGIS services provision, integrated administrative data sources and the scope and appropriateness of their data, and other issues.

Currently, 95 registers and 312 State information systems are registered in the Register of Registers and State Information Systems. These registers and information systems are managed by 134 different controllers and 166 main managers. Most registers and information systems are closed-type and aimed at meeting departmental information needs. The service management is not centralised, and access to these data resources requires contacting individual data controllers or managers according to different procedures established by institutions themselves.

In the context of the project, the service supply should be analysed in three aspects: consolidation, opening and exchange of public sector data required for the State information needs. Data quality assurance must also be considered as a separate component of the supply, as any use of data is impossible without a quality context.

No public authority provides a consolidation service for public sector data required for the State information needs. On a conditional basis, the Official Statistics Portal could serve as a kind of consolidated information space where official statistics are provided not only by the Agency but also by other institutions managing official statistics in accordance with Part I of the Official Statistics Programme.

2.4. Project implementation plan

The planned duration of the project: by June 2026, the project activities are planned to be carried out in parallel with the data management cycle processes, but first starting with the inventory of the State resources.

2.5. Project target groups

The target groups are public administration institutions, scientific institutions, business and society in a broad sense. The project ensures increase in data accessibility, opening and integrity.

2.6. Legal background and environment of the project

Key legislation governing or relating to the project activities:

1. 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).
2. Law on the Right to Receive Information and Data Reuse of the Republic of Lithuania
3. Law on Official Statistics and State Data Governance of the Republic of Lithuania

DocuSign Envelope ID: 5A45EFF2-9542-436F-B64A-A4C98DF04360

4. Lietuvos Respublikos Vyriausybės 2021 m. spalio 13 d. nutarimu Nr. 849 „Dėl Lietuvos Respublikos teisės gauti informaciją ir duomenų pakartotinio naudojimo įstatymo įgyvendinimo“

5. Aštuonioliktosios Lietuvos Respublikos Vyriausybės programos nuostatų įgyvendinimo planas, patvirtintas Lietuvos Respublikos Vyriausybės 2021 m. kovo 10 d. nutarimu Nr. 155 „Dėl Aštuonioliktosios Lietuvos Respublikos Vyriausybės programos nuostatų įgyvendinimo plano įgyvendinimo“

6. Duomenų atvėrimo tvarkos aprašas, patvirtintas Lietuvos Respublikos ekonomikos ir inovacijų ministro 2020 m. gruodžio 28 d. įsakymu Nr. 4-1150 (2022 m. kovo 31 d. įsakymo Nr. 4-517 redakcija)

7. Duomenų rinkinių sudarymo ir perdavimo į Lietuvos atvirų duomenų portalą naudojantis Valstybės duomenų valdysenos informacine sistema tvarkos aprašas, patvirtintas Lietuvos statistikos departamento generalinio direktoriaus 2022 m. sausio 20 d. įsakymu Nr. DĮ-21

8. Lietuvos statistikos departamento generalinio direktoriaus 2022 m. sausio 13 d. įsakymas Nr. DĮ-13 „Dėl Valstybės duomenų valdysenos informacinės sistemos duomenų teikimo būdų patvirtinimo“.

Lietuvoje duomenų atvėrimo veiklą reglamentuoja Lietuvos Respublikos teisės gauti informaciją ir duomenų pakartotinio naudojimo įstatymas (toliau – TGIĮ), nustatantis asmenų teisės gauti įstatyme įvardytų subjektų informaciją apie jų veiklą bei duomenis, kuriais jie disponuoja ir (ar) kuriuos jie tvarko vykdydami viešojo administravimo įgaliojimus ir viešąsias funkcijas ir kuriuos būtų galima pakartotinai naudoti komerciniams arba nekomerciniams tikslams, įgyvendinimo priemones ir tvarką.

TGIĮ taikomas dviem grupėms subjektų:

1) viešąsias funkcijas atliekančioms valstybės ir savivaldybių institucijoms ir įstaigoms, įmonėms ir viešosioms įstaigoms, kurių savininkė ar viena iš dalininkių yra valstybė ar savivaldybė ir kurios finansuojamos iš valstybės ar savivaldybių biudžetų bei valstybės pinigų fondų, įskaitant bibliotekas, muziejus ir valstybės archyvus, taip pat šių subjektų asociacijoms ir regionų plėtros taryboms (toliau – institucijos);

2) viešosioms įstaigoms, kurių savininkė arba bent viena iš dalininkių, turinti pusę ir daugiau balsų visuotiniame dalininkų susirinkime, yra valstybė ar savivaldybė, kurios nėra finansuojamos iš valstybės ir savivaldybių biudžetų bei valstybės pinigų fondų, tačiau atlieka viešąsias funkcijas, taip pat akcinėms bendrovėms ar uždarosioms akcinėms bendrovėms, kuriose valstybei arba savivaldybei tiesiogiai arba netiesiogiai priklauso akcijos, suteikiančios daugiau kaip pusę balsų visuotiniame akcininkų susirinkime, ir valstybė ar savivaldybė tiesiogiai ar netiesiogiai gali daryti lemiamą įtaką rinkdama ir atšaukdama akcinės bendrovės arba uždarosios akcinės bendrovės vadovą, taip pat daugiau kaip pusę valdybos arba stebėtojų tarybos narių, ir kurios teikia viešąsias paslaugas bent vienoje iš šių sričių: dujų ir šilumos ūkio, elektros energetikos, vandentvarkos, transporto paslaugų, uostų ir oro uostų, pašto paslaugų, naftos ir dujų gavybos, anglių ar kito kietojo kuro žvalgymo arba gavybos, viešojo keleivinio transporto pagal 2007 m. spalio 23 d. Europos Parlamento ir Tarybos reglamento (EB) Nr. 1370/2007 dėl keleivinio geležinkelių ir kelių transporto viešųjų paslaugų ir panaikinančio Tarybos reglamentus (EEB) Nr. 1191/69 ir (EEB) Nr. 1107/70 su visais pakeitimais 2 straipsnį, oro susisiekimo paslaugų teikimo pagal 2008 m. rugsėjo 24 d. Europos Parlamento ir Tarybos reglamento (EB) Nr. 1008/2008 dėl oro susisiekimo paslaugų teikimo Bendrijoje bendrųjų taisyklių (nauja redakcija) su visais pakeitimais 16 straipsnį, visuomenės aptarnavimo paslaugų teikimo pagal 1992 m. gruodžio 7 d. Tarybos reglamento (EEB) Nr. 3577/92, taikančio laisvės teikti paslaugas principą jūrų transportui valstybėse narėse (jūrų kabotažas), su visais pakeitimais 4 straipsnį (toliau – valstybės valdomi subjektai).

TGIĮ 15 straipsnio 3 dalyje nustatyta, kad institucijos ir valstybės valdomi subjektai, sudarydami duomenų rinkinius ir juos perduodami į Lietuvos atvirų duomenų portalą, naudojasi Vyriausybės įgaliotos institucijos valdomos valstybės informacinės sistemos funkcionalumu įgaliotos institucijos nustatyta tvarka.

4. Resolution No. 849 of 13 October 2021 of the Government of the Republic of Lithuania “On the Implementation of the Law on the Right to Receive Information and Data Reuse of the Republic of Lithuania”.

5. Plan for the Implementation of the Provisions of the Eighteenth Programme of the Government Republic of Lithuania, approved by Resolution No. 155 of 10 March 2021of the Government of the Republic of Lithuania “On the Implementation of the Plan for the Implementation of the Provisions of the Eighteenth Programme of the Government of the Republic of Lithuania”

6. Description of Procedure for Data Opening, approved by Order No. 4-1150 of 28 December 2020 of the Minister of the Economy and Innovation of the Republic of Lithuania (new version of Order No. 4-517 of 31 March 2022)

7. Description of Procedure for Creating and Transferring Datasets to the Lithuanian Open Data Portal via the State Data Governance Information System, approved by Order DĮ-21 of 20 January 2022 of the Director General of Statistics Lithuania

8. Order No. DĮ-13 of 13 January 2022 of the Director General of Statistics Lithuania “On the approval of methods of provision of data of the State Data Governance Information System”

In Lithuania, data opening activities are regulated by the Law on the Right to Receive Information and Data Reuse of the Republic of Lithuania which establishes the means and procedure for implementing the right of individuals to receive information from the entities named in the Law about their activities and data that they dispose and/or process in the exercise of the public administration powers and public functions, and that could be reused for commercial or non-commercial purposes.

The Law on the Right to Receive Information and Data Reuse applies to two groups of subjects:

1) State and municipal institutions performing public functions, enterprises and public bodies owned or co-owned by the State or a municipality and financed from the State or municipal budgets and State monetary funds, including libraries, museums and State archives, as well as associations and regional development councils of these subjects (hereinafter referred to as the “Institutions”);

2) Public institutions whose owner or at least one of the shareholders holding half or more of the votes at the general meeting of shareholders is the State or municipality, which are not financed from the State and municipal budgets and State monetary funds, but which perform public functions, as well as joint-stock companies or closed joint-stock companies, in which the State or the municipality directly or indirectly owns shares conferring more than half of the votes at the general meeting of shareholders, and the State or municipality can directly or indirectly exercise a decisive influence on the election and dismissal of the manager of the joint-stock company or closed joint-stock company, as well as more than half members of the board or supervisory board, and which provide public services in at least one of the following areas: gas and heat industry, electricity, water management, transport services, ports and airports, postal services, oil and gas extraction, coal or other solid fuel exploration or mining, public passenger transport according to Article 2 of Regulation (EC) No 1370/2007 of the European Parliament and of the Council of 23 October 2007 on public passenger transport services by rail and by road and repealing Council Regulations (EEC) No 1191/69 and 1107/70 with all amendments, provision of air transport services according to Article 16 of Regulation (EC) No 1008/2008 of the European Parliament and of the Council of 24 September 2008 on common rules for the operation of air services in the Community (Recast) with all amendments, provision of public service according to Article 4 of Council Regulation (EEC) No 3577/92 of 7 December 1992 applying the principle of freedom to provide services to maritime transport within Member States (maritime cabotage) with all amendments (hereinafter referred to as the “State-controlled subjects”).

Article 15(3) of the Law on the Right to Receive Information and Data Reuse provides that institutions and State-controlled subjects shall use the functionality of the state information system managed by the government-authorised institution in accordance with the procedures laid down by the authorised authority when compiling datasets and transferring them to the Lithuanian Open Data Portal.

DocuSign Envelope ID: 5A45EFF2-9542-436F-B64A-A4C98DF04360

Lietuvos Respublikos Vyriausybės 2021 m. spalio 13 d. nutarimu Nr. 849 „Dėl Lietuvos Respublikos teisės gauti informaciją ir duomenų pakartotinio naudojimo įstatymo įgyvendinimo“ agentūra buvo įgaliota sudaryti sąlygas institucijoms ir valstybės valdomiems subjektams naudotis jo valdoma ir tvarkoma VDVIS ir nustatyti naudojimosi ja tvarką.

Minėta tvarka buvo nustatyta Duomenų rinkinių sudarymo ir perdavimo į Lietuvos atvirų duomenų portalą naudojantis Valstybės duomenų valdysenos informacine sistema tvarkos apraše, patvirtintame Lietuvos statistikos departamento generalinio direktoriaus 2022 m. sausio 20 d. įsakymu Nr. DĮ-21:

Duomenų rinkinių sudarymo ir perdavimo į Lietuvos atvirų duomenų portalą naudojantis Valstybės duomenų valdysenos informacine sistema tvarkos aprašo 7 punkte numatyta, kad reikalingi pirminiai duomenys pateikiami į VDVIS siekiant sudaryti duomenų rinkinį ir jį perduoti į Atvirų duomenų portalą. Pirminiai duomenys teikiami į VDVIS tik automatizuotu („sistema–sistema“) būdu, naudojant patvirtintą standartinės duomenų dalijimosi jungties būdą. Aprašo 12 punkte numatyta, kad agentūra konsultuoja ir prireikus, institucijai neturint sistemos administratoriaus ar sistemos priežiūros paslaugų teikėjo, padeda institucijai įdiegti ir sukonfigūruoti pirminio duomenų šaltinio duomenų struktūros aprašui generuoti reikalingus įrankius ir VDVIS jungtį. Agentūra sudaro duomenų rinkinį ir jį perduoda į Atvirų duomenų portalą, kai institucija oficialiu raštu pateikia šaltinio duomenų struktūros aprašą ir nurodo atvirų duomenų rinkinio pavadinimą, atvirų duomenų rinkinio atnaujinimo dažnumą (13 punktas). Agentūra, sudarydama duomenų rinkinį, duomenis nuasmenina ir pašalina kitus konfidencialius duomenis, išskyrus atvejus, kai teisės aktai numato kitaip (17 punktas). Sudarant duomenų rinkinį, duomenys tvarkomi ir duomenų saugumas užtikrinamas, vadovaujantis agentūros generalinio direktoriaus įsakymu „Dėl Valstybės duomenų valdysenos informacinės sistemos nuostatų patvirtinimo“ ir įsakymu „Dėl Valstybės duomenų valdysenos informacinės sistemos saugos politiką įgyvendinančių dokumentų patvirtinimo ir Valstybės duomenų valdysenos informacinės sistemos veiklos atkūrimo darbo grupės sudarymo“ (20 punktas).

Lietuvos Respublikos oficialiosios statistikos ir valstybės duomenų valdysenos įstatyme (toliau – OSVDVĮ), priimtame liepos 19 d. ir įsigaliojančiame 2023 m. sausio 1 d. yra nustatyti keli projekto teisinei aplinkai svarbūs momentai:

1) Yra apibrėžiama valstybės duomenų sąvoka, apimanti OSVDVĮ 21 straipsnio 1 dalyje numatytiems tikslams naudojamas pirminių duomenų, administracinių duomenų kopijas, informaciją, dokumentus ir (arba) jų kopijos ir kitus duomenis, išskyrus statistinius duomenis.

2) Pirminiais duomenimis OSVDVĮ laikomi pradiniai neapdoroti valstybės ir kitų informacinių sistemų ir registrų objektams registruoti pateikti duomenys, įskaitant asmens duomenis, tarp jų ir specialių kategorijų asmens duomenis.

3) Minėto 21 straipsnio 1 dalyje, kaip vienas iš valstybės duomenų valdymo, tvarkymo ir naudojimo tikslų, yra 10 punkte įvardytas rinkinių sudarymas ir skelbimas juos pakartotinai naudoti Teisės gauti informaciją ir duomenų pakartotinio naudojimo įstatymo ir kitų teisės aktų, reglamentuojančių valstybės duomenų skelbimą pakartotinai naudoti, nustatyta tvarka.

4) Valstybės duomenų tvarkymo veiksmai, siekiant OSVDVĮ 21 straipsnio 1 dalyje įvardytų tikslų, yra įtraukiami į metinę Valstybės duomenų valdysenos programą – Europos Sąjungos teisės aktais, Lietuvos Respublikos įstatymais, Vyriausybės nutarimais, Ministro Pirmininko potvarkiais, esant ekstremaliajai situacijai ir (ar) įvykiui – operacijų vadovo sprendimais pavedamų atlikti darbų metinis sąrašą, tvirtinama Lietuvos Respublikos finansų ministro. Projekte siekiama įgyvendinti valstybės informacinių išteklių integracija yra įtraukta į Valstybės duomenų valdysenos programą.

Upon Resolution No. 849 of 13 October 2021 of the Government of the Republic of Lithuania “On the Implementation of the Law on the Right to Receive Information and Data Reuse of the Republic of Lithuania”, the Agency was authorized to create conditions for institutions and the State-controlled subjects to use the Agency-managed SDGIS and to determine the procedure for its use.

The said procedure was set in the Description of Procedure for Creating and Transferring Datasets to the Lithuanian Open Data Portal via the State Data Governance Information System, approved by Order DĮ-21 of 20 January 2022 of the Director General of Statistics Lithuania:

Point 7 of the Description of Procedure for Creating and Transferring Datasets to the Lithuanian Open Data Portal via the State Data Governance Information System sets out that the required primary data shall be provided to SDGIS in order to create a dataset and transfer it to the Open Data Portal. Primary data shall be provided to SDGIS only in an automated (‘system-to-system’) manner by using an approved standard data sharing connector. Point 12 of the Description of Procedure provides that the Agency shall advise and, if necessary, in the absence of a system administrator or a system maintenance provider, assist the institution in launching and configuring the tools necessary for generating the primary data source data structure description and the SDGIS connector. The Agency shall generate a dataset and transfers it to the Open Data Portal when the institution provides the source data structure description in official writing and indicates the name of the open dataset, the frequency of updating of the open dataset (Point 13). When compiling the dataset, the Agency shall depersonalise the data and remove other confidential data, unless otherwise provided for by legislation (Point 17). When compiling the dataset, the data shall be processed and data security shall be ensured in accordance with the following Orders of the Director General of the Agency: “Regarding approval of the Regulations of the State Data Governance Information System” and “Regrading approval of the documents implementing the security policy of the State Data Governance Information System and the establishment of the Working Group on Recovery of Activity of the State Data Governance Information System” (Point 20).

The Law on Official Statistics and State Data Governance of the Republic of Lithuania, adopted on 19 July and entering into force on 1 January 2023, sets outs several important aspects of the legal environment of the project:

1) The concept of State data is defined, which includes copies of primary data and administrative data, information, documents and/or copies thereof, and other data, excluding statistical data, used for the purposes provided for in Article 21(1) of this Law.

2) Under this Law, the primary data are initial raw data submitted for registration of objects in state and other information systems and registers, including personal data, among them also special categories of personal data.

3) According to the said Article 21(1), one of the objectives of the state data management and use indicated in Point 10 is creation of datasets and publication thereof for re-use in accordance with the procedure established by the Law on the Right to Receive Information and Data Reuse and other legal acts regulating the publication of state data for reuse.

4) State data processing actions, to achieve the objectives set out in Article 21(1) of this Law, shall be included in the annual State Data Governance Programme – the annual list of the activities assigned by the European Union legislation, laws of the Republic of Lithuania, resolutions of the Government of the Republic of Lithuania, and in the event of the announced state of emergency – by decisions of the Operations Manager, approved by the Minister of Finance of the Republic of Lithuania. The integration of state information resources, which is aimed to be implemented by this project, is included in the State Data Governance Programme.

DocuSign Envelope ID: 5A45EFF2-9542-436F-B64A-A4C98DF04360

Centralizuotas duomenų atvėrimas per VDVIS, kuriam prielaidas sukuria TGIĮ ir OSVDVĮ, galimas tik integravus valstybės informacinius išteklius į VDVIS. Tokia priemonė buvo įtraukta į Aštuonioliktosios Lietuvos Respublikos Vyriausybės programos nuostatų įgyvendinimo planą, patvirtintą Lietuvos Respublikos Vyriausybės 2021 m. kovo 10 d. nutarimu Nr. 155 „Dėl Aštuonioliktosios Lietuvos Respublikos Vyriausybės programos nuostatų įgyvendinimo plano įgyvendinimo“:

„9.2.11. Integruoti Valstybės duomenų valdysenos informacinėje sistemoje valstybės informacinių sistemų ir registrų duomenis, realizuoti centralizuotą jų atvėrimą ir eksperimentavimo platformas (angl. *sandbox*), užtikrinti efektyvius duomenų, reikalingų priimant sprendimus, mainus tarp institucijų bei sukurti duomenų anoniminimo ir sujungimo mechanizmą, sudarant statistinį nuolatinių gyventojų ir statistinių ūkio subjektų registrus“.

Duomenų atvėrimo tvarkos apraše (Lietuvos Respublikos ekonomikos ir inovacijų ministro 2022 m. kovo 31 d. įsakymo Nr. 4-517 redakcija) 11 punkte nustatyta, kad visi institucijų ir valstybės valdomų subjektų atvertini duomenys, kurių nuasmeninimą ir konfidencialumą reikia užtikrinti, parengiami atverti ir į Atvirų duomenų portalą perduodami naudojantis VDVIS. Tai reiškia, kad į VDVIS atvėrimo tikslams perduodami pirminiai visi institucijų ir valstybės valdomų subjektų duomenys.

2.7. Santykis su BDAR

Agentūra, sudarydama atvirų duomenų rinkinius ir juos perduodama į Atvirų duomenų portalą, veikia kaip VDVIS valdytojas, institucijų perduodamų duomenų, kurių pagrindu rengiami atvirų duomenų rinkiniai, gavėjas ir tolesnis duomenų valdytojas. Agentūra nėra registrų ir informacinių sistemų, kurių duomenys atveriami naudojantis VDVIS tvarkytojas. Agentūra, vykdydama jai nustatytas funkcijas duomenų atvėrimo procese, vadovaujasi aukščiau paminėtais duomenų pakartotinį naudojimą reglamentuojančiais teisės aktais, kurie yra privalomi tiek agentūrai, tiek institucijoms, duomenis atverčiančioms per VDVIS.

Institucija, perduodama pirminius duomenis į VDVIS, kad būtų sudarytas ir perduotas į ADP atvirų duomenų rinkinys, vykdo teisės aktų nustatytus įpareigojimus, todėl asmens duomenis, esančius pirminiais duomenimis, reikalingais atvirų duomenų rinkiniui sudaryti, perduoda agentūrai 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) 6 straipsnio 1 dalies c punkto pagrindu (vykdant duomenų valdytojui taikomą teisinę prievolę), specialių kategorijų asmens duomenis – ir reglamento 9 straipsnio 2 dalies g punkto pagrindu (dėl viešojo intereso priežasčių). Kadangi asmens duomenų perdavimui atlikti egzistuoja teisinis pagrindas, numatytas Reglamento (ES) 2016/679 6 straipsnio 1 dalies c punkte, 9 straipsnio 2 dalies g punkte, duomenų subjektų sutikimas dėl jų asmens duomenų perdavimo agentūrai nėra reikalingas ir asmens duomenų pateikimas agentūrai negali būti vertinamas kaip asmens duomenų saugumo pažeidimas.

2.8. Projekto darbuotojai

projekto veiklas įgyvendins 74 darbuotojai, kuriuos galima suskirstyti į kelias pareigybių grupes: programuotojai, programuotojai-analitikai / konfidencialumo / kokybės specialistai, DB administratoriai, informacijos vadybininkai, duomenų teisininkai ir projekto vadovai.

The centralised opening of data through SDGIS, preconditioned by the Law on the Right to Receive Information and Data Reuse and Law on OSSDG, can only be achieved through the integration of the State information resources into SDGIS. Such measure was included into the Plan for the Implementation of the Provisions of the Eighteenth Programme of the Government Republic of Lithuania, approved by Resolution No. 155 of 10 March 2021of the Government of the Republic of Lithuania “On the Implementation of the Plan for the Implementation of the Provisions of the Eighteenth Programme of the Government of the Republic of Lithuania”:

“9.2.11. To integrate the data of the State information systems and registers in the State Data Governance Information System, to implement the centralized opening of such data and sandboxes, to ensure the efficient exchange of data required for decision-making between institutions, and to create a mechanism for anonymisation and aggregation of data through statistical register of permanent residents and statistical register of economic entities”.

Point 11 of the Description of Procedure for Data Opening (Recast No 4-517 of 31 March 2022 of the Minister of the Economy and Innovation of the Republic of Lithuania) provides that all open data of institutions and State-controlled subjects, the depersonalization and confidentiality of which must be ensured, are prepared for opening and transmitted to the Open Data Portal through SDGIS. This means that all primary data of institutions and State-controlled subjects are transferred to SDGIS for the purposes of opening.

2.7. Relationship with GDPR

By compiling open datasets and transferring them to the Open Data Portal, the Agency acts as SDGIS manager, a recipient of data transferred by institutions, on the basis of which open datasets are prepared, and a subsequent data manager. The Agency is not manager of the registers and information systems whose data are opened using SDGIS. The Agency, while performing the functions assigned to it in the data opening process, follows the above-mentioned legal acts regulating the reuse of data, which are mandatory for both the Agency and the institutions opening their data through SDGIS.

While transmitting primary data to SDGIS in order to compile open dataset and transmit it to ODP, the institution fulfils the obligations set by the legislation, therefore, it transfers the personal data that are primary data required for the compilation of the open dataset to the Agency according to Article 6(1)(c) of 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) (in fulfilment of the legal obligation applicable to the data controller), special categories of personal data – according Article 9(2)(g) of the Regulation (on public interest grounds). Since there is a legal basis for the transfer of personal data provided for in Article 6(1)(c) and Article 9(2)(g) of Regulation (EU) 2016/679, the consent of the data subjects for the transfer of their personal data to the Agency is not required, and provision of personal data to the Agency cannot be considered a breach of personal data security.

2.8. Project staff

The project activities will be carried out by 74 employees, who can be divided into several groups: programmers, developer-analysts/ confidentiality/quality specialists, DB administrators, information managers, data lawyers and project managers.

DocuSign Envelope ID: 5A45EFF2-9542-436F-B64A-A4C98DF04360

3. Reikalavimai skaičiavimo ištekliams

Nr.	Reikalavimas
1.	Metaduomenų inventorizacijai ir duomenų integracijai turi būti rezervuota pakankamai skaičiavimo ir duomenų laikymo išteklių.
2.	Tiekėjas turi išplėsti Palantir Foundry licenciją papildomais infrastruktūros ištekliais (toliau – papildoma infrastruktūra) ir iki 2024 m. gruodžio 5 d užtikrinti ne mažesnius išteklių kiekius, nei nurodyta žemiau esančioje lentelėje.

Platformos išteklių tipas	Kiekis	Matavimo vienetas
Paketinis skaičiavimas	179 000	skaičiavimo valanda
Interaktyvus skaičiavimas	930	skaičiavimo valanda
Vidutinė sunaudojama disko vieta	6 900	GB per mėnesį
Vidutinė sunaudojama indeksuota vieta	80	GB per mėnesį

4. Reikalavimai papildomai duomenų valdymo platformos (DVP) infrastruktūrai

Nr.	Reikalavimas
3.	Papildomos infrastruktūros duomenų saugojimo funkcionalumas turi atitikti DVP reikalavimus: - palaikyti paskirstytas, saugias ir plačiai pasiekiamas duomenų saugojimo infrastruktūras, tokias kaip, pvz., Azure Blob Store, HDFS ar Amazon S3; - turi galėti dinamiškai plėstis (angl. *horizontal scaling*) pagal realaus laiko resursų poreikį, taip užtikrindama reikalingus resursus turimam duomenų kiekiui ir naudotojų skaičiui.
4.	Papildomos infrastruktūros tarnybinių stočių veikimas turi būti nuolatos stebimas. Į iškilusius incidentus turi būti operatyviai reaguojama ir sutrikimai turi būti šalinami pagal standartines veiklos procedūras.
5.	Turi būti užtikrintas DVP prieinamumas ne mažiau kaip 99 proc. laiko visą parą vidutiniškai per metus.
6.	DVP turi būti laikoma Europos Sąjungos valstybėse narėse ir (arba) Europos ekonominės erdvės valstybėse narėse esančiuose duomenų centruose.
7.	Turi būti galimybė perkelti DVP į kitą nei tiekėjo infrastruktūrą (pvz., Valstybinis duomenų centras) agentūros sąnaudomis. Tiekėjas turi pateikti tokio parkėlimo instrukcijas/rekomendacijas.
	Pateikiama DVP papildoma infrastruktūra turi atitikti šiuos informacinei infrastruktūrai keliamus techninius kibernetinio saugumo reikalavimus:
8.	Tarptautinio standarto ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems — Requirements arba lygiaverčio jam standarto.
9.	Tarptautinio standarto ISO/IEC 27002:2013 Information technology – Security techniques – Code of practice for information security controls arba lygiaverčio jam standarto. DVP papildomoje infrastruktūroje saugomi duomenys turi būti apsaugoti nuo nesankcionuoto priėjimo, naudojimo, pakeitimo, atskleidimo, sunaikinimo ar praradimo.
10.	Šių tarptautinių standartų arba lygiaverčių 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).

3. Requirements for computing resources

No.	Requirement
1.	Sufficient computing and data storage resources shall be reserved for metadata inventory and data integration.
2.	The supplier shall extend the Palantir Foundry license with additional infrastructure resources (hereinafter referred to as “additional infrastructure”) and by 5 December 2024 to ensure no less than the amount of resources indicated in the table below.

Platform resource type	Amount	Unit of measurement
Batch calculation	179 000	counting hour
Interactive calculation	930	counting hour
Average disk space used	6 900	GB per month
Average indexed space consumed	80	GB per month

4. Requirements for additional data management platform (DMP) infrastructure

No.	Requirement
3.	Data storage functionality of additional infrastructure shall meet requirements of the DMP: - - support distributed, secure and widely available data storage infrastructures, such as, for example, Azure Blob Store, HDFS or Amazon S3; - - horizontal scaling according to real-time resource needs shall be possible, thus ensuring necessary resources for the available amount of data and the number of users.
4.	Operation of the service stations of additional infrastructure shall be constantly monitored. Arising incidents shall be responded to promptly, and problems shall be resolved in accordance with standard operating procedures.
5.	Availability of the DMP shall be ensured at least 99 per cent 24/7 time per year on average.
6.	DMP shallt be stored in data centers located in member states of the European Union and/or member states of the European Economic Area.
7.	It shall be possible to move the DMP to a non-supplier infrastructure (e.g., the State Data Center) at the Agency's expense. The supplier shall provide instructions/recommendations for such transfer.
	The provided DMP additional infrastructure shall meet the following technical cyber security requirements for information infrastructure:
8.	International standard ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems — Requirements or an equivalent standard.
9.	International standard ISO/IEC 27002:2013 Information technology – Security techniques – Code of practice for information security controls or an equivalent standard. Data stored in the additional infrastructure of the DMP shall be protected against unauthorized access, use, alteration, disclosure, destruction or loss.
10.	These international standards or equivalent standards: 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).

DocuSign Envelope ID: 5A45EFF2-9542-436F-B64A-A4C98DF04360

Nr.	Reikalavimas
11.	Siekiant užtikrinti perduodamos informacijos saugą, turi būti naudojama ne žemesne nei TLS 1.2 kriptografijos protokolo versija šiuose komunikacijos scenarijuose: sistema–naudotojas ir pagal poreikį sistema–sistema.
12.	Duomenys DVP papildomoje infrastruktūroje turi būti šifruojami tiek tranzito metu (angl. in transit), tiek ramybės būsenoje (angl. at rest).
13.	Turi būti galimybė agentūrai naudoti savo šifravimo raktą (angl. bring your own key) duomenims šifruoti DVP papildomoje infrastruktūroje ir prireikus jį ištrinti, taip užtikrinant, kad duomenys liks užšifruoti ir nepasiekiami.
14.	DVP papildoma infrastruktūra turi būti apsaugota nuo: - neautentifikuotos prieigos; - naudotojų veiksmų, neatitinkančių jų autorizacijos rolės; - nesankcionuoto naudotojo sesijos perėmimo; - nesankcionuoto duomenų perėmimo ar jų įterpimo; - žalingo kodo įterpimo (angl. Injection, XSS (Cross-site scripting)); - kitų saugumo pažeidimų, kurie įvardijami OWASP - TOP 10 (https://www.owasp.org) arba lygiaverčiame sąraše.
15.	Sistemos slaptažodžiai negali būti saugojami programiniame kode.
16.	Sistemos svetainė turi drausti išsaugoti slaptažodžius.
17.	Atliekant sistemos svetainės administravimo darbus ryšys turi būti šifruojamas naudojant ne trumpesnį kaip 128 bitų raktą.
18.	Šifruojant naudojami skaitmeniniai sertifikatai privalo būti išduoti patikimų sertifikavimo tarnybų. Sertifikato raktas turi būti ne trumpesnis kaip 2048 bitų.
19.	Svetainės kriptografinės funkcijos turi būti įdiegtos tarnybinės stoties, kurioje yra svetainė, dalyje arba kriptografiniame saugumo modulyje (angl. Hardware security module).
20.	Visi kriptografiniai moduliai turi gebėti saugiai sutrikti (angl. fail securely).
21.	Draudžiama sistemos tarnybinėje stotyje saugoti sesijos duomenis (identifikatorių), pasibaigus susijungimo sesijai.
22.	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).
23.	Turi būti naudojama sistemos svetainė naudotojo įvedamų duomenų tikslumo kontrolė (angl. validation).
24.	Tarnybinė stotis, kurioje yra sistemos svetainė, neturi rodyti sistemos svetainės naudotojui klaidų pranešimų apie svetainės programinį kodą ar tarnybinę stotį.
25.	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).

No.	Requirement
11.	In order to ensure security of transmitted information, a cryptographic protocol version no lower than TLS 1.2 shall be used in the following communication scenarios: system-to-user and system-to-system as needed.
12.	Data in the additional infrastructure of the DMP shall be encrypted both in transit and at rest.
13.	It shall be possible for the Agency to bring your own key to encrypt data in the additional infrastructure of the DMP and delete it if necessary, thus ensuring that data remains encrypted and inaccessible.
14.	Additional infrastructure of the DMP shall be protected against: - unauthenticated accesses; - user actions that do not correspond to their authorization role; - unauthorized interception of the user's session; - unauthorized interception of data or their insertion; - malicious code insertion (Injection, XSS (Cross-site scripting)); - other security violations that are identified by OWASP - TOP 10 (https://www.owasp.org) or equivalent list.
15.	System passwords cannot be stored in code.
16.	System site must prohibit saving passwords.
17.	When performing administration work on the system site, the connection shall be encrypted using a key of at least 128 bits.
18.	Digital certificates used for encryption shall be issued by trusted certification services. The certificate key must be at least 2,048 bits.
19.	The website's cryptographic functions shall be implemented in the part of the service station where the website is located or in the hardware security module.
20.	All cryptographic modules shall be able to fail securely.
21.	It is prohibited to store session data (identifier) at the system service station after the connection session has ended.
22.	Web Application Firewall shall be used. Attack signatures shall be updated using reliable sources that provide up-to-date information. The latest attack signatures shall be installed no later than twenty-four hours from the date of the manufacturer's announcement of the latest attack signatures, or no later than seventy-two hours from the date of the manufacturer's announcement of the latest attack signatures, if assessment (testing) of implementation of attack signatures and their possible impact on the operation of state information resources or critical information infrastructure is carried out by decision of the manager of the state's information resources or critical information infrastructure.
23.	Validation (control) of accuracy of data entered by the user of the system site shall be used.
24.	The service station hosting the system site shall not display to the user of the system site error messages about the site's code or the service station.
25.	Security measures of the system site shall be able to prohibit access to the service station from IP addresses that have performed malicious activities (unauthorized attempts to connect, insert SQL inserts, etc.).

DocuSign Envelope ID: 5A45EFF2-9542-436F-B64A-A4C98DF04360

Nr.	Reikalavimas
26.	Tarnybinė stotis, kurioje yra sistemos svetainė, turi leisti tik svetainės funkcionalumui užtikrinti reikalingus protokolo metodus.
27.	Turi būti uždrausta naršyti sistemos svetainės aplankuose (angl. *directory browsing*).
28.	Turi būti įdiegta sistemos svetainė turinio nesankcionuoto pakeitimo (angl. *defacement*) stebėsenos sistema.
29.	DVP infrastruktūroje turi būti fiksuojamos naudotojų registracijos užklausos, prisijungimo sesijos, jų pradžia, pabaiga, naudotojų veiksmai, teisių naudotis sistema pakeitimai, veiksmai su sistemos objektais, audito funkcijos įjungimas ar išjungimas, audito įrašų trynimas, kūrimas ar keitimas, laiko ir (ar) datos pakeitimai ir kiti veiksmai.
30.	Turi būti sudaryta galimybė tokių auditų žurnalų eksportavimui už DVP infrastruktūros ribų.
31.	Kiekviename audito duomenų įraše turi būti fiksuojama įvykio data ir tikslus laikas, įvykio rūšis, naudotojo duomenys, įvykio rezultatas.
32.	Priemonės, naudojamos sistemos sąsajoje su viešųjų elektroninių ryšių tinklu, turi būti nustatytos taip, kad fiksuotų visus įvykius, susijusius su įeinančiais ir išeinančiais duomenų srautais.
33.	Sistemoje fiksuojami įvykiai turi būti saugomi techninėje ar programinėje įrangoje, pritaikytoje audito duomenims saugoti.
34.	Dėl įvairių trikdžių nustojus fiksuoti auditui skirtus duomenis, apie tai nedelsiant turi būti informuojamas sistemos administratorius.
35.	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).
36.	Draudžiama audito duomenis trinti, keisti, kol nesibaigęs audito duomenų saugojimo terminas.
37.	Audito duomenų kopijos turi būti apsaugotos nuo pažeidimo, praradimo, nesankcionuoto pakeitimo ar sunaikinimo.
38.	Turi būti naudojami mažiausiai du laiko sinchronizavimo šaltiniai.
39.	Naudotojų darbo sesija turi būti automatiškai užbaigiama, jei neveikimo laikas viršija nustatytą trukmę.
40.	DVP infrastruktūros prieigos teisių modelio ir saugumo funkcionalumų visuma turi suteikti galimybę DVP infrastruktūroje saugomiems duomenims atitikti Europos Sąjungos Bendrąjį duomenų apsaugos reglamentą (BDAR).

No.	Requirement
26.	The service station hosting the system site shall allow only protocol methods necessary to ensure functionality of the site.
27.	Directory browsing shall be prohibited.
28.	Defacement monitoring system shall be installed on the website of the system.
29.	Infrastructure of the DMP shall record user registration requests, login sessions, their start and end, user actions, changes in rights to use the system, actions with system objects, enabling or disabling the audit function, deleting, creating or changing audit records, time and (or) date changes and other actions.
30.	It shall be possible to export such audit logs outside the infrastructure of the DMP.
31.	Each audit data record shall record date and exact time of the event, type of event, user data, and result of the event.
32.	Means used to interface the system with the public electronic communications network shall be set to record all events related to incoming and outgoing data flows.
33.	Events recorded in the system shall be stored in hardware or software adapted to store audit data.
34.	If the recording of audit data stops due to various disturbances, the system administrator shall be informed immediately.
35.	Audit data shall be stored for at least sixty days, ensuring all meaningful values of its content (for example, identification data of a system user with whom employment relations have been terminated and who has been removed from the system shall be preserved for the entire necessary audit data storage period).
36.	It is forbidden to delete or change audit data until the audit data storage term has expired.
37.	Copies of audit data shall be protected against damage, loss, unauthorized alteration or destruction.
38.	At least two time synchronization sources shall be used.
39.	Users' work session should be automatically terminated if the idle time exceeds the specified duration.
40.	Set of access rights model and security functionalities of the DMP infrastructure shall enable data stored in the DMP infrastructure to comply with the European Union's General Data Protection Regulation (GDPR).

DocuSign Envelope ID: 5A45EFF2-9542-436F-B64A-A4C98DF04360

5. Reikalavimai saugumui

Nr.	Reikalavimas
41.	Tiekėjo siūlomos paslaugos neturi kelti grėsmės nacionaliniam saugumui: - Tiekėjas, teikdamas pasiūlymą, patvirtina, kad jo siūlomos paslaugos nekelia grėsmės nacionaliniam saugumui. Paslaugų teikėjas ar jį kontroliuojantis asmuo negali būti registruoti (jeigu paslaugų teikėjas ar jį kontroliuojantis asmuo yra fizinis asmuo – nuolat gyvenantis ar turintis pilietybę) Lietuvos Respublikos viešųjų pirkimų įstatymo 92 straipsnio 14 dalyje numatytame sąraše nurodytose valstybėse ar teritorijoje (https://e-seimas.lrs.lt/portal/legalAct/lt/TAP/16f99e01af6811ecaf79c2120caf5094); Paslaugų teikimas negali būti vykdomas iš šio Lietuvos Respublikos viešųjų pirkimų įstatymo 92 straipsnio 14 dalyje numatytame sąraše nurodytų valstybių ar teritorijų (https://e-seimas.lrs.lt/portal/legalAct/lt/TAP/16f99e01af6811ecaf79c2120caf5094).
42.	Tiekėjas turi turėti pasitvirtinęs vidines taisykles (tvarkas), kuriose būtų nustatytos kibernetinio saugumo ir duomenų apsaugos įgyvendinimo taisyklės ir procedūros
43.	Tiekėjas turi turėti įdiegęs tinkamas jo pateiktos papildomos infrastruktūros tinklo saugumo sistemas: ugniasienė, įsibrovimų nustatymo sistema arba kita aktyvi ar pasyvi įranga, naudojama tinklo saugumui užtikrinti.
44.	Tiekėjas turi turėti įdiegęs priemones jo pateiktos papildomos infrastruktūros tinklo stebėsenai realiame laike tam, kad būtų užkirstas kelias įtartinai veiklai tinkle ir fiksuojami reikiami įrodymai.
45.	Turi būti naudojama praėjimo kontrolė į patalpas, kur saugojama tiekėjo pateikta papildoma infrastruktūra (patalpų išskaidymas, lankytojų palyda, nešiojimas matomoje vietoje pažymėjimų, rakinamos durys, vaizdo stebėseną ir pan.).
46.	Tiekėjas turi naudoti priemones, skirtas sumažinti nuo žmogaus nepriklausančias rizikas (gaisras, potvynis, nelaimingi atsitikimai ir pan.) bei išvengti rizikų neteisėtam duomenų tvarkymui.
47.	Tiekėjas turi turėti nustatytas veiklos tęstinumo procedūras, kurių reikia laikytis kibernetinio saugumo incidento ar asmens duomenų saugumo pažeidimo atveju, kad būtų užtikrintas reikiamas agentūros duomenų tvarkymo IT sistemomis tęstinumas ir prieinamumas.
48.	Tiekėjas turi turėti nustatytą tvarką, kurioje aprašomi tiekėjo darbuotojų mokymai, siekiant juos supažindinti su kibernetinio saugumo ir duomenų apsaugos taisyklėmis bei skatinant juos turėti daugiau sąmoningumo kibernetinio saugumo ir duomenų apsaugos klausimais.

5. Security requirements

No.	Requirement
41.	Services offered by the supplier shall not pose threat to national security: - When submitting an offer, the supplier confirms that the services the supplier offers do not pose threat to national security. The service provider or the person controlling the service provider cannot be registered (if the service provider or the person controlling the service provider is a natural person – permanent resident or citizen) in the states or territories specified in the list provided for in Article 92(14) of the Law on Public Procurement of the Republic of Lithuania (https://e-seimas.lrs.lt/portal/legalAct/lt/TAP/16f99e01af6811ecaf79c2120caf5094); The service provision may not be carried out from the states or territories specified in the list provided for in Article 92(14) of this Law on Public Procurement of the Republic of Lithuania (https://e-seimas.lrs.lt/portal/legalAct/lt/TAP/16f99e01af6811ecaf79c2120caf5094).
42.	The supplier shall have approved internal rules (procedures) that would determine rules and procedures for the implementation of cyber security and data protection.
43.	The supplier shall have installed appropriate network security systems for the additional infrastructure provided by him: firewall, intrusion detection system or other active or passive equipment used to ensure network security.
44.	The supplier shall have in place measures for real-time monitoring of the additional infrastructure network provided by him in order to prevent suspicious activities in the network and capture necessary evidence.
45.	Access control shall be used to the premises where additional infrastructure provided by the supplier is stored (decomposition of premises, escort of visitors, wearing of certificates in a visible place, locked doors, video monitoring, etc.).
46.	The supplier shall use measures to reduce risks beyond human control (fire, flood, accidents, etc.) and avoid risks of illegal data processing.
47.	The supplier shall have established business continuity procedures to be followed in the event of a cyber security incident or personal data security breach to ensure the necessary continuity and availability of the Agency's data processing with IT systems.
48.	The supplier shall have an established procedure that describes trainings of the supplier's employees in order to familiarize them with the rules of cyber security and data protection and to encourage them to be more aware of cyber security and data protection issues.

DocuSign Envelope ID: 5A45EFF2-9542-436F-B64A-A4C98DF04360

UŽSAKOVAS
Valstybės duomenų agentūra
Gedimino pr. 29, LT-01500 Vilnius
Įmonės kodas: 188600177
PVM mokėtojo kodas: nėra
A. s. Nr. LT02 4040 0636 1000 0121
Bankas: Lietuvos Respublikos finansų ministerija
Banko kodas 40400
Tel. + 370 656 97 121
El. p. statistika@stat.gov.lt
Tinklapis: http://www.stat.gov.lt

Generalinio direktoriaus pavaduotoja, atliekanti generalinio direktoriaus funkcijas, Inga Masiulaitytė-Šukevič

E418C627BC95493...

September 28, 2023

CUSTOMER
State data Agency
Gedimino Ave. 29, LT-01500 Vilnius, Lithuania
Company code: 188600177
VAT number: none
Settlement account No. LT02 4040 0636 1000 0121
Bank: Ministry of Finance of the Republic of Lithuania
Bank code 40400
Tel. + 370 656 97 121
E-mail: statistika@stat.gov.lt
Website: http://www.stat.gov.lt

Inga Masiulaitytė-Šukevič, Deputy Director General, Acting Director General

DocuSigned by:

E418C627...

September 28, 2023

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: JPMorgan Chase Bank
Sąskaitos savininkas: Palantir Technologies UK, Ltd.
A. s. Nr.: 41036032
IBAN: GB09CHAS60924241036032
SWIFT: CHASGB2L
Tel. +44 7408 886228
El. p. accountsreceivable@palantir.com / legalnotices@palantir.com

Direktorius Ryan Taylor

2023 m. rugsėjo 28 d

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: JPMorgan Chase Bank
Account Holder: Palantir Technologies UK, Ltd.
Account Number: 41036032
IBAN: GB09CHAS60924241036032
SWIFT: CHASGB2L
Phone No. +44 7408 886228
E-mail: accountsreceivable@palantir.com / legalnotices@palantir.com

Ryan Taylor, Director

September 28, 2023