AGREEMENT ON PROCESSING OF PERSONAL DATA AND INFORMATION	SUSITARIMAS DĖL ASMENS DUOMENŲ IR INFORMACIJOS TVARKYMO
By providing the services provided in the contract Regarding the license lease for Palantir Foundry, including infrastructure, signed October 18, 2024 (hereinafter referred to as the "Contract"), Palantir Technologies Lithuania, UAB name (hereinafter referred to as the "Supplier") will process personal data on behalf of the State Data Agency (hereinafter referred to as the "Customer"), in accordance with this Agreement on processing of personal data and information (hereinafter referred to as the "Agreement"). 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:	Teikdamas 2024 m. spalio 18 d. pasirašytoje sutartyje „Dėl Palantir Foundry, įskaitant infrastruktūrą, licencijos nuomos" (toliau – „Sutartis") numatytas paslaugas, UAB „Palantir Technologies Lithuania" (toliau – Tiekėjas) tvarkys asmens duomenis Valstybės duomenų agentūros (toliau – „Užsakovas") vardu pagal šį Susitarimą dėl asmens duomenų ir informacijos tvarkymo (toliau – „Susitarimas"). Kadangi, vykdydamas Sutartį, Tiekėjas gali matyti asmens duomenis, šalys siekia užtikrinti asmens duomenų apsaugą ir atitiktį 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamento (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (toliau – „Bendrasis duomenų apsaugos reglamentas") reikalavimams ir sutaria dėl asmens duomenų tvarkymo sąlygų taip:
1. DEFINITIONS 1.1. For the purposes of this Agreement 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 Agreement shall have the meanings	**1. APIBRĖŽTYS** 1.1. Šio Susitarimo tikslais toliau nurodyti terminai ir sąvokos turi žemiau pateikiamas reikšmes, jei kontekstas nereikalauja kitaip: 1.1.1. **Duomenų subjektas** – tai fizinis asmuo, kurio duomenis gali matyti Tiekėjo grupė (kaip apibrėžta žemiau). 1.1.2. **Duomenų tvarkymo tikslas** – tai Sutarties vykdymo paskirtis ir tikslas, susijęs su atitinkamos šalies pagal Sutartį atsirandančių teisių ir pareigų vykdymu. 1.1.3. **Paslaugos** – tai visos paslaugos ir darbai, kuriuos Tiekėjo grupė (kaip apibrėžta žemiau) pagal Sutartį atlieka, teikia ir perduoda Užsakovui, taip pat šių paslaugų ir darbų rezultatai. 1.1.4. **Sistema** – tai Valstybės duomenų valdysenos informacinė sistema. 1.2. Šio Susitarimo 1.1 punkte neapibrėžti terminai ir sąvokos turi reikšmes, nustatytas duomenų apsaugos teisės aktuose ir Sutartyje.

given to them in the data protection legislation and in the Contract.	
2. TERMS AND CONDITIONS FOR PERSONAL DATA PROCESSING	**2. ASMENS DUOMENŲ TVARKYMO SĄLYGOS IR NUOSTATOS**
2.1. The Parties agree that in the implementation of the Contract, the Supplier as a processor or its subsidiaries and affiliates (the "Supplier Group") as subprocessors may be required to perform the data processing operations specified in Subparagraph 2.7 of this Agreement with the specified personal data and/or sets thereof on behalf of the Customer. The implementation of the data processing purpose specified in this section of the Agreement in combination with the purposes defined in the License Terms under Subparagraph 3.1. shall be considered as the subject of personal data processing agreed by the parties.	2.1. Šalys susitaria, kad vykdydamas Sutartį Tiekėjas, veikdamas kaip duomenų tvarkytojas, arba jo dukterinės įmonės ir susijusios bendrovės (toliau – „Tiekėjo grupė"), veikiančios kaip subtvarkytojai (pagalbiniai duomenų tvarkytojai), gali būti įpareigoti atlikti šio Susitarimo 2.7 papunktyje nurodytas duomenų tvarkymo operacijas su tam tikrais asmens duomenimis ir (arba) jų rinkiniais Užsakovo vardu. Šiame Susitarimo skirsnyje nurodytas duomenų tvarkymo tikslas kartu su Licencijos sąlygose 3.1 papunktyje apibrėžtais tikslais laikomas asmens duomenų tvarkymo dalyku, dėl kurio šalys susitarė.
2.2. The parties note that the Supplier Group does not exclusively seek to process personal data; however, the personal data processing operations shall be carried out only when strictly necessary for the proper implementation of the Contract.	2.2. Šalys pažymi, kad Tiekėjo grupė nesiekia tvarkyti asmens duomenų vien tik savo iniciatyva; tačiau asmens duomenų tvarkymo operacijos bus vykdomos tik tada, kai tai yra griežtai būtina tinkamam Sutarties įgyvendinimui.
2.3. The parties agree that for the purposes of the Contract, the Supplier Group operates as a (Sub-) Processor and the Customer operates as a Controller.	2.3. Šalys susitaria, kad vykdydama Sutartį Tiekėjo grupė veikia kaip (Sub-)Tvarkytojas, o Užsakovas – kaip Valdytojas.
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 Agreement 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.	2.4. Šalys susitaria, kad Užsakovas savo nuožiūra ir atsakomybe nustatys duomenų subjektų kategorijas ir asmens duomenų kategorijas, kurios kiekvienu konkrečiu atveju bus teikiamos Tiekėjo grupei. Užsakovas pateiks Tiekėjo grupei tik tuos asmens duomenis, kurie būtini siekiant 2.1 punkte nurodyto šio Susitarimo tikslo, ir prisiima visą su tuo susijusią riziką (įskaitant riziką, kai Tiekėjo grupei pateikiama daugiau asmens duomenų, nei būtina). Siekdamas užtikrinti tinkamą perduodamų asmens duomenų apimtį, Užsakovas gali, savo sąskaita ir pastangomis, imtis papildomų priemonių, pvz., asmens duomenų šifravimo, pseudonimų suteikimo ir pan.
2.5. If, based on the Supplier Group's estimation and in accordance with section 2.4 of the Agreement, the data provided by the Customer in particular case are insufficient for proper implementation of the purpose provided in section 2.1 of the Agreement, 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	2.5. Jeigu Tiekėjo grupė, remdamasi savo vertinimu ir vadovaudamasi šio Susitarimo 2.4 punktu, nustato, kad Užsakovo pateikti duomenys konkrečiu atveju yra nepakankami tinkamam 2.1 punkte nurodyto šio Susitarimo tikslo įgyvendinimui, Tiekėjo grupė informuoja Užsakovą, prašydama pateikti papildomus asmens duomenis, kurie yra būtini šiuo konkrečiu atveju. Gavęs atitinkamą pranešimą iš

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 categories of personal data and categories of data subjects that the Customer can transfer to the Supplier Group for processing in accordance with this Agreement are in particular specified in the 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 in particular such personal data that is specified in Table 1 that may be updated from time to time. 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. The Customer's and the Supplier Group's employee's name and

Tiekėjo grupės, Užsakovas priima galutinį sprendimą, ar papildomi asmens duomenys turėtų būti pateikti, ir prisiima visą su tokiu sprendimu susijusią riziką (įskaitant riziką, kad nepateikus papildomų duomenų, Tiekėjo grupė gali nesugebėti tinkamai įvykdyti įsipareigojimų pagal Sutartį).

2.6. Įgyvendindamas Sutartį, Tiekėjas gali rinkti metrikas, analitinius duomenis, statistinę informaciją ar kitus duomenis, susijusius su Užsakovo programinės įrangos naudojimu: (a) siekdamas teikti ir užtikrinti programinės įrangos bei paslaugų prieinamumą ir naudą Užsakovui; (b) statistiniams tikslams, taip pat siekdamas analizuoti, palaikyti ir tobulinti programinę įrangą bei paslaugas (su sąlyga, kad šie duomenys bus pateikti taip, kad jų nebūtų galima susieti su konkrečiu asmeniu).

2.7. Šalys susitaria, kad asmens duomenų kategorijos ir duomenų subjektų kategorijos, kurias Užsakovas gali perduoti Tiekėjo grupei tvarkyti pagal šį Susitarimą, yra konkrečiai nurodytos 1 lentelėje pateiktuose sąrašuose. Užsakovas įsipareigoja perduoti Tiekėjo grupei tvarkyti būtent tuos asmens duomenis, kurie yra nurodyti 1 lentelėje ir kurie gali būti periodiškai atnaujinami. Už šių sąrašų sudarymą ir atnaujinimą atsako Užsakovas.

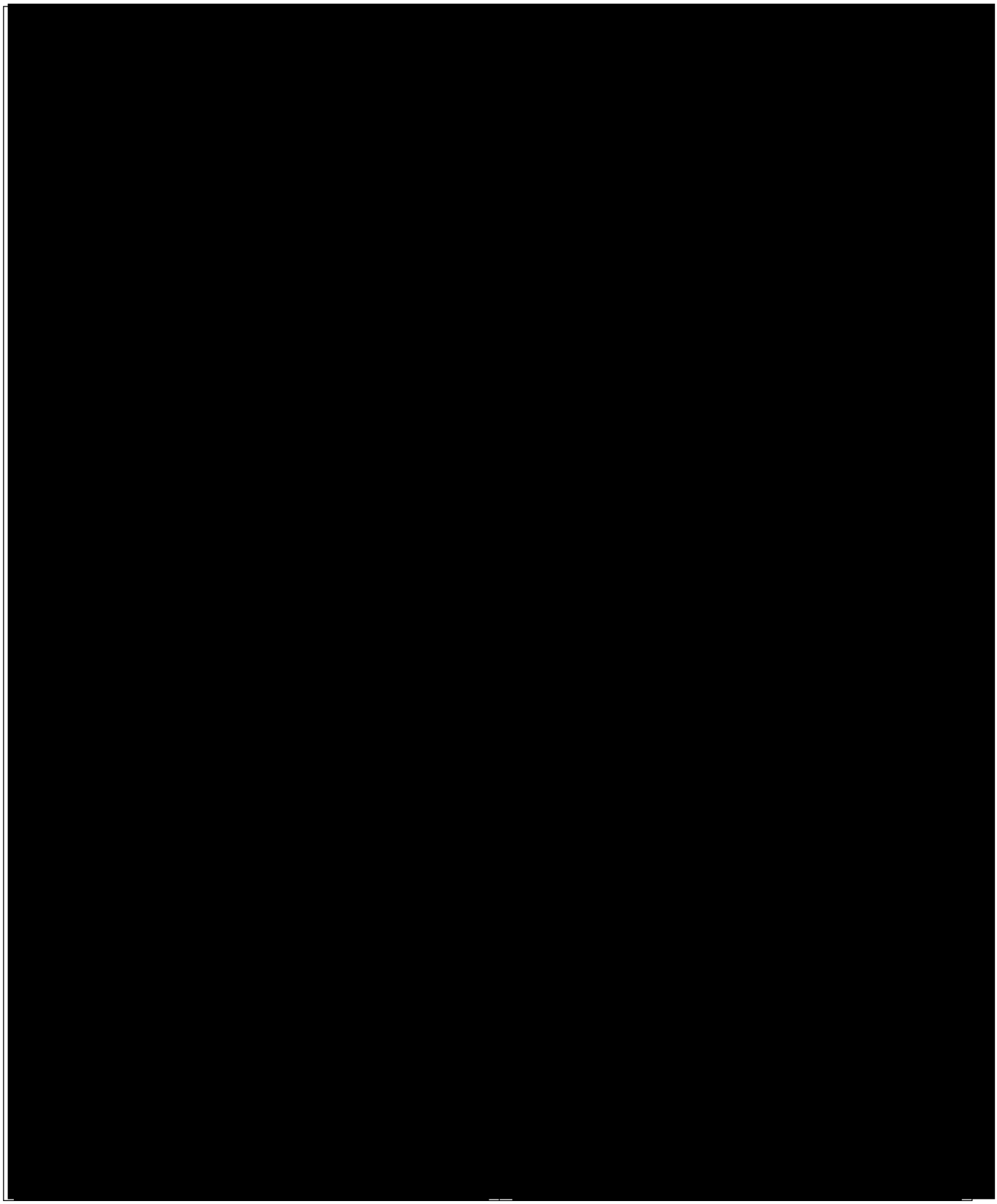
1 lentelė

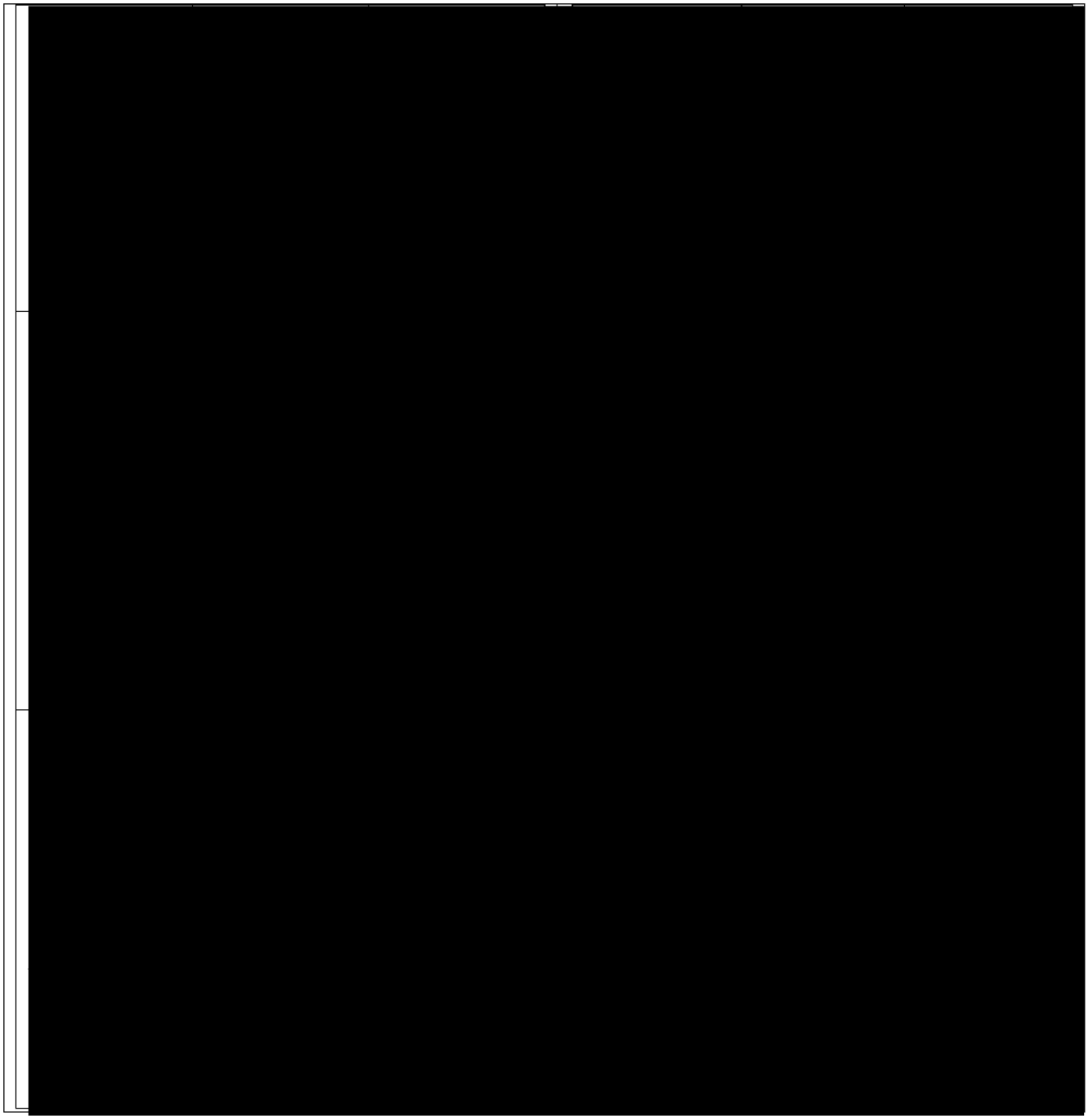
Duomenų tvarkymo tikslas ir objektas	Sutarties įgyvendinimui ir SDM IS veikimo užtikrinimui
Asmens duomenų kategorijos	Asmens duomenys apie Lietuvos gyventojus ir nerezidentus, gauti iš administracinių duomenų šaltinių. Užsakovo ir Tiekėjo grupės darbuotojo vardas ir pavardė, padalinys, pareigos,

	surname, division, position, telephone, e-mail, user code, other information to identify the employee and grant rights to work with the system.		telefono numeris, el. paštas, vartotojo kodas, kiti duomenys, skirti darbuotojo identifikavimui ir teisių suteikimui dirbti su sistema.
Categories of data subjects	Residents of Lithuania, employees of the Customer, employees of the Supplier Group	Duomenų subjektų kategorijos	Lietuvos gyventojai, Užsakovo darbuotojai, Tiekėjo grupės darbuotojai.
Activity related to data processing	Familiarization with personal data by performing the following actions: o Extraction of personal data from administrative data sources and the Customer's databases and integration. o Recovery of corrupted software data (including personal data). o System recovery in cases of complete or partial malfunction. o System event log analysis.	Veikla, susijusi su duomenų tvarkymu	Susipažinimas su asmens duomenimis atliekant šiuos veiksmus: - Asmens duomenų ištraukimas iš administracinių duomenų šaltinių ir Užsakovo duomenų bazių bei integravimas. - Sugadintų programinės įrangos duomenų (įskaitant asmens duomenis) atkūrimas. - Sistemos atkūrimas visiško ar dalinio sutrikimo atveju. - Sistemos įvykių žurnalo analizė.

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 Agreement 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. Upon returning/deleting data, the Supplier provides a written confirmation of data removal.	2.8. Šalys sutaria, kad Tiekėjo grupė pradės asmens duomenų tvarkymą, kai Užsakovas pateiks šiuos duomenis arba suteiks prieigą prie šių duomenų, ir baigs tvarkymą, kai Tiekėjo grupė įvykdys Susitarimo 2.1 punkte nurodytą tikslą ir (arba) ištrins duomenis pasibaigus jų saugojimo laikotarpiui (jei toks yra) arba, Užsakovo prašymu, grąžins juos Užsakovui ir (arba) ištrins. Grąžinant (ištrinant) duomenis, Užsakovas pateikia raštišką duomenų pašalinimo patvirtinimą.
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 Agreement in compliance with the personal data protection legislation and the instructions (if any) documented in written form by the Customer. 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 30 days 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 (Agreement) imposes on that other subcontractor the same data protection obligations as those imposed on the Supplier Group by this Contract and Agreement. The Supplier must evaluate whether proper technical and organizational measures will be implemented in such a way that the personal data processing complies with the requirements of the personal data protection legislation and provide a written confirmation to the Customer herewith other information about the subcontractor. Where the Customer objects to suggested subcontractor, the Supplier Group shall not engage the intended subcontractors. 3.3. The Customer gives the Supplier Group a general consent for engagement of other subcontractors ("Subprocessor(s)") for personal data processing on behalf of the Customer, 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 30 days in	**3. ASMENS DUOMENŲ TVARKYMO REIKALAVIMAI** 3.1. Tiekėjo grupė įsipareigoja atlikti asmens duomenų tvarkymo veiksmus tik dėl Susitarimo 2.1 punkte nurodyto tikslo, laikydamasi asmens duomenų apsaugos teisės aktų ir Užsakovo raštu pateiktų nurodymų (jei tokių yra). 3.2. Jei tai numatyta Sutartyje, Užsakovas suteikia Tiekėjo grupei bendrą sutikimą įtraukti subrangovus asmens duomenų tvarkymui. Jei Sutartyje nenurodyta kitaip, prieš įtraukdama naują subrangovą arba pakeisdama esamą subrangovą, Tiekėjo grupė raštu informuoja Užsakovą ne vėliau kaip prieš 30 dienų, pateikdama planuojamo subrangovo detales bei kitą Užsakovo prašomą informaciją, susijusią su duomenų tvarkymo veikla. Jei Tiekėjo grupė pasitelkia subrangovą konkrečiai asmens duomenų tvarkymo veiklai, Sutartis (Susitarimas) nustato tokiam subrangovui tas pačias duomenų apsaugos prievoles, kurios pagal šią Sutartį ir Susitarimą yra taikomos Tiekėjo grupei. Tiekėjas privalo įvertinti, ar bus įgyvendintos tinkamos techninės ir organizacinės priemonės, užtikrinančios, kad asmens duomenų tvarkymas atitiks asmens duomenų apsaugos teisės aktų reikalavimus, ir pateikti Užsakovui raštišką patvirtinimą kartu su kita informacija apie subrangovą. Jei Užsakovas nepritaria siūlomam subrangovui, Tiekėjo grupė negali pasitelkti numatyto subrangovo. 3.3. Užsakovas suteikia Tiekėjo grupei bendrą sutikimą įtraukti kitus subrangovus („Subtvarkytoją(us)“) asmens duomenų tvarkymui Užsakovo vardu, įskaitant, bet neapsiribojant, nurodytais 2 lentelėje. Tiekėjo grupė privalo informuoti Užsakovą apie bet kokius planuojamus pakeitimus, susijusius su naujų Subtvarkytojų įtraukimu ar esamų pakeitimu, ne vėliau kaip prieš 30

advance, 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 Agreement imposes on that other Subprocessor the same data protection obligations as those imposed on the Supplier Group by this Contract and Agreement. The Supplier must evaluate whether proper technical and organizational measures will be implemented in such a way that the personal data processing complies with the requirements of the personal data protection legislation and provide a written confirmation to the Customer herewith other information about the subprocessor. Where the Customer objects to suggested subprocessor, the Supplier Group shall not engage the intended subprocessor.	dienų, suteikdama Užsakovui galimybę pareikšti prieštaravimą dėl tokių pakeitimų. Kai Tiekėjo grupė pasitelkia Subtvarkytoją konkrečiai asmens duomenų tvarkymo veiklai, Sutartis ir Susitarimas nustato šiam Subtvarkytojui tas pačias duomenų apsaugos prievoles, kurios pagal šią Sutartį ir Susitarimą taikomos Tiekėjo grupei. Tiekėjas turi įvertinti, ar bus įgyvendintos tinkamos techninės ir organizacinės priemonės, užtikrinančios, kad asmens duomenų tvarkymas atitiks asmens duomenų apsaugos teisės aktų reikalavimus, ir pateikti Užsakovui raštišką patvirtinimą kartu su kita informacija apie Subtvarkytoją. Jei Užsakovas nepritaria siūlomam Subtvarkytojui, Tiekėjo grupė negali pasitelkti numatyto Subtvarkytojo.
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.	3.4. Tiekėjo grupė įsipareigoja, Užsakovo prašymu, nedelsiant nutraukti bet kokį asmens duomenų tvarkymą, išskyrus saugojimą, ir atnaujinti tvarkymo veiklą tik gavusi Užsakovo nurodymą.
3.5. The Supplier Group undertakes, upon receipt of a written request of the Customer, to delete (or return) personal data and copies thereof which are processed based on this Contract and Agreement.	3.5. Tiekėjo grupė įsipareigoja, gavusi raštišką Užsakovo prašymą, ištrinti (arba grąžinti) pagal šią Sutartį ir Susitarimą tvarkomus asmens duomenis ir jų kopijas.
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 reasonably assist the Customer and/or the third parties in auditing the processed personal data. The information that must be provided should include information about the operation of the systems used, security measures, how the data storage requirements are met, the location of the data, the transfer of data, who has the right to access the data and who are the recipients of the data, the subprocessors used, etc.	3.6. Tiekėjo grupė įsipareigoja, Užsakovo prašymu, pateikti visą informaciją, patvirtinančią su asmens duomenų tvarkymu susijusių įsipareigojimų laikymąsi, ir pagrįstai padėti Užsakovui ir (arba) trečiosioms šalims audituoti / tikrinti tvarkomus asmens duomenis. Pateikiama informacija turi apimti duomenis apie naudojamų sistemų veikimą, saugumo priemones, kaip laikomasi duomenų saugojimo reikalavimų, duomenų vietą, jų perdavimą, kas turi teisę prieiti prie duomenų ir kas yra duomenų gavėjai, pasitelktus subtvarkytojus ir pan.
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.	3.7. Šalys susitaria, kad asmens duomenys gali būti tvarkomi tik laikantis asmens duomenų apsaugos teisės aktų reikalavimų, nepažeidžiant duomenų subjektų teisių ir užtikrinant tinkamą jų įgyvendinimą bei apsaugą, kaip numatyta asmens duomenų apsaugos teisės aktuose.
Table 2	2 lentelė
[redacted]	





[redacted]

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, in accordance with General Data Protection Regulation Article 32 (1), 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. ASMENS DUOMENŲ APSAUGA, TECHNINĖS IR ORGANIZACINĖS PRIEMONĖS** 4.1. Atsižvelgdama į techninio vystymosi lygį / techninę pažangą, asmens duomenų tvarkymo pobūdį, apimtį, kontekstą ir tikslus bei į asmens duomenų tvarkymo rizikas, kurių tikimybė ir rimtumas gali skirtis atsižvelgiant į duomenų subjektų teises ir laisves, Tiekėjo grupė įsipareigoja įgyvendinti tinkamas technines ir organizacines priemones, kaip numatyta Bendrojo duomenų apsaugos reglamento 32 straipsnio 1 dalyje. Šios priemonės skirtos apsaugoti asmens duomenis nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo ar bet kokio kito neteisėto tvarkymo bei užtikrinti duomenų subjektų teisių apsaugą. Tiekėjo grupė taip pat įsipareigoja imtis visų asmens duomenų saugumo priemonių, reikalaujamų pagal galiojančius teisės aktus.
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, which must be regularly updated in response to emerging threats, technological developments, and changes in data protection legislation, necessary to achieve the purpose specified in section 2.1 of the Agreement 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	4.2. Atsižvelgiant į tai, kad Tiekėjo grupė yra savo srities profesionalė, turinti žinių ir patirties informacinių technologijų srityje, Tiekėjo grupė pati pasirenka ir nustato technines bei organizacines priemones, kurios turi būti reguliariai atnaujinamos reaguojant į atsirandančias grėsmes, technologinę plėtrą ir duomenų apsaugos teisės aktų pokyčius. Šios priemonės yra būtinos siekiant įgyvendinti Susitarimo 2.1 punkte nurodytą tikslą ir užtikrinti tinkamą saugumą; tačiau bet kuriuo atveju tokios priemonės neturi pažeisti asmens duomenų apsaugos teisės aktų reikalavimų. Nepaisant to, Užsakovas turi teisę pateikti Tiekėjo grupei pasiūlymus arba instrukcijas dėl techninių ir organizacinių saugumo priemonių taikymo. Tiekėjo grupė įsipareigoja

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.	apsvarstyti tokius Užsakovo pasiūlymus, juos įvertinti ir pateikti Užsakovui motyvuotą atsisakymą įgyvendinti Užsakovo nurodymus arba nedelsiant pradėti šių veiksmų įgyvendinimą.
4.3. Notwithstanding the provisions of sections 4.1 and 4.2 of the Agreement, 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.	4.3. Nepaisant Susitarimo 4.1 ir 4.2 punktuose nustatytų sąlygų, tais atvejais, kai Užsakovas paveda asmens duomenų tvarkymą Tiekėjo grupei, kai Paslaugų teikėjas nuotoliniu būdu jungiasi prie Užsakovo naudojamos Sistemos ir (ar) kitų informacinių sistemų, Užsakovas savo pastangomis ir lėšomis privalo užtikrinti maksimalų reikalaujamą ryšio saugumą bei taikyti būtinus ir tinkamus įrankius bei priemones (pvz., šifravimą ir kt.), siekdamas apsaugoti duomenis, jų srautą ir ryšį.
4.4. The Supplier Group shall ensure that personal data are processed only by authorized persons committed to ensure the confidentiality of the data.	4.4. Tiekėjo grupė privalo užtikrinti, kad asmens duomenis tvarkytų tik įgalioti asmenys, įsipareigoję užtikrinti duomenų konfidencialumą.
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.	4.5. Atsižvelgdama į tvarkomų asmens duomenų pobūdį ir turimą informaciją, Tiekėjo grupė įsipareigoja bendradarbiauti su Užsakovu, siekdama užtikrinti Bendrojo duomenų apsaugos reglamento 32–36 straipsniuose nustatytų įsipareigojimų laikymąsi.
4.6. The Supplier Group will reasonably assist Customer in complying with Customer's obligations in respect of data protection impact assessments (including a 'risk assessment', 'privacy impact assessment', 'data protection assessment' or any equivalent documentation) and prior consultation or mandatory submission to a data protection authority where applicable under Data Protection Laws, by e.g. providing a report, accountability information or Documentation	4.6. Tiekėjo grupė pagrįstai padės Užsakovui vykdyti įsipareigojimus, susijusius su duomenų apsaugos poveikio vertinimais (įskaitant „rizikos vertinimą“, „privatumo poveikio vertinimą“, „duomenų apsaugos vertinimą“ arba bet kokią lygiavertę dokumentaciją) ir privaloma konsultacija ar pateikimu duomenų apsaugos institucijai, jei tai taikoma pagal duomenų apsaugos teisės aktus, pvz., pateikdama ataskaitą, atskaitomybės informaciją ar dokumentaciją.
4.7. 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. If the data subject's request is sent to the Supplier Group directly, it shall be forwarded to the Customer without undue delay, but not later than within 36 hours.	4.7. Užsakovo prašymu Tiekėjo grupė, atsižvelgdama į asmens duomenų tvarkymo pobūdį ir technines galimybes, įsipareigoja pateikti turimą informaciją, būtiną Užsakovui atsakyti į duomenų subjekto prašymus įgyvendinti / naudotis duomenų subjekto teises ir vykdyti kitus asmens duomenų apsaugos teisės aktų reikalavimus. Jei duomenų subjekto prašymas tiesiogiai pateikiamas Tiekėjo grupei, jis turi būti persiųstas Užsakovui nedelsiant, bet ne vėliau kaip per 36 valandas.
5. OTHER REQUIREMENTS FOR PERSONAL AND OTHER DATA OR INFORMATION PROCESSING	**5. KITI REIKALAVIMAI ASMENS IR KITŲ DUOMENŲ AR INFORMACIJOS TVARKYMUI**
5.1. In providing the necessary infrastructure services under the Contract, the Supplier Group shall	5.1. Teikdama pagal Sutartį būtinas infrastruktūros paslaugas, Tiekėjo grupė užtikrina, kad teikiamos

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:	paslaugos atitiktų Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 5 d. nutarimu Nr. 818 patvirtintos Kibernetinio saugumo subjektams taikomų organizacinių ir techninių kibernetinio saugumo reikalavimų aprašo VI skyriaus „Reikalavimai elektroninės informacijos talpinimo paslaugų teikėjams ir skaitmeninių paslaugų teikėjams" nustatytus reikalavimus:
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.	5.1.1. Organizuoti ir atlikti rizikos vertinimą bent kartą per dvejus metus arba po reikšmingų organizacinių ar sisteminių pokyčių. Elektroninės informacijos talpinimo paslaugų ir skaitmeninių paslaugų teikėjams leidžiama šį rizikos vertinimą atlikti kartu su veiklos rizikos vertinimu ir (arba) informacinių technologijų saugumo atitikties vertinimu.
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.	5.1.2. Bendradarbiaujant su viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjais, imtis būtinų priemonių užtikrinti kibernetinį saugumą.
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.	5.1.3. Įdiegti organizacines ir technines priemones, užtikrinančias naudojamų sistemų ir įrangos, skirtos skaitmeninėms paslaugoms ar elektroninės informacijos talpinimui teikti, kibernetinį saugumą.
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. Patvirtinti kibernetinio saugumo valdymo taisykles, jas atnaujinti po reikšmingų organizacinių ar sisteminių pokyčių ir pateikti Nacionaliniam kibernetinio saugumo centrui (NKSC), jei to paprašytų NKSC. Kibernetinio saugumo valdymo taisyklėse, skirtose elektroninės informacijos talpinimui ar skaitmeninėms paslaugoms, numatyta:
5.1.4.1. Descriptions of the measures required for cyber incidents management.	5.1.4.1. Kibernetinių incidentų valdymui reikalingų priemonių aprašymai.
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.	5.1.4.2. Elektroninės informacijos talpinimo ar skaitmeninių paslaugų nepertraukiamo teikimo užtikrinimo planas, jo taikymo sąlygos bei maksimaliai leidžiamas paslaugų neveikimo laikas.
5.1.4.3. Functions and responsibilities of the persons responsible for managing cyber incidents.	5.1.4.3. Asmenų, atsakingų už kibernetinių incidentų valdymą, funkcijos ir atsakomybės.
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.	5.1.4.4. Viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikimui naudojamų sistemų ir įrangos stebėsenos, tikrinimo, testavimo ir audito tvarka bei sąlygos.
5.1.4.5. Compliance with Lithuanian and international standards for cyber security or secure electronic information processing.	5.1.4.5. Atitiktis Lietuvos ir tarptautiniams kibernetinio saugumo ar saugaus elektroninės informacijos tvarkymo standartams.
5.1.5. To inform, free of charge, the recipients of electronic information hosting or digital services about identified cyber incidents related to electronic	5.1.5. Nemokamai informuoti elektroninės informacijos talpinimo ar skaitmeninių paslaugų gavėjus apie nustatytus kibernetinius incidentus,

information hosting or digital services classified as having a significant impact, as provided in the National Cyber Incident Management Plan.	susijusius su elektroninės informacijos talpinimu ar skaitmeninėmis paslaugomis, kurie yra klasifikuojami kaip darantys reikšmingą poveikį, kaip numatyta Nacionaliniame kibernetinių incidentų valdymo plane.
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.	5.1.6. Pranešti elektroninės informacijos talpinimo ar skaitmeninių paslaugų gavėjams ir Nacionaliniam kibernetinio saugumo centrui ne vėliau kaip prieš penkias (5) darbo dienas apie planuojamus darbus, kurie gali sutrikdyti elektroninės informacijos talpinimo ar skaitmeninių paslaugų kibernetinį saugumą.
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.	5.1.7. Informuoti elektroninės informacijos talpinimo ar skaitmeninių paslaugų gavėjus, kuriose šalyse gali būti saugoma jų elektroninė informacija, kuri yra kuriama, valdoma ar pateikiama saugoti naudojant elektroninės informacijos talpinimo ar skaitmenines paslaugas, ir kokiais atvejais tokia informacija yra perduodama kitoms šalims.
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.	5.1.8. Nustatyti tvarką, kaip įspėti elektroninės informacijos talpinimo ar skaitmeninių paslaugų gavėjus apie elektroninės informacijos talpinimo ar skaitmeninių paslaugų kibernetinio saugumo pažeidimus bei kokių veiksmų tokiais atvejais turi imtis gavėjai ir (arba) paslaugų teikėjai.
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.	5.1.9. Paskelbti rekomendacijas elektroninės informacijos talpinimo ar skaitmeninių paslaugų gavėjams dėl kibernetinio saugumo užtikrinimo priemonių naudojant elektroninės informacijos talpinimo ar skaitmenines paslaugas.
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.	5.2. Tiekėjo grupė užtikrina, kad visa Užsakovo elektroninė informacija, kuri yra kuriama, tvarkoma arba pateikiama saugoti per Tiekėjo grupės paslaugas, būtų saugoma Europos Sąjungoje.
5.3. The Supplier Group may process personal data on a global basis as necessary. To the extent such global access involves a transfer made by the Supplier 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 ("Restricted Transfers"), such transfers shall be subject to the terms of the EU Standard Contractual Clauses approved by the European Commission for the Transfer of Personal Data from the Supplier to the respective (Sub-)Processors established in Third Countries including appropriate safeguards as necessary. At Customer's written request and as applicable, Supplier will provide Customer with	5.3. Tiekėjo grupė gali tvarkyti asmens duomenis pasauliniu mastu, jei to reikia. Kai tokia pasaulinė prieiga apima Tiekėjo atliekamą asmens duomenų, gautų iš Europos Sąjungos ir (arba) Europos ekonominės erdvės (EEE), perdavimą Tiekėjo grupei ar jos Subtvarkytojams, esantiems šalyse už Europos Sąjungos ir (arba) EEE ribų, kurios nėra gavusios privalomo Europos Komisijos sprendimo dėl tinkamumo („Riboti perdavimai"), tokie perdavimai yra vykdomi pagal ES Standartines sutarties sąlygas, patvirtintas Europos Komisijos, skirtas asmens duomenų perdavimui iš Tiekėjo atitinkamiems (Sub-)Tvarkytojams, įsisteigusiems trečiosiose šalyse, įskaitant tinkamas apsaugos priemones, jei reikia. Užsakovo rašytiniu prašymu ir, jei taikytina, Tiekėjas pateiks Užsakovui dokumentus, patvirtinančius

documentation evidencing compliance of Restricted Transfers, e.g. a summary so that Customer can reasonably verify Supplier's compliance with the data security and data protection obligations under this Agreement.	Ribotų perdavimų atitiktį, pvz., santrauką, kad Užsakovas galėtų pagrįstai įsitikinti Tiekėjo laikymusi duomenų saugumo ir duomenų apsaugos įsipareigojimų pagal šį Susitarimą.
6. PERSONAL DATA BREACH	**6. ASMENS DUOMENŲ SAUGUMO PAŽEIDIMAS**
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, that is required by General Data Protection Regulation Article 33 (3), and data related to such breach.	6.1. Asmens duomenų saugumo pažeidimo atveju arba jei Tiekėjo grupė pagrįstai įtaria tokį pažeidimą, Tiekėjo grupė nedelsdama, tačiau bet kuriuo atveju ne vėliau kaip per 24 valandas po sužinojimo apie saugumo pažeidimą, raštu informuoja Užsakovą ir pateikia turimą informaciją, kurios reikalauja Bendrasis duomenų apsaugos reglamento (BDAR) 33 straipsnio 3 dalis, bei su tuo pažeidimu susijusius duomenis.
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. This includes assistance with communications to data subjects if required under General Data Protection Regulation Article 34.	6.2. Užsakovo prašymu, atsižvelgdama į technines galimybes ir nedelsdama, Tiekėjo grupė pateiks Užsakovui reikiamus papildomus dokumentus, informaciją ir duomenis, kurie būtini Užsakovui identifikuoti ir (arba) patikrinti asmens duomenų saugumo pažeidimo faktą, ištirti aplinkybes ir imtis skubių priemonių pažeidimui pašalinti arba sumažinti jo neigiamas pasekmes. Tai apima pagalbą bendraujant su duomenų subjektais, jei to reikalaujama pagal Bendrojo duomenų apsaugos reglamento 34 straipsnį.
7. RESPONSIBILITY OF THE SUPPLIER GROUP AND DISPUTE RESOLUTION	**7. TIEKĖJO GRUPĖS ATSAKOMYBĖ IR GINČŲ SPRENDIMAS**
7.1. In the event of liability arising from performance by a Party under this Agreement, the Parties agree that the maximum liability of either Party to the other Party including its affiliates shall not exceed the greater of (i) per claim, an amount equal to the net remuneration paid or to be paid by the Customer for the Services in the contractual year in which the damage occurs and (ii) an aggregate amount up to a maximum of 10 million Euro (in words: ten million Euro) for the duration of the Agreement. This liability restrictions shall not apply to applicable mandatory statutory liability provisions which cannot be derogated from the agreement.	7.1. Atsiradus atsakomybei, susijusiai su Šalies vykdymu pagal šį Susitarimą, Šalys susitaria, kad maksimali bet kurios Šalies atsakomybė kitai Šaliai, įskaitant jos filialus, neviršys didesnės iš šių sumų: (i) už kiekvieną pretenziją – sumos, lygiavertės grynajam atlygiui, Užsakovo sumokėtam arba mokėtinam už paslaugas sutartiniais metais, kuriais atsirado žala, ir (ii) bendros sumos, neviršijančios 10 milijonų eurų (žodžiais: dešimt milijonų eurų) per visą Susitarimo galiojimo laikotarpį. Šie atsakomybės apribojimai netaikomi privalomoms įstatyminėms atsakomybės nuostatoms, nuo kurių negali būti nukrypstama susitarimu.
7.2. Any dispute, disagreement or claim arising out of or relating to this Agreement 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	7.2. Bet koks ginčas, nesutarimas ar pretenzija, kylanti iš šio Susitarimo prie Sutarties arba susijusi su jo pažeidimu, bus sprendžiama derybų būdu. Jei klausimas negali būti išspręstas derybose per 15 dienų nuo ginčo pradžios, toks ginčas, nesutarimas ar

dispute, disagreement or claim will be settled by the court of the Republic of Lithuania.	pretenzija bus sprendžiamas Lietuvos Respublikos teisme.

CUSTOMER
State Data Agency (Statistics Lithuania)
Gedimino Ave. 29, LT-01500 Vilnius, Lithuania
Company code: 188600177
VAT number: none
Settlement Account No: LT02 4040 0636 1000 0121
The Ministry of Finance of the Republic of Lithuania
Code of financial institution: 40400
Tel.: +370 656 97121
E-mail: statistika@stat.gov.lt
http://www.vda.lrv.lt
Jūratė Petrauskienė, Director General

[redacted]

UŽSAKOVAS
Valstybės duomenų agentūra
Gedimino pr. 29, LT-01500 Vilnius, Lietuva
Juridinio asmens kodas: 188600177
PVM mokėtojo kodas: nėra
Atsiskaitomoji sąskaita: LT02 4040 0636 1000 0121
Lietuvos Respublikos finansų ministerija
Finansų įsaigos kodas: 40400
Tel.: +370 656 97121
El. paštas: statistika@stat.gov.lt
http://www.vda.lrv.lt
Generalinė direktorė Jūratė Petrauskienė

[redacted]

SUPPLIER
Palantir Technologies Lithuania, UAB
Upės g. 23-1 LT-08128, Vilnius
Company number: 306032659
VAT number: LT1000 1508 0417
Bank Name: Citibank Europe plc
Account Holder: Palantir Technologies Lithuania UAB
Account Number: 0039560283
IBAN: E26CITI99005139560283
SWIFT: CITIIE2X
Phone No. +370 604 19 041
E-mail: legalnotices@palantir.com
Tadas Rudzevičius, director

[redacted]

TIEKĖJAS
Palantir Technologies Lithuania, UAB
Upės g. 23-1 LT-08128, Vilnius
Juridinio asmens kodas: 306032659
PVM mokėtoje kodas: LT1000 1508 0417
Bankas: Citibank Europe plc
Sąskaitos pavadinimas: Palantir Technologies Lithuania UAB
Sąskaitos numeris: 0039560283
IBAN: E26CITI99005139560283
SWIFT kodas: CITIIE2X
Tel. +370 604 19 041
El. paštas: legalnotices@palantir.com
Direktorius Tadas Rudzevičius

[redacted]