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

3 priedas

ASMENS DUOMENŲ TVARKYMO SĄLYGOS

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

Annex 3

CLAUSES FOR PERSONAL DATA PROCESSING

I SKYRIUS
SĄLYGŲ TIKSLAS

1. Teikdama Palantir Foundry licencijos išplėtimo papildomais infrastruktūros ištekliais pirkimo sutartyje (toliau – Sutartis) numatytas paslaugas, **Palantir Technologies UK, Ltd.** (toliau – **duomenų tvarkytojas**) tvarkys asmens duomenis **Valstybės duomenų agentūros** (toliau – **duomenų valdytojas**) vardu pagal šias Asmens duomenų tvarkymo sąlygas (toliau – Sąlygos).

2. Sąlygomis įgyvendinami 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 (Bendrojo duomenų apsaugos reglamento) (toliau – Reglamentas (ES) 2016/679) 28 straipsnio 3 dalies reikalavimai, nustatomos duomenų valdytojo ir duomenų tvarkytojo teisės bei pareigos, duomenų valdytojo vardu tvarkant asmens duomenis. Sąlygomis siekiama apsaugoti duomenų subjektų teises, mažinti konkrečią asmens duomenų apsaugos riziką ir užtikrinti duomenų valdytojo ir duomenų tvarkytojo santykių bei atitinkamų teisių ir pareigų aiškumą.

II SKYRIUS
ŠALIŲ ĮSIPAREIGOJIMAI

3. Duomenų valdytojas:

3.1. įsipareigoja užtikrinti, kad asmens duomenys būtų tvarkomi laikantis Reglamento (ES) 2016/679, kitų asmens duomenų apsaugą ir (ar) tvarkymą reglamentuojančių Europos Sąjungos ar Lietuvos Respublikos teisės aktų ir šių Sąlygų;

3.2. turi teisę ir pareigą priimti sprendimus dėl asmens duomenų tvarkymo tikslų ir priemonių;

3.3. yra atsakingas, įskaitant, bet neapsiribojant, už tai, kad asmens duomenų tvarkymas, kurį duomenų tvarkytojui pavesta atlikti, turėtų teisinį pagrindą.

4. Duomenų tvarkytojas įsipareigoja:

4.1. tvarkyti asmens duomenis tik pagal duomenų valdytojo pateiktus dokumentais įformintus nurodymus, išskyrus atvejus, kai to reikalaujama pagal Europos Sąjungos ar Lietuvos Respublikos teisės aktus, kurie yra taikomi duomenų tvarkytojui (tokiais atvejais duomenų tvarkytojas informuoja duomenų valdytoją apie šiuos reikalavimus, išskyrus atvejus, kai teisės aktai draudžiama minėtą informaciją pateikti dėl svarbaus viešojo intereso). Tokie nurodymai pateikti Sąlygų 1 ir 2 prieduose. Duomenų valdytojas taip pat gali pateikti tolesnius nurodymus viso asmens duomenų tvarkymo metu, tačiau tokie su Sąlygomis susiję nurodymai visada turi būti pagrįsti dokumentais;

4.2. nedelsiant informuoti duomenų valdytoją, jei duomenų valdytojo nurodymai, duomenų tvarkytojo nuomone, prieštarauja Reglamentui (ES) 2016/679 arba kitiems asmens duomenų apsaugą reglamentuojantiems Europos Sąjungos ar Lietuvos Respublikos teisės aktams;

4.3. tvarkyti su asmens duomenų tvarkymo veikla, vykdoma duomenų valdytojo vardu, susijusius įrašus. Ši pareiga taikoma kiekvienam duomenų tvarkytojui ir, kai taikoma, duomenų tvarkytojo atstovui pagal Reglamento (ES) 2016/679 30 straipsnio 2 dalį.

5. Atsakomybė už duomenų valdytojo nurodymus, prieštaraujančius Reglamentui (ES) 2016/679 arba kitiems asmens duomenų apsaugą reglamentuojantiems Europos Sąjungos ar Lietuvos Respublikos teisės aktams, kuriuos duomenų valdytojas reikalavo vykdyti nepaisant Sąlygų 4.2 papunktyje nustatyta tvarka duomenų tvarkytojo pateiktos duomenų valdytojui informacijos apie duomenų valdytojo pateiktų nurodymų prieštaravimą Reglamentui (ES) 2016/679 arba kitiems asmens duomenų apsaugą reglamentuojantiems Europos Sąjungos ar Lietuvos Respublikos teisės aktams, ir dėl šių duomenų valdytojo nurodymų vykdymo kilusias pasekmes tenka duomenų valdytojui.

6. Šios Sąlygos neatleidžia Šalių nuo kitų pareigų, kurios joms taikomos pagal Reglamentą (ES) 2016/679 ar kitus teisės aktus.

CHAPTER I
PURPOSE OF THE CLAUSES

1. By providing the services provided in the Purchase Contract for the extension of the Palantir Foundry license with additional infrastructure resources (hereinafter referred to as the "Contract"), **Palantir Technologies UK, Ltd.** (hereinafter referred to as the "**Data Processor**") will process personal data on behalf of the **State Data Agency** (hereinafter referred to as the "**Data Controller**"), in accordance with these Clauses for Data Processing (hereinafter referred to as the "Clauses").

2. The Clauses implement the requirements of Article 28(3) 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) (hereinafter referred to as "Regulation (EU) 2016/679), and set out the rights and obligations of the Data Controller and the Data Processor in processing of personal data on behalf of the Data Controller. The Clauses shall be aimed at protecting the rights of the data subjects, minimising the specific risks with respect to protection of personal data and ensure the clarity of the relationship between the Data Controller and the Data Processor and the respective rights and obligations of the Data Controller and the Data Processor.

CHAPTER II
OBLIGATIONS OF THE PARTIES

3. The Data Controller:

3.1. is responsible for ensuring that personal data is processed in accordance with Regulation (EU) 2016/679, other European Union or the Republic of Lithuania law governing protection and/or processing of personal data and these Clauses;

3.2. has the right and obligation to make decisions on the purposes and means of processing of personal data;

3.3. shall be responsible, among other, for ensuring that processing of personal data which is assigned to the Data Processor has legal grounds.

4. The Data Processor:

4.1. processes personal data only in accordance with the documented instructions issued by the Data Controller, except for the cases where this is required by the European Union or Member State law applicable to the Data Processor (in such cases, the Data Processor shall inform the Data Controller of the legal requirement before processing, unless that law prohibits such information for reasons of substantial public interest). Such instructions shall be set out in Annex 1 and Annex 2 to the Clauses. The Data Controller shall also be entitled to issue further instructions during the entire period of the processing of personal data; however, such instructions related to the Clauses must always be documented;

4.2. shall immediately notify the Data Controller if, in the opinion of the Data Processor, the Data Controller's instructions are in conflict with Regulation (EU) 2016/679 or other European Union or the Republic of Lithuania law governing protection of personal data;

4.3. shall maintain records related to the activities of processing of personal data carried out on behalf of the Data Controller. The aforementioned obligation shall apply to each Data Processor and, where applicable, the representative of the Data Processor in accordance with Article 30(2) of Regulation (EU) 2016/679.

5. The liability for the Data Controller's instructions that are in conflict with Regulation (EU) 2016/679 or other legal acts of the European Union or the Republic of Lithuania that regulate the governing protection of personal data, which the Data Controller required to implement in spite of the information on contradiction of the Data Controller's instructions with Regulation (EU) 2016/679 or other European Union or the Republic of Lithuania law governing protection of personal data provided by the Data Processor to the Data Controller in accordance with the procedure laid down in Subparagraph 4.2 of the Clauses, as well as for the consequences of the execution of such instructions of the Data Controller, shall be borne by the Data Controller.

6. These Clauses shall not release the Parties from other obligations applicable to them under Regulation (EU) 2016/679 or other legal acts.

III SKYRIUS
KONFIDENCIALUMAS

7. Duomenų tvarkytojas prieigą prie duomenų valdytojo vardu tvarkomų asmens duomenų suteikia tik tiems asmenims, kuriems vadovauja duomenų tvarkytojas, ir kurie yra įpareigoti laikytis konfidencialumo arba kuriems taikoma teisinė konfidencialumo pareiga, ir tik tuo atveju, jei jiems būtina su jais susipažinti. Šalys užtikrina, kad:

7.1. Pasikeitus asmenims, kurie tvarko asmens duomenis, jų prieigos teisės prie duomenų valdytojo asmens duomenų panaikinamos ne vėliau nei paskutinę jo užduočių, dėl kurių jiems būtina prieiga prie duomenų valdytojo asmens duomenų, patikėtų tvarkyti duomenų tvarkytojui, dieną, o tuo atveju jei nutrūksta duomenų tvarkytojo darbuotojo darbo santykiai – ne vėliau nei paskutinę jo darbo dieną.

7.2. Asmenų, kuriems suteikta prieiga prie asmens duomenų, sąrašas turi būti periodiškai peržiūrimas ne rečiau kaip kartą kas tris mėnesius. Vadovaujantis šia peržiūra, tokia prieiga prie asmens duomenų panaikinama, jei tokia prieiga nebereikalinga, todėl asmens duomenys nebegalės būti prieinami tiems asmenims.

8. Duomenų tvarkytojas duomenų valdytojo prašymu įrodo, kad asmenims, kuriems vadovauja duomenų tvarkytojas ir kuriems pavesta tvarkyti asmens duomenis, taikoma Sąlygų 7 punkte nurodyta konfidencialumo pareiga. Šie įrodymai duomenų valdytojui teikiami neatlygintinai.

IV SKYRIUS
DUOMENŲ TVARKYMO SAUGUMAS

9. Vadovaujantis Reglamento (ES) 2016/679 32 straipsniu, duomenų valdytojas ir duomenų tvarkytojas įgyvendina tinkamas technines ir organizacines priemones, kad būtų užtikrintas pavojų atitinkančio lygio saugumas, atsižvelgiant į techninių galimybių išsivystymo lygį, įgyvendinimo sąnaudas bei duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus, taip pat duomenų tvarkymo keliamus įvairios tikimybės ir rimtumo pavojus fizinių asmenų teisėms ir laisvėms.

10. Duomenų valdytojas įvertina fizinių asmenų teisėms ir laisvėms galinčią kilti riziką tvarkant asmens duomenis ir įgyvendina priemones šiai rizikai sumažinti. Priklausomai nuo jų tinkamumo, priemonės gali būti šios:

10.1. asmens duomenų pseudonimizavimas ir (ar) šifravimas;

10.2. galimybė užtikrinti nuolatinį duomenų tvarkymo sistemų ir paslaugų konfidencialumą, vientisumą, prieinamumą ir atsparumą;

10.3. galimybė laiku atkurti prieinamumą ir prieigą prie asmens duomenų, įvykus fiziniam ar techniniam incidentui;

10.4. techninių ir organizacinių priemonių, užtikrinančių duomenų tvarkymo saugumą, reguliaraus testavimo, tikrinimo ir įvertinimo procesas.

11. Pagal Reglamento (ES) 2016/679 32 straipsnį duomenų tvarkytojas, nepriklausomai nuo duomenų valdytojo, taip pat įvertina duomenų tvarkymo riziką, susijusią su asmens duomenų tvarkymo veikla, kuriai atlikti duomenų valdytojas pasitelkė duomenų tvarkytoją, galinčią kilti fizinių asmenų teisėms ir laisvėms, ir įgyvendina priemones šiai rizikai sumažinti. Šiuo tikslu duomenų valdytojas duomenų tvarkytojui pateikia visą informaciją, reikalingą tokiai rizikai nustatyti ir įvertinti.

12. Be to, duomenų tvarkytojas padeda duomenų valdytojui užtikrinti duomenų valdytojo pareigų pagal Reglamento (ES) 2016/679 32 straipsnį vykdymą, teikdamas *inter alia* duomenų valdytojui informaciją apie technines ir organizacines priemones, kurias duomenų tvarkytojas jau įgyvendino pagal Reglamento (ES) 2016/679 32 straipsnį kartu su visa kita informacija, reikalinga duomenų valdytojui įvykdyti duomenų valdytojo pareigas pagal Reglamento (ES) 2016/679 32 straipsnį.

13. Jei, atsižvelgiant į duomenų valdytojo atliktą vertinimą, nustatytai rizikai sumažinti duomenų tvarkytojas turi įgyvendinti papildomas priemones, duomenų valdytojas šias priemones nurodo Sąlygų 2 priede, o duomenų tvarkytojas savo sąskaita turi įgyvendinti papildomas priemones ir tas, kurias jau įgyvendino pagal Reglamento (ES) 2016/679 32 straipsnį. Duomenų tvarkytojas turi duomenų valdytojui suteikti visą informaciją, kuri būtina siekiant įrodyti Sąlygų IV ir X skyriuose nustatytų duomenų tvarkytojo pareigų vykdymą. Ši informacija duomenų valdytojui teikiama neatlygintinai.

CHAPTER III
CONFIDENTIALITY

7. The Data Processor shall grant access to the personal data processed on behalf of the Data Controller only to the persons under the Data Processor's authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and only on a need-to-know basis. The Parties shall ensure that:

7.1. In case of a need to change in the persons having access to personal data, their right of access to the Data Controller's personal data shall be revoked not later than on the last day on which their tasks require them to have access to the personal data of the Data Controller entrusted to Data Processor. In case of discontinuation of employment relationship with the employee of the Data Processor, the access rights to the Data Controller's personal data shall be revoked not later than on the last day of work.

7.2. The list of persons granted access to personal data shall be reviewed on a periodical basis at least every 3 months. Following the afore-mentioned review, such access to personal data shall be suspended if such access is no longer necessary; thus, personal data cannot be accessible to such persons.

8. Upon the Data Controller's request, the Data Processor shall demonstrate that the persons who are supervised by the Data Processor and to whom processing of personal data is assigned are subject to the obligation of confidentiality provided for in Paragraph 7 hereof. This demonstration shall be provided to the Data Controller free of charge.

CHAPTER IV
SECURITY OF PROCESSING

9. Following Article 32 of Regulation (EU) 2016/679, the Data Controller and the Data Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

10. The Data Controller shall assess possible risk to the rights and freedoms of natural persons in processing of personal data and implement measures to minimise such risk. Depending on the appropriateness of the measures, they may be as follows:

10.1. the pseudonymisation and/or encryption of personal data;

10.2. the ability to ensure the continues confidentiality, integrity, availability and resilience of processing systems and services;

10.3. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

10.4. a process for regular testing, inspecting and evaluating the technical and organisational measures for ensuring the security of the processing.

11. According to Article 32 of Regulation (EU) 2016/679, the Data Processor shall also – independently from the Data Controller – evaluate the risks to the rights and freedoms of natural persons inherent in the processing activity entrusted to it by the Data Controller, and implement the measures to mitigate those risk. To this end, the Data Controller shall provide the Data Processor with all information necessary for identification and assessment of such risk.

12. Furthermore, the Data Processor shall help the Data Controller in ensuring compliance with the Data Controller's obligation provided for in Article 32 of Regulation (EU) 2016/679 inter alia providing the Data Controller with information on technical and organisational measures which have already been implemented by the Data Processor under Article 32 of Regulation (EU) 2016/679 together with all other information necessary for the Data controller to comply with its obligation under Article 32 of Regulation (EU) 2016/679.

13. If, according to the assessment made by the Data Controller, the mitigation of the identified risks requires further measures to be implemented by the Data Processor, the Data Controller shall specify these additional measures in Annex 2 hereto, and the Data Processor shall implement, at its own expense, the additional measures and the measures which have already been implemented under Article 32 of Regulation (EU) 2016/679. The Data Processor shall make available to the Data Controller all information necessary to demonstrate compliance with obligations of the Data Processor as provided for in Chapters IV and X of the Clauses. This information shall be provided to the Data Controller free of charge.

V SKYRIUS
KITŲ DUOMENŲ TVARKYTOJŲ PASITELKIMAS

14. Duomenų tvarkytojas turi laikytis Reglamento (ES) 2016/679 28 straipsnio 2 ir 4 dalyse nurodytus reikalavimus, kad galėtų pasitelkti kitą duomenų tvarkytoją (toliau – pagalbinis duomenų tvarkytojas).

15. Duomenų valdytojas leidžia duomenų tvarkytojui Sąlygų 1 priedo 1 punkte nurodytais tikslais pasitelkti šiame punkte nurodytus pagalbinius duomenų tvarkytojus. Siekiant pasitelkti minėtus pagalbinius duomenų tvarkytojus asmens duomenų tvarkymui kitais tikslais nei tikslai, nustatyti Sąlygų 1 priedo 1 punkte, būtinas rašytinis duomenų valdytojo leidimas.

Eil. Nr.	Pavadinimas, vardas, pavardė	Įmonės kodas / individualios veiklos pažymėjimo numeris arba verslo liudijimo numeris	Buveinės adresas / gyvenamosios vietos adresas	Asmens duomenų tvarkymo aprašymas
1.	Nurodykite pasitelktą pagalbinį duomenų tvarkytoją			

16. Duomenų tvarkytojas pasitelkia pagalbinį duomenų tvarkytoją tik pagal šias Sąlygas gavęs specialų išankstinį duomenų valdytojo leidimą. Duomenų tvarkytojas turi raštu pateikti prašymą dėl specialaus leidimo pasitelkti pagalbinį duomenų tvarkytoją bent jau trisdešimt dienų iki numatomos atitinkamo pagalbinio duomenų tvarkytojo pasitelkimo dienos. Duomenų valdytojas per dvidešimt dienų nuo duomenų tvarkytojo prašymo gavimo dienos raštu praneša duomenų tvarkytojui, ar leidžiama pasitelkti prašyme nurodytą pagalbinį duomenų tvarkytoją.

17. Kai duomenų tvarkytojas konkrečiai duomenų tvarkymo veiklai duomenų valdytojo vardu atlikti pasitelkia pagalbinį duomenų tvarkytoją, sutartimi ar kitu teisės aktu pagal Europos Sąjungos ar Lietuvos Respublikos teisę, tam pagalbiniam duomenų tvarkytojui nustatomos tos pačios duomenų apsaugos prievolės, kaip ir prievolės, nustatytos Sąlygose ar kitame teisės akte, visų pirma prievolė pakankamai užtikrinti, kad tinkamos techninės ir organizacinės priemonės bus įgyvendintos tokiu būdu, kad duomenų tvarkymas atitiktų Sąlygų ir Reglamento (ES) 2016/679 reikalavimus. Prieš pradėdamas tvarkyti asmens duomenis, duomenų tvarkytojas informuoja pagalbinį duomenų tvarkytoją apie tai, kurio duomenų valdytojo asmens duomenų tvarkymui jis yra pasitelkiamas, nurodydamas duomenų valdytojo tapatybę ir kontaktinius duomenis.

18. Sąlygų su pagalbiniu duomenų tvarkytoju kopija ir jos vėlesni pakeitimai, duomenų valdytojo prašymu, pateikiami duomenų valdytojui, tokiu būdu suteikiant duomenų valdytojui galimybę užtikrinti, kad pagalbiniam duomenų tvarkytojui taikomos tos pačios duomenų apsaugos prievolės, kaip yra nustatyta Sąlygose. Duomenų tvarkytojas turi informuoti duomenų valdytoją apie visus netinkamo pagalbinio duomenų tvarkytojo pareigų, nustatytų tokia sutartimi ar kitu teisės aktu, atvejus. Duomenų valdytojui nėra privaloma pateikti asmens duomenų tvarkymo sutarties dėl su verslu susijusių nuostatų, kurios nedaro įtakos su pagalbiniu duomenų tvarkytoju sudarytos sutarties teisinėms asmens duomenų apsaugos sąlygoms.

19. Duomenų tvarkytojas turi susitarti su pagalbiniu duomenų tvarkytoju, jei toks pasitelkiamas, kad duomenų tvarkytojo bankroto atveju, duomenų valdytojas turi teisę tęsti duomenų tvarkymo santykius su duomenų tvarkytojo pasitelktu pagalbiniu duomenų tvarkytoju tiesiogiai ir (arba) teikti tiesioginius nurodymus dėl duomenų tvarkymo, pavyzdžiui, nurodyti pagalbiniam duomenų valdytojui ištrinti arba grąžinti asmens duomenis.

20. Duomenų tvarkytojas yra atsakingas už reikalavimą, kad pagalbinis duomenų tvarkytojas laikytųsi bent tų pareigų, kurios duomenų tvarkytojui taikomos pagal Sąlygas ir Reglamentą (ES) 2016/679. Jei pagalbinis duomenų tvarkytojas nevykdo asmens duomenų apsaugos prievolių, duomenų tvarkytojas išlieka visiškai atsakingas duomenų valdytojui už pagalbinio duomenų tvarkytojo prievolių vykdymą. Tai nedaro įtakos duomenų subjektų teisėms pagal Reglamentą (ES) 2016/679, ypač Reglamento (ES) 2016/679 79 ir 82 straipsniuose numatytoms teisėms, duomenų valdytojo ir duomenų tvarkytojo, įskaitant pagalbinius duomenų tvarkytojus, atžvilgiu.

CHAPTER V
ENGAGEMENT OF OTHER DATA PROCESSORS

14. The Data Processor shall comply with the requirements set forth in Articles 28(2) and 28(4) of Regulation (EU) 2016/679 in order to engage another data processor (hereinafter referred to as the "Sub-processor").

15. The Data Controller shall allow the Data Processor to engage the Sub-processors referred to in this Paragraph for the purposes set out in Paragraph 1 of Annex 1 to the Clauses. The engagement of the aforementioned Sub-processors for the processing of personal data for purposes other than those set out in Paragraph 1 of Annex 1 to the Clauses shall be subject to the written authorisation of the Data Controller.

Se-quence No.	Title, name, surname	Company code / Individual activity certificate number / Business license number	Registered office address / Address of place of residence	Description of personal data processing
1.	Specify the engaged Sub-processor			

16. The Data Processor shall engage the Sub-processor only upon receipt of a prior special written authorisation of the Data Controller in accordance with these Clauses. The Data Processor shall submit a written request for special authorisation for engagement of the Sub-processor at least 30 days before the date of engagement of the respective Sub-processor. The Data Controller shall notify the Data Processor in writing, within twenty days of receipt of the Data Processor's request, whether it is permitted to engage the Sub-processor specified in the request.

17. Where the Data Processor engages the Sub-processor for carrying out the particular processing on behalf of the Data Controller, the same data protection obligations as set out between the Data Controller and the Data Processor shall be imposed on the Sub-processor by way of a contract or another legal act under European Union or the Republic of Lithuania law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures so that processing meets the requirements of Regulation (EU) 2016/679. Prior to personal data processing, the Data Processor shall inform the Sub-processor of the identity and contact details of the Data Controller for which the Sub-processor processes personal data.

18. Upon request of the Data Controller, a copy of the contract with the Sub-processor and subsequent amendments thereto shall be provided to the Data Controller, thus enabling the Data Controller to ensure that the Sub-processor is subject to the same data protection obligations as laid down by the Clauses. The Data Processor shall notify the Data Controller of any failure by the Sub-processor to fulfil its obligations under that contract or other legal act binding on Sub-processor. The Data Processor shall not be obliged to provide the provisions of the data processing agreement on the business-related issues which do not have an impact on the terms and conditions of the legal protection of personal data of the contract concluded with the Sub-processor.

19. The Data Processor shall agree on a third-party beneficiary clause with the Sub-processor (if any) providing that in case of bankruptcy of the primary Data Processor, the Data Controller shall be entitled to enforce the data processing agreement directly against the Sub-processor engaged by the primary Data Processor and/or issue direct instructions on processing, for example, instruct the Sub-processor to delete or return personal data.

20. The Data Processor shall be responsible for requiring that the Sub-processor at least complies with the obligations to which the Data Processor is subject pursuant to the Clauses and Regulation (EU) 2016/679. If the Sub-processor fails to fulfil the personal data protection obligations, the Data Processor shall remain fully liable towards the Data Controller for fulfilment of the Sub-processor's obligations. This shall not affect the data subjects' rights provided for in Regulation (EU) 2016/679, in particular, the rights provided for in Articles 79 and 82 of Regulation (EU) 2016/679 in respect of the Data Controller and the Data Processor, including the rights in respect of the Sub-processors.

VI SKYRIUS
DUOMENŲ PERDAVIMAS Į TREČIĄSIAS VALSTYBES ARBA TARPTAUTINĖMS ORGANIZACIJOMS

21. Duomenų tvarkytojas asmens duomenis gali perduoti į valstybes ne Europos Ekonominės Erdvės teritorijoje (toliau – trečiosios valstybės) ar tarptautinėms organizacijoms tik gavęs duomenų valdytojo dokumentais įformintus nurodymus ir laikantis Reglamento (ES) 2016/679 V skyriaus reikalavimų.

22. Jei asmens duomenis trečiosioms valstybėms ar tarptautinėms organizacijoms reikia perduoti pagal Europos Sąjungos ar Lietuvos Respublikos teisės aktus, kurių turi laikytis duomenų tvarkytojas, nors duomenų valdytojas nedavė nurodymų duomenų tvarkytojui tai atlikti, duomenų tvarkytojas informuoja duomenų valdytoją apie šį teisinį reikalavimą prieš duomenų perdavimą, nebent tas teisės aktas draudžia perduoti tokią informaciją.

23. Duomenų tvarkytojas be duomenų valdytojo dokumentais įformintų nurodymų arba be konkretaus reikalavimo pagal Europos Sąjungos ar Lietuvos Respublikos teisės aktus negali pagal šias Sąlygas:

23.1. perduoti asmens duomenis duomenų valdytojui ar duomenų tvarkytojui trečiojoje valstybėje ar tarptautinėje organizacijoje;

23.2. perduoti asmens duomenų tvarkymą pagalbiniam duomenų tvarkytojui trečiojoje valstybėje;

23.3. leisti, kad asmens duomenis tvarkytų duomenų tvarkytojas trečiojoje valstybėje.

24. Duomenų valdytojo nurodymai ar leidimai dėl asmens duomenų perdavimo į trečiąją valstybę, įskaitant, jei taikoma, asmens duomenų perdavimo į trečiąsias valstybes Reglamento (ES) 2016/679 V skyriuje nustatytus pagrindai, kuriais duomenų valdytojo nurodymai yra grindžiami, pateikiami Sąlygų 2 priede.

25. Šios Sąlygos nėra standartinės duomenų apsaugos sąlygos, apibrėžtos Reglamento (ES) 2016/679 46 straipsnio 2 dalies c ir d punktuose, ir šalys negali remtis Sąlygomis kaip asmens duomenų perdavimo į trečiąsias valstybes ar tarptautinėms organizacijoms pagrindu pagal Reglamento (ES) 2016/679 V skyrių.

VII SKYRIUS
PAGALBA DUOMENŲ VALDYTOJUI

26. Atsižvelgdamas į duomenų tvarkymo pobūdį, duomenų tvarkytojas, kiek tai įmanoma, padeda duomenų valdytojui tinkamomis techninėmis ir organizacinėmis priemonėmis įvykdyti duomenų valdytojo prievoles atsakyti į prašymus naudotis duomenų subjekto teisėmis, nustatytomis Reglamento (ES) 2016/679 III skyriuje. Tai reiškia, kad duomenų tvarkytojas, kiek tai įmanoma, padeda duomenų valdytojui, kad duomenų valdytojas įgyvendintų:

26.1. teisę būti informuotam renkant asmens duomenis iš duomenų subjekto;

26.2. teisę būti informuotam, kai asmens duomenys yra gauti ne iš duomenų subjekto;

26.3. teisę susipažinti su duomenimis;

26.4. teisę reikalauti ištaisyti duomenis;

26.5. teisę reikalauti ištrinti duomenis („teisę būti pamirštam“);

26.6. teisę apriboti duomenų tvarkymą;

26.7. prievolę pranešti apie asmens duomenų ištaisymą ar ištrynimą arba duomenų tvarkymo apribojimą;

26.8. teisę į duomenų perkeliamumą;

26.9. teisę nesutikti su duomenų tvarkymu;

26.10. teisę, kad nebūtų taikomi sprendimai, pagrįsti vien automatiniu tvarkymu, įskaitant profiliavimą.

27. Be duomenų tvarkytojo prievolės padėti duomenų valdytojui pagal Sąlygų 12 punktą, duomenų tvarkytojas, atsižvelgdamas į tvarkymo pobūdį ir duomenų tvarkytojui prieinamą informaciją, taip pat padeda duomenų valdytojui užtikrinti:

CHAPTER VI
TRANSFER OF DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS

21. The Data Processor shall be entitled to transfer personal data to countries outside the European Economic Area (hereinafter referred to as “third countries”) or international organisations only after receipt of the documented instructions of the Data Controller and in accordance with the requirements of Chapter V of Regulation (EU) 2016/679.

22. If personal data must be transferred to third countries or international organisations in accordance with European Union or the Republic of Lithuania law which must be complied with by the Data Processor although the Data Controller has not given instructions to do this to the Data Processor, the Data Processor shall notify the Data Controller of the aforementioned legal requirement prior to transfer of data, unless such legal act prohibits communication of such information.

23. The Data Processor shall not be entitled to carry out the following actions without the documented instructions of the Data Controller or the particular request under European Union or the Republic of Lithuania law in accordance with these Clauses:

23.1. to transfer personal data to a data controller or a data processor in a third country or in an international organisation;

23.2. to transfer processing of personal data to a sub-processor in a third country;

23.3. to allow a data processor to process personal data in a third country.

24. The Data Controller’s instructions or approval regarding transfers of personal data to a third country including, if applicable, the transfer tool under Chapter V of Regulation (EU) 2016/679 on which the Data Controller’s instructions are based, shall be set out in Annex 2 of these Clauses.

25. These Clauses shall not be standard data protection clauses defined in Articles 46(2)(c) and 46(2)(d) of Regulation (EU) 2016/679 and the Parties shall not be entitled to rely on the Clauses as the basis of transfer of personal data to third countries or international organisations in accordance with Chapter V of Regulation (EU) 2016/679.

CHAPTER VII.
ASSISTANCE TO THE DATA CONTROLLER

26. Taking into account the nature of processing, the Data Processor shall assist the Data Controller to fulfil the Data Controller’s obligation to respond to the requests for exercise of the data subject’s rights provided for in Chapter III of Regulation (EU) 2016/679 by appropriate technical and organisational measures, insofar as this is possible. This implies that the Data Processor shall, insofar as this is possible, assist the Data Controller in its obligation to give effect to the following data subject rights:

26.1. the right to be informed when personal data have been obtained from the data subject;

26.2. the right to be informed when personal data have been obtained not from the data subject;

26.3. the data subject’s right to access data;

26.4. the right to rectification;

26.5. the right to erasure (“right to be forgotten”);

26.6. the right to restriction of processing;

26.7. the notification obligation regarding rectification or erasure of personal data or restriction of processing;

26.8. the right to data portability;

26.9. the right to object to processing;

26.10. the right not to be subject to decisions based solely on automated processing, including profiling.

27. In addition to the Data Processor’s obligation to assist the Data Controller in accordance with Paragraph 12 hereof, the Data Processor, taking into account the nature of processing and information available to the Data Processor, shall also assist the Data Controller in ensuring compliance with:

27.1. duomenų valdytojo pareigą nedelsiant ir, jei įmanoma, ne vėliau kaip per 72 valandas po to, kai apie tai sužinojo, pranešti apie asmens duomenų saugumo pažeidimą kompetentingai priežiūros institucijai – Valstybinei duomenų apsaugos inspekcijai, nebent asmens duomenų saugumo pažeidimas neturėtų kelti pavojaus fizinių asmenų teisėms ir laisvėms;

27.2. duomenų valdytojo pareigą nepagrįstai nedelsiant pranešti duomenų subjektui apie asmens duomenų pažeidimą, kai asmens duomenų saugumo pažeidimas gali sukelti didelę riziką fizinių asmenų teisėms ir laisvėms;

27.3. duomenų valdytojo pareigą atlikti numatytų asmens duomenų tvarkymo operacijų poveikio duomenų apsaugai vertinimą, kai asmens duomenų tvarkymo būdas gali sukelti didelę riziką fizinių asmenų teisėms ir laisvėms;

27.4. duomenų valdytojo pareigą konsultuotis su kompetentinga priežiūros institucija – Valstybine duomenų apsaugos inspekcija prieš pradedant duomenų tvarkymą, jei poveikio duomenų apsaugos vertinimas rodo, kad duomenų tvarkymas sukeltų didelę riziką, jei duomenų valdytojas nesiimtų priemonių tai rizikai sumažinti.

28. Šalys Sąlygų 2 priede nustato tinkamas technines ir organizacines priemones, kurias turi taikyti duomenų tvarkytojas siekiant padėti duomenų valdytojui įgyvendinti duomenų subjekto teises ir vykdyti Reglamento (ES) 2016/679 33–36 straipsniuose įtvirtintas pareigas. Tai taikoma prievolėms, nurodytoms Sąlygų 27 punkte.

29. Duomenų tvarkytojas teikia pagalbą duomenų valdytojui pagal Sąlygų 12, 26-28 punktus neatlygintinai.

VIII SKYRIUS
PRANEŠIMAS APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ

30. Duomenų tvarkytojas, sužinojęs apie asmens duomenų saugumo pažeidimą, nepagrįstai nedelsdamas apie tai praneša duomenų valdytojui. Duomenų tvarkytojas praneša duomenų valdytojui ne vėliau kaip per dvidešimt keturias valandas po to, kai duomenų tvarkytojas sužinojo apie asmens duomenų saugumo pažeidimą, kad duomenų valdytojas galėtų įvykdyti duomenų valdytojo pareigą pranešti apie asmens duomenų saugumo pažeidimą kompetentingai priežiūros institucijai, pagal Reglamento (ES) 2016/679 33 straipsnį.

31. Sąlygų 27.1 papunktyje nurodyta duomenų tvarkytojo pareiga padėti duomenų valdytojui pranešti kompetentingai priežiūros institucijai apie asmens duomenų pažeidimą reiškia, kad duomenų tvarkytojas privalo duomenų valdytojui padėti gauti toliau išvardytą informaciją, kuri, remiantis Reglamento (ES) 2016/679 33 straipsnio 3 dalimi, turi būti nurodyta duomenų valdytojo pranešime kompetentingai priežiūros institucijai:

31.1. asmens duomenų pobūdis, įskaitant, jei įmanoma, atitinkamų duomenų subjektų kategorijos ir apytikslis jų skaičius bei atitinkamų asmens duomenų kategorijos ir apytikslis skaičius;

31.2. tikėtinos asmens duomenų pažeidimo pasekmės;

31.3. priemonės, kurių ėmėsi ar siūlo imtis duomenų valdytojas dėl asmens duomenų pažeidimo, įskaitant, jei reikia, priemones, skirtas sušvelninti galimą neigiamą pažeidimo poveikį;

31.4. bet kokia kita reikšminga informacija, kuri yra ar gali būti reikalinga duomenų valdytojui rengiant pranešimą arba atsakant į papildomus su asmens duomenų saugumo pažeidimu susijusius kompetentingos priežiūros institucijos raštus.

32. Sąlygų 2 priede nustatomi visi elementai, kuriuos turi pateikti duomenų tvarkytojas, padėdamas duomenų valdytojui pranešti kompetentingai priežiūros institucijai apie asmens duomenų saugumo pažeidimą. Jei duomenų tvarkytojas duomenų valdytojui pateikia ne visą informaciją apie asmens duomenų saugumo pažeidimą arba vėliau paaiškėja papildoma informacija, duomenų tvarkytojas privalo nepagrįstai nedelsdamas, bet ne vėliau kaip per dvidešimt keturias valandas nuo informacijos paaiškėjimo pateikti papildomą pranešimą duomenų valdytojui, nurodydamas visą trūkstamą informaciją.

33. Duomenų tvarkytojas duomenų valdytojo prašymu, papildomai prie Sąlygų 32 punkte nurodytos informacijos, pateikia dokumentų, pavyzdžiui, pagrindžiančių atliktus veiksmus, taikytas priemones ar atliktus vidinius patikrinimus ir jų išvadų, kopijas.

34. Duomenų tvarkytojas šiame Sąlygų skyriuje nurodytus veiksmus atlieka neatlygintinai.

27.1. the Data Controller's obligation to without undue delay and, where feasible, not later than within 72 hours after having become aware of it, notify the competent supervisory authority – the State Data Protection Inspectorate – of the personal data breach, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;

27.2. the Data Controller's obligation to notify without undue delay the data subject if personal data breach is likely to result in a high risk to the rights and freedoms of natural persons;

27.3. the Data Controller's obligation to carry out a data protection impact assessment of the envisaged personal data processing operations where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

27.4. the Data Controller's obligation to consult the competent supervisory authority – the State Data Protection Inspectorate – prior to processing if the data protection impact assessment indicates that processing of data would result in high risk if the Data Controller fails to take measures to mitigate the risk.

28. The Parties shall establish in Annex 2 hereto the appropriate technical and organisational measures which should be taken by the Data Processor to assist the Data Controller with the data subject rights and with the obligations under Articles 33 to 36 of Regulation (EU) 2016/679. This applies to the obligations set out in Paragraph 27 of the Clauses.

29. The Data Processor shall provide assistance to the Data Controller in accordance with Paragraphs 12, 26–28 of the Clauses free of charge.

CHAPTER VIII
NOTIFICATION OF PERSONAL DATA BREACH

30. The Data Processor shall notify the Data Controller without undue delay after becoming aware of a personal data breach. The Data Processor shall notify the Data Controller within 24 hours from the moment on which the Data Processor becomes aware of the personal data breach so that the Data Controller could fulfil the Data Controller's obligations to report the personal data breach to the competent supervisory authority in accordance with Article 33 of Regulation (EU) 2016/679.

31. The obligation to assist the Data Controller to notify the competent supervisory authority of a personal data breach provided for in Paragraph 27.1 hereof shall imply that the Data Processor must assist the Data Controller to obtain the information specified below which, according to Article 33(3) of Regulation (EU) 2016/679, must be indicated in the Data Controller's notification to the competent supervisory authority:

31.1. the nature of the personal data including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data concerned;

31.2. the likely consequences of the personal data breach;

31.3. the measures taken or proposed to be taken by the Data Controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects;

31.4. any other relevant information which is or may be necessary for the Data Controller when preparing the notification or responding to additional requests of the competent supervisory authority related to the personal data breach.

32. Annex 2 to the Clauses shall set out all elements which must be provided by the Data Processor to assist the Data Controller to notify the competent supervisory authority of a personal data breach. If the Data Processor fails to provide all information on the personal data breach to the Data Controller or later additional information becomes evident, the Data Processor shall be obliged to without undue further delay but not later than within 24 hours from the moment of becoming aware of new information give an additional notification to the Data Controller specifying all missing information.

33. Upon request of the Data Controller, in addition to the information provided for in paragraph 31 hereof, the Data Processor shall provide copies of the documents, for example, the documents justifying the carried out actions, applied measures or carried out internal inspections and conclusions of the inspections.

34. The Data Processor shall perform the activities referred to in this section of the Clauses free of charge.

IX SKYRIUS
DUOMENŲ TRYNIMAS IR GRĄŽINIMAS

35. Pasibaigus asmens duomenų tvarkymo paslaugų teikimui, duomenų tvarkytojas privalo duomenų valdytojo pasirinkimu ištrinti visus asmens duomenis, tvarkomus duomenų valdytojo vardu, ir įrodyti duomenų valdytojui, kad tai padarė ir (arba) grąžinti visus asmens duomenis duomenų valdytojui ir ištrinti esamas kopijas, nebent asmens duomenis reikia saugoti pagal Europos Sąjungos ar Lietuvos Respublikos teisės aktus.

X SKYRIUS
DUOMENŲ TVARKYTOJO AUDITAS IR TIKRINIMAS

36. Duomenų tvarkytojas duomenų valdytojui neatlygintinai suteikia visą informaciją, reikalingą įrodyti, kad laikomasi Reglamento (ES) 2016/679 28 straipsnyje ir Sąlygose nustatytų pareigų, ir sudaro sąlygas bei padeda atlikti duomenų valdytojui ar kitam duomenų valdytojo įgaliotam auditoriui auditą, įskaitant patikrinimus vietoje.

37. Duomenų valdytojo atliekamam duomenų tvarkytojo ir pagalbinių duomenų tvarkytojų auditui, įskaitant patikrinimus, taikomos Sąlygų 2 Priedo 7 ir 8 punktuose nurodytos procedūros.

38. Duomenų tvarkytojas turi suteikti priežiūros institucijoms, kurios pagal galiojančius teisės aktus turi prieigą prie duomenų valdytojo ir duomenų tvarkytojo įrenginių, arba atstovams, veikiantiems tokių priežiūros institucijų vardu, prieigą prie duomenų tvarkytojo fizinių priemonių ar atlikti kitus priežiūros institucijų nurodytus veiksmus auditui ar kitam patikrinimui atlikti. Šalys turi kompetentingų priežiūros institucijų prašymu pateikti šiose Sąlygose nurodytą informaciją, įskaitant auditų rezultatus.

XI SKYRIUS
BAIGIAMOSIOS NUOSTATOS

39. Sąlygos įsigalioja nuo Sutarties pasirašymo dienos.

40. Sutartyje numatytų paslaugų teikimo laikotarpiu Sąlygų taikymas negali būti nutrauktas, jei Sutarties šalys nėra susitarusios dėl kitų asmens duomenų tvarkymą reglamentuojančių nuostatų.

41. Jei Sutartyje numatytų paslaugų teikimas nutraukiamas, o asmens duomenys ištrinami arba grąžinami duomenų valdytojui pagal Sąlygų 35 punktą ir Sąlygų 2 Priedo 4 punktą, Sąlygų taikymas gali būti nutraukiamas bet kuriai šaliai pateikus rašytinį pranešimą.

42. Nedarant poveikio jokioms Reglamento (ES) 2016/679 nuostatoms, duomenų tvarkytojui pažeidus pareigas pagal Sąlygas, duomenų valdytojas gali nurodyti duomenų tvarkytojui laikinai sustabdyti asmens duomenų tvarkymą iki pastarasis pradės laikytis Sąlygų arba Sąlygų taikymas bus nutrauktas. Duomenų tvarkytojas nedelsdamas informuoja duomenų valdytoją, jei dėl kokios nors priežasties jis negali vykdyti Sąlygų.

43. Duomenų valdytojas turi teisę nutraukti Sąlygų taikymą ir Sutartį, jeigu:

43.1. duomenų tvarkytojas iš esmės arba nuolat pažeidžia Sąlygas arba savo įsipareigojimus pagal Reglamentą (ES) 2016/679;

43.2. duomenų tvarkytojas nesilaiko privalomo teismo arba priežiūros institucijos sprendimo dėl įpareigojimų pagal Sąlygas arba Reglamentą (ES) 2016/679;

43.3. duomenų valdytojas sustabdė duomenų tvarkytojo atliekamą asmens duomenų tvarkymą pagal Sąlygų 42 punktą ir (ar) 43.1 papunktį ir (ar) 43.2 papunktį ir atitiktis šioms Sąlygoms nėra atkurta per duomenų valdytojo nurodytą terminą ne ilgesnį nei vienas mėnuo nuo asmens duomenų tvarkymo sustabdymo dienos.

44. Sąlygos turi pirmenybę prieš bet kokias panašias su asmens duomenų tvarkymu susijusias nuostatas kituose Šalių susitarimuose.

45. Sąlygų neatskiriama dalis yra:

45.1. Sąlygų 1 priedas „Informacija apie asmens duomenų tvarkymą“;

45.2. Sąlygų 2 priedas „Nurodymai, kaip tvarkyti asmens duomenis“.

46. Kiekviena Šalis paskiria asmenį, atsakingą už Sąlygų vykdymą.

CHAPTER IX
ERASURE AND RETURN OF DATA

35. Upon termination of the provision of personal data processing services, the Data Processor shall be obliged, at the choice of the Data Controller, to delete all personal data processed on behalf of the Data Controller and demonstrate to the Data Controller that the Data Processor did this and/or return all personal data to the Data Controller and delete the existing copies unless the personal data must be stored in accordance with the laws of the European Union or the Republic of Lithuania.

CHAPTER X
AUDIT AND INSPECTION OF THE DATA PROCESSOR

36. The Data Processor shall make available to the Data Controller all information necessary to demonstrate compliance with the obligations set out in Article 28 of Regulation (EU) 2016/679 and the Clauses as well as enable and assist the Data Controller or another auditor mandated by the Data Controller to carry out an audit including on-the-spot inspections.

37. An audit (including inspections) of the Data Processor and Sub-processors carried out by the Data Controller shall be subject to the procedures provided for in Paragraphs 7 and 8 of Annex 2 hereto.

38. The Data Processor shall grant the supervisory authorities which, according to the law in force, have access to the equipment of the Data Controller and the Data Processor, or the representatives acting on behalf of such supervisory authorities access to the Data Processor's physical facilities or fulfil other instructions of the supervisory authorities to carry out an audit or another inspection. The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority on request.

CHAPTER XI
FINAL PROVISIONS

39. The Clauses shall come into force from the date of signature of the Contract.

40. During the period of provision of the services provided for in the Contract, the Clauses cannot be terminated if the Parties have not agreed on other provisions governing the processing of personal data.

41. If provision of services provided for in the Contract is terminated and personal data are deleted or returned to the Data Controller in accordance with Paragraph 35 of the Clauses and Paragraph 4 of Annex 2 to the Clauses, the Clauses may be terminated by a written notice given by either Party.

42. Without prejudice to any provisions of Regulation (EU) 2016/679, if the Data Processor breaches the obligations hereunder, the Data Controller shall be entitled to instruct the Data Processor to suspend personal data processing on a temporary basis till the latter complies with the Clauses or the Clauses are terminated. The Data Processor shall immediately notify the Data Controller if the Data Processor cannot perform its tasks as agreed in the Clauses for any reason.

43. The Data Controller shall be entitled to terminate the application of the Clauses and the Contract if::

43.1. the Data Processor substantially or persistently breaches the Clauses or obligations under Regulation (EU) 2016/679;

43.2. the Data Processor fails to comply with the binding decision of the court or supervisory authority in relation to the obligations provided for in the Clauses or Regulation (EU) 2016/679;

43.3. the processing of personal data by the Data Processor has been suspended by the Data Controller pursuant to Paragraph 42 and (or) Subparagraph 43.1 and (or) Subparagraph 43.2 of the Clauses and compliance with these Clauses is not restored within a period specified by the Data Controller not exceeding one month from the date of suspension of the processing of personal data.

44. The Clauses shall take precedence over any similar provisions related to processing of personal data set out in other agreements between the Parties.

45. The integral part of the Clauses comprises:

45.1. Annex 1 to the Clauses "Information on processing of personal data";

45.2. Annex 2 to the Clauses "Instructions on processing of personal data".

46. Each Party shall appoint a person responsible for executing the Clauses.

XII SKYRIUS
ŠALIŲ REKVIZITAI, PARAŠAI

DUOMENŲ VALDYTOJAS

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 97121
El. p. statistika@stat.gov.lt
Tinklapis: www.stat.gov.lt

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

DocuSigned by:
E418C627BC95493...
September 28, 2023

DUOMENŲ TVARKYTOJAS

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

Direktorius, Ryan Taylor

2023 m. rugsėjo 28 d

CHAPTER XII
DETAILS AND SIGNATURES OF THE PARTIES

DATA CONTROLLER

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 97121
Email: statistika@stat.gov.lt
Website: www.stat.gov.lt

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

DocuSigned by:
E418C627BC95493...
September 28, 2023

DATA PROCESSOR

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
Email: legalnotices@palantir.com / accountsreceivable@palantir.com

Ryan Taylor, Director

September 28, 2023

Asmens duomenų tvarkymo sąlygų
1 priedas

INFORMACIJA APIE ASMENS DUOMENŲ TVARKYMĄ

1. Duomenų tvarkytojo atliekamo asmens duomenų tvarkymo tikslas yra:

Palantir Foundry licencijos išplėtimas papildomais infrastruktūros ištekliais pagal Sutartį.

2. Duomenų tvarkytojo asmens duomenų tvarkymas daugiausia susijęs su (tvarkymo pobūdžiu):

Asmens duomenų saugojimas pateiktoje infrastruktūroje.

3. Duomenų tvarkymas apima šiuos asmens duomenis:

3.1. Lietuvos gyventojų ir užsieniečių asmens duomenys, saugomi pateiktoje infrastruktūroje.

3.2. Duomenų valdytojo darbuotojų ir kitų asmenų, naudojančių pateiktą infrastruktūrą, duomenys: vardas, pavardė, padalinys, pareigos, telefonas, el. paštas, naudotojo kodas, kita informacija, skirta asmeniui identifikuoti ir teisėms naudoti infrastruktūrą suteikti, naudojant infrastruktūrą atlikti veiksmai.

4. Duomenų tvarkymas apima šias duomenų subjektų kategorijas:

4.1. Lietuvos gyventojai ir užsieniečiai.

4.2. Duomenų valdytojo darbuotojai ir kiti asmenys, naudojantys pateiktą infrastruktūrą.

5. Duomenų tvarkytojas gali tvarkyti asmens duomenis duomenų valdytojo vardu, kai įsigalioja Sąlygos. Duomenų tvarkymo trukmė:

Asmens duomenys tvarkomi, kol galioja Sutartis.

_____

Annex 1 to the Clauses for Personal Data Processing

INFORMATION ON PROCESSING OF PERSONAL DATA

1. The purpose of processing of personal data by the Data Processor shall be:

Extension of the Palantir Foundry license with additional infrastructure resources under the Contract.

2. Processing of personal data by the Data Processor shall be mainly related to (nature of processing):

Personal data storage in the provided infrastructure.

3. The data processing shall cover the following the type of personal data:

3.1. Personal data of the residents of Lithuania and non-residents stored in the provided infrastructure.

3.2. Data of the Data Controller's employees and other persons who are users of the provided infrastructure: name, surname, division, position, telephone, email, user code, other information to identify the employee and to grant work rights, user actions performed using the infrastructure.

4. The processing shall cover the following categories of data subjects:

4.1. Residents of Lithuania and non-residents.

4.2. The Data Controller's employees and other persons who are users of the provided infrastructure.

5. The Data Processor shall be entitled to process personal data on behalf of the Data Controller after entry into force of the Clauses. Duration of processing:

Personal data are processed for as long as the Contract is in force.

_____

Asmens duomenų tvarkymo sąlygų
2 priedas

Annex 2 to the Clauses for Personal Data Processing

NURODYMAI, KAIP TVARKYTI ASMENS DUOMENIS

1. Duomenų tvarkymo nurodymas

Duomenų tvarkytojas duomenų valdytojo vardu saugo asmens duomenis pagal Sutartį pateiktoje papildomoje infrastruktūroje.

2. Duomenų tvarkymo saugumas

Duomenų tvarkytojas turi teisę ir privalo priimti sprendimus dėl techninių ir organizacinių saugumo priemonių naudojimo užtikrinti reikiamą (ir suderintą) duomenų saugumo lygį. Duomenų tvarkytojo taikomos organizacinės ir techninės duomenų saugumo priemonės turi užtikrinti tokio lygio saugumą, kuris atitiktų tvarkomų asmens duomenų pobūdį, aprėptį, kontekstą ir tikslus, taip pat duomenų tvarkymo keliamus įvairios tikimybės ir rimtumo pavojus asmenų teisėms ir laisvėms ir jų tvarkymo riziką.

Tačiau duomenų tvarkytojas bet kuriuo atveju įgyvendina šias su duomenų valdytoju suderintas priemones:

- paslaugas pagal Sutartį teikia tik kvalifikuoti ir tinkamai apmokyti dirbti duomenų tvarkytojo darbuotojai;
- paslaugas pagal Sutartį teikiantys duomenų tvarkytojo darbuotojai yra tinkamai informuoti ir geba taikyti duomenų saugos, asmens duomenų apsaugos reikalavimus;
- prieiga prie asmens duomenų suteikiama tik tiems duomenų tvarkytojo darbuotojams, kuriems asmens duomenys reikalingi jų darbo funkcijoms atlikti;
- pasibaigus darbo santykiams arba nustojus vykdyti darbo funkcijas, kurioms atlikti būtina prieiga prie asmens duomenų, nedelsiant panaikinama duomenų tvarkytojo darbuotojo prieiga prie asmens duomenų;
- duomenų tvarkytojo darbuotojai, kurie atlikdami darbo funkcijas tvarko asmens duomenis, prieš pradėdami vykdyti šias funkcijas įsipareigoja laikytis konfidencialumo principo ir laikyti paslaptyje bet kokią su asmens duomenimis susijusią informaciją, su kuria jie susipažino vykdydami savo pareigas bei pasirašo konfidencialumo pasižadėjimą. Pareiga saugoti asmens duomenų paslaptį galioja visą darbuotojo darbo laiką, taip pat galioja darbuotoją paskyrus į kitas pareigas ir pasibaigus darbo santykiams;
- duomenų tvarkytojo darbuotojai privalo nedelsdami pranešti duomenų tvarkytojo įgaliotam asmeniui apie asmens duomenų sugadinimą, asmens duomenų sunaikinimą, asmens duomenų saugumo pažeidimą arba bet kokią įtartiną situaciją, kuri gali kelti grėsmę tvarkomų asmens duomenų saugumui.

3. Pagalba duomenų valdytojui

Duomenų tvarkytojas, kiek tai įmanoma ir atsižvelgiant į toliau nurodytą pagalbos sritį bei apimtį, padeda duomenų valdytojui įgyvendinti Reglamento (ES) 2016/679, Lietuvos Respublikos teisės aktų ir Sąlygų reikalavimus.

Duomenų tvarkytojas nedelsdamas, tinkamai ir neatlygintinai atsako į duomenų valdytojo užklausas, susijusias su duomenų tvarkymu pagal Sąlygas.

Duomenų tvarkytojas saugo atitinkamus duomenų tvarkymo veiklos, kurią vykdo duomenų valdytojo vardu, įrašus.

INSTRUCTIONS ON PROCESSING OF PERSONAL DATA

1. Instruction to process data

The Data Processor, on behalf of the Data Controller, shall store personal data in the additional infrastructure provided under the Contract.

2. Security of processing

The Data Processor shall be entitled and obliged to take decisions on the use of technical and organisational security measures to ensure necessary (and agreed) level of data security. The technical and organisational data security measures applied by the Data Processor shall ensure a level of security appropriate to the nature, scope, context and purposes of the processed personal data as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

However, in any case the Data Processor shall implement the following measures agreed with the Data Controller:

- only qualified and appropriately trained staff of the Data Processor shall provide services under the Contract;
- the Data Processor's employees providing services under the Contract shall be adequately informed and able to apply data security and personal data protection requirements;
- access to personal data shall be granted only to those employees of the Data Processor who need personal data to perform their work functions;
- access to personal data by an employee of the Data Processor shall be immediately terminated upon termination of the employment relationship or cessation of the performance of the work functions for which access to personal data is necessary;
- the Data Processor's employees who process personal data in the course of performing their work functions shall, prior to carrying out those functions, undertake to observe the principle of confidentiality and to keep secret any information relating to personal data of which they have become aware in the course of their duties, and shall sign an undertaking of confidentiality. The obligation to keep personal data secret is valid for the entire time of the employee's work, as well as after the employee is assigned to another position and after the end of the employment relationship;
- the employees of the Data Processor shall immediately notify the Data Processor's authorised person of any damage to persona data, destruction of personal data, breach of security of personal data or any suspicious situation which may pose a threat to the security of processed personal data.

3. Assistance to the Data Controller

The Data Processor shall, insofar as this is possible and taking into account the area and scope of assistance specified below, assist the Data Controller to implement the requirements of Regulation (EU) 2016/679, laws of the Republic of Lithuania and the Clauses.

The Data Processor shall respond promptly, appropriately and free of charge to the Data Controller's requests related to the data processing in accordance with the Clauses.

The Data Processor shall keep appropriate records of the data processing activities carried out on behalf of the Data Controller.

Jei duomenų subjektas kreipiasi į duomenų tvarkytoją su prašymu įgyvendinti Reglamento (ES) 2016/679 III skyriuje nustatytas duomenų subjekto teises, duomenų tvarkytojas nepagrįstai nedelsdamas, bet ne vėliau kaip per 3 darbo dienas nuo prašymo gavimo, perduoda duomenų subjekto prašymą duomenų valdytojui, apie tai informuodamas duomenų subjektą.

Duomenų tvarkytojas padeda duomenų valdytojui įgyvendinti duomenų subjekto prašymą pateikdamas visus reikiamus dokumentus ar kitą informaciją, reikalingą tam, kad duomenų valdytojas galėtų tinkamai užtikrinti duomenų subjekto teisių įgyvendinimą.

Duomenų tvarkytojas pats įgyvendina duomenų subjekto prašymą tik duomenų valdytojo nurodymu, laikydamasis duomenų valdytojo pateiktų duomenų subjekto prašymo įgyvendinimo sąlygų.

Jei duomenų subjektas pateikia prašymą patvirtinti, ar su duomenų subjektu susiję asmens duomenys yra tvarkomi, ir pateikti tvarkomų asmens duomenų kopiją, duomenų valdytojo nurodymu duomenų tvarkytojas neatlygintinai pateikia reikiamas duomenų kopijas duomenų valdytojui.

Duomenų tvarkytojas padeda duomenų valdytojui atlikti poveikio duomenų apsaugai vertinimą Reglamento (ES) 2016/679 35 straipsnyje numatytais atvejais, įskaitant atvejus, kai asmens duomenų tvarkymas atitinka operacijas, nustatytas Duomenų tvarkymo operacijų, kurioms taikomas reikalavimas atlikti poveikio duomenų apsaugai vertinimą, sąraše, patvirtiname Valstybinės duomenų apsaugos inspekcijos direktoriaus 2019 m. kovo 14 d. įsakymu Nr. 1T-35(1.12.E) „Dėl Duomenų tvarkymo operacijų, kurioms taikomas reikalavimas atlikti poveikio duomenų apsaugai vertinimą, sąrašo patvirtinimo“.

Duomenų tvarkytojas neatlygintinai pateikia duomenų valdytojui per duomenų valdytojo nurodytą protingą terminą duomenų valdytojo prašomą informaciją, kuri duomenų valdytojui pagrįstai reikalinga poveikio duomenų apsaugai vertinimui atlikti.

Duomenų tvarkytojas padeda įgyvendinti duomenų valdytojui prievolę prieš pradedant tvarkyti asmens duomenis konsultuotis su priežiūros institucija – Valstybine duomenų apsaugos inspekcija, jeigu pagal Reglamento (ES) 2016/679 35 straipsnį atliktame poveikio duomenų apsaugai vertinime nurodyta, kad duomenis tvarkant kiltų pavojus, jei duomenų valdytojas nesiimtų priemonių pavojui sumažinti.

Duomenų tvarkytojas neatlygintinai pateikia duomenų valdytojui per duomenų valdytojo nurodytą protingą terminą šią informaciją, jeigu duomenų valdytojas jos neturi:

- duomenų tvarkytojo taikomas technines ir organizacines priemones, skirtas duomenų saugumui užtikrinti bei duomenų subjektų teisėms ir laisvėms apsaugoti;
- duomenų valdytojo ar priežiūros institucijos – Valstybinės duomenų apsaugos inspekcijos, prašomą informaciją, kuri duomenų valdytojui pagrįstai reikalinga siekiant įgyvendinti duomenų valdytojo prievolę konsultuotis su priežiūros institucija – Valstybine duomenų apsaugos inspekcija.

Duomenų tvarkytojas ne vėliau kaip per dvidešimt keturias valandas po to, kai duomenų tvarkytojas sužinojo apie asmens duomenų saugumo pažeidimą, elektroniniu paštu praneša duomenų valdytojui apie asmens duomenų saugumo pažeidimą. Pranešime turi būti pateikta ši informacija:

- asmens duomenų saugumo pažeidimo data ir laikas (jeigu tiksli data ir (ar) laikas nežinomi, nurodoma apytiksliai);
- asmens duomenų saugumo pažeidimo pobūdis ir aplinkybės;
- asmens duomenų saugumo pažeidimo paaiškėjimo data ir laikas;
- asmens duomenų saugumo pažeidimo paaiškėjimo aplinkybės;
- duomenų subjektų, kurių asmens duomenų saugumas pažeistas, skaičius (jeigu tikslus skaičius nežinomas, nurodoma apytiksliai);
- duomenų subjektų, kurių asmens duomenų saugumas pažeistas, kategorijos;
- asmens duomenų, kurių saugumas pažeistas, kategorijos;
- asmens duomenų, kurių saugumas pažeistas, skaičius (jeigu tikslus skaičius nežinomas, nurodoma apytiksliai);
- nustatytos ir (ar) galimos asmens duomenų saugumo pažeidimo pasekmės;

If the data subject contacts the Data Processor with a request to exercise the data subject's rights set out in Chapter III of Regulation (EU) 2016/679, the Data Processor shall, without undue delay, but no later than within 3 working days of receipt of the request, forward the data subject's request to the Data Controller, and shall inform the data subject thereof.

The Data Processor shall assist the Data Controller in the implementation of the data subject's request by providing any necessary documents or other information required to enable the Data Controller to ensure the proper exercise of the data subject's rights.

The Data Processor shall implement the data subject's request itself only on the instructions of the Data Controller, in accordance with the terms and conditions for implementation of the data subject's request provided by the Data Controller.

If the data subject submitss a request for confirmation of the processing of personal data relating to the data subject and for a copy of the personal data processed, the Data Processor shall, at the direction of the Data Controller, provide the Data Controller with the necessary copies of the data free of charge.

The Data Processor shall assist the Data Controller in carrying out a data protection impact assessment in the cases provided for in Article 35 of Regulation (EU) 2016/679, including cases where the processing of personal data corresponds to the operations set out in the list of processing operations subject to the requirement to carry out data protection impact assessment, approved by Order No.1T-35(1.12.E) of 14 March 2019 of the Director of the State Data Protection Inspectorate "On the Approval of the List of Processing Operations Subject to the Requirement of Data Protection Impact Assessment".

The Data Processor shall provide the Data Controller, free of charge, within a reasonable period of time specified by the Data Controller, with the information requested by the Data Controller which is reasonably necessary for the Data Controller to carry out the data protection impact assessment.

The Data Processor shall assist the Data Controller in implementing the obligation to consult the supervisory authority – the State Data Protection Inspectorate – prior to the processing of personal data, where data protection impact assessment carried out in accordance with Article 35 of Regulation (EU) 2016/679 has indicated that the processing of the personal data would be at risk if the Data Controller did not take measures to mitigate the risk.

The Data Processor shall provide the Data Controller, free of charge, within a reasonable period specified by the Data Controller, with the following information, if the Data Controller does not have it:

- the technical and organisational measures applied by the Data Processor to ensure data security and to protect the rights and freedoms of data subjects;
- information requested by the Data Controller or the supervisory authority – the State Data Protection Inspectorate – which is reasonably necessary for the Data Controller to comply with the Data Controller's obligation to consult the supervisory authority – the State Data Protection Inspectorate.

The Data Processor shall notify the Data Controller of the personal data breach by email no later than twenty-four hours after the Data Processor has become aware of the personal data security breach. The notification must contain the following information:

- the date and time of the personal data security breach (if the exact date and/or time is not known, it shall be approximate);
- the nature and circumstances of the personal data security breach;
- the date and time of the discovery of the personal data security breach;
- the circumstances in which the personal data breach was discovered;
- the number of data subjects whose personal data security has been breached (if the exact number is not known, it shall be approximate);
- categories of data subjects whose personal data security has been breached;
- categories of personal data whose security has been breached;
- the number of personal data whose security has been breached (if the exact number is not known, it shall be approximate);
- the identified and/or potential consequences of the personal data security breach;

- priemonės, kurių imtasi siekiant sustabdyti ir (ar) nutraukti asmens duomenų saugumo pažeidimą;
- priemonės, kurių imtasi, siekiant sumažinti ir (ar) pašalinti asmens duomenų saugumo pažeidimo pasekmes;
- priemonės, kurių turėtų imtis duomenų valdytojas, kad būtų sustabdytas ir (ar) nutrauktas asmens duomenų saugumo pažeidimas;
- priemonės, kurių turėtų imtis duomenų valdytojas, kad būtų sumažintos ir (ar) pašalintos asmens duomenų saugumo pažeidimo pasekmės;
- priemonės, kurių turėtų imtis duomenų subjektai, kad būtų sumažintos ir (ar) pašalintos asmens duomenų saugumo pažeidimo pasekmės;
- asmuo, galintis suteikti daugiau informacijos apie asmens duomenų saugumo pažeidimą, ir jo kontaktiniai duomenys;
- kita reikšminga informacija, susijusi su asmens duomenų saugumo pažeidimu.

Jeigu duomenų tvarkytojas dėl objektyvių priežasčių negali pateikti duomenų valdytojui visos reikalingos informacijos apie asmens duomenų saugumo pažeidimą, pranešime duomenų valdytojui turi būti nurodyta, kada trūkstama informacija, duomenų tvarkytojo nuomone, galės būti pateikta. Paaiškėjus papildomai informacijai apie asmens duomenų saugumo pažeidimą, duomenų tvarkytojas privalo ją elektroniniu paštu pateikti duomenų valdytojui nepagrįstai nedelsdamas, bet ne vėliau kaip per dvidešimt keturias valandas nuo informacijos paaiškėjimo momento.

Duomenų tvarkytojas privalo bendradarbiauti su duomenų valdytoju nustatant asmens duomenų saugumo pažeidimo aplinkybes, įgyvendinant priemones, skirtas asmens duomenų saugumo pažeidimui sustabdyti ir (ar) nutraukti, asmens duomenų saugumo pažeidimo pasekmėms pašalinti ir (ar) sušvelninti, taip pat pranešant kompetentingai priežiūros institucijai apie asmens duomenų saugumo pažeidimą. Duomenų tvarkytojas privalo per duomenų valdytojo nurodytą protingą terminą pateikti duomenų valdytojo prašomą informaciją, susijusią su asmens duomenų saugumo pažeidimu.

Tais atvejais, kai asmens duomenų saugumo pažeidimą nustato pagalbinis duomenų tvarkytojas, jis apie asmens duomenų saugumo pažeidimą praneša duomenų tvarkytojui. Informaciją apie asmens duomenų saugumo pažeidimą Sąlygose nustatyta tvarka duomenų valdytojui teikia duomenų tvarkytojas.

4. Duomenų saugojimo laikotarpis/duomenų trynimo procedūros

Pasibaigus Sutartyje numatytų paslaugų teikimui, duomenų tvarkytojas privalo duomenų valdytojo pasirinkimu ištrinti visus asmens duomenis, tvarkomus duomenų valdytojo vardu, ir (arba) grąžinti visus asmens duomenis duomenų valdytojui ir ištrinti esamas kopijas, nebent asmens duomenis reikia saugoti pagal Europos Sąjungos ar Lietuvos Respublikos teisės aktus. Duomenų tvarkytojas privalo raštu informuoti duomenų valdytoją apie asmens duomenų ištrynimą ir (ar) asmens duomenų grąžinimą, taip pat apie tai, kokie asmens duomenys ar jų kopijos nėra ištrinami ar grąžinami pagal Europos Sąjungos ar Lietuvos Respublikos teisės aktus bei kokie teisės aktai tai reglamentuoja.

5. Duomenų tvarkymo vieta

Atsižvelgiant į Sąlygas, be išankstinio rašytinio duomenų valdytojo leidimo asmens duomenys negali būti tvarkomi kitoje teritorijoje nei Europos Sąjungos šalys.

6. Nurodymai dėl asmens duomenų perdavimo į trečiąją valstybę ar tarptautinėms organizacijoms

Duomenų valdytojo nurodymas dėl asmens duomenų perdavimo į trečiąją valstybę ar tarptautinėms organizacijoms, prireikus, bus pateiktas atskiru rašytiniu dokumentu, laikantis Reglamento (ES) 2016/679 V skyriaus nuostatų.

Jei duomenų valdytojas nenurodo Sąlygose arba vėliau nepateikia dokumentais pagrįstų nurodymų dėl asmens duomenų perdavimo į trečiąją valstybę ar tarptautinėms organizacijoms, duomenų tvarkytojas neturi teisės atlikti tokį perdavimą pagal Sąlygas.

- the measures taken to stop and/or terminate the personal data security breach;
- the measures taken to mitigate and/or eliminate the consequences of the personal data security breach;
- the measures to be taken by the Data Controller to stop and/or terminate the personal data security breach;
- the measures to be taken by the Data Controller to mitigate and/or eliminate the consequences of the personal data security breach;
- the measures to be taken by the data subjects to mitigate and/or eliminate the consequences of the personal data security breach;
- the person who can provide further information about the personal data security breach and his/her contact details;
- any other relevant information relating to the personal data security breach.

If, for objective reasons, the Data Processor is unable to provide the Data Controller with all the necessary information about a breach of personal data security, the notification to the Data Controller must indicate when, in the opinion of the Data Processor, the missing information can be provided. In the event that additional information about the personal data security breach becomes available, the Data Processor shall provide it to the Data Controller by email without undue delay, but no later than within twenty-four hours from the moment the information becomes available.

The Data Processor shall cooperate with the Data Controller in identifying the circumstances of the personal data security breach, in implementing measures to stop and/or terminate the personal data security breach, to eliminate and/or mitigate the consequences of the personal data security breach, as well as notify the competent supervisory authority of the personal data security breach. The Data Processor shall provide the information requested by the Data Controller in relation to the personal data security breach within a reasonable period specified by the Data Controller.

Where personal data security breach is detected by a sub-processor, the sub-processor shall notify the personal data security breach to the Data Processor.

The Data Processor shall provide the Data Controller with the information on the personal data security breach in accordance with the procedures set out in the Clauses.

4. Data retention period/Data erasure procedures

Upon termination of provision of services provided for in the Contract, the Data Processor shall be obliged, at the choice of the Data Controller, to delete all personal data processed on behalf of the Data Controller and (or) return all personal data to the Data Controller and delete the existing copies unless the personal data must be stored in accordance with the legislation of the European Union or the Republic of Lithuania. The Data Processor shall inform the Data Controller in writing about the deletion and/or return of personal data, as well as about which personal data or copies thereof are not deleted or returned in accordance with the legislation of the European Union or the Republic of Lithuania, and which legal acts regulate this.

5. Data processing location

In accordance with the Clauses, personal data shall not be processed in a territory other than the countries of the European Union without the prior written consent of the Data Controller.

6. Instructions on transfer of personal data to a third country or international organisations

The Data Controller's instruction on the transfer of personal data to a third country or international organisations, if necessary, will be provided in a separate written document, in accordance with the provisions of Chapter V of Regulation (EU) 2016/679.

If the Data Controller does not specify in the Clauses or subsequently does not provide documented instructions on the transfer of personal data to a third country or international organisations, the Data Processor shall not be entitled to carry out such transfer in accordance with the Clauses.

7. Procedūros, skirtos duomenų valdytojo atliekamiems duomenų tvarkytojo asmens duomenų tvarkymo auditams, įskaitant patikrinimams vietoje

Duomenų tvarkytojas per duomenų valdytojo nurodytą protingą terminą neatlygintinai pateikia duomenų valdytojui visą informaciją, būtiną siekiant įrodyti, kad vykdomos Sąlygose nustatytos prievolės, ir, duomenų valdytojo prašymu, sudaro sąlygas bei padeda atlikti duomenų tvarkymo veiklos, kuriai taikomos Sąlygos, auditą, įskaitant patikrinimus, pagrįstais laiko tarpais arba tais atvejais, kai nustatoma, kad nesilaikoma Sąlygų reikalavimų. Priimdamas sprendimą dėl audito ar patikrinimo, duomenų valdytojas gali atsižvelgti į atitinkamus duomenų tvarkytojo turimus sertifikatus.

Duomenų valdytojas gali pats atlikti auditą (patikrinimą) arba įgalioti nepriklausomą auditorių. Auditas (patikrinimas) gali apimti patikrinimus duomenų tvarkytojo patalpose ar fiziniuose objektuose ir gali būti atliekamas tinkamai apie jį pranešus duomenų tvarkytojui ne vėliau kaip prieš 5 darbo dienas iki numatytos audito ar patikrinimo dienos.

Remdamasis audito ar patikrinimo rezultatais, duomenų valdytojas gali paprašyti duomenų tvarkytoją imtis papildomų priemonių, kad būtų užtikrinta atitiktis Reglamentui (ES) 2016/679, galiojančioms Europos Sąjungos ar Lietuvos Respublikos duomenų apsaugos nuostatoms ir Sąlygoms.

Priežiūros institucijos – Valstybinės duomenų apsaugos inspekcijos, prašymu, duomenų valdytojas ir duomenų tvarkytojas pateikia priežiūros institucijos nurodytą informaciją, įskaitant bet kokio audito ar patikrinimo rezultatus.

8. Procedūros, skirtos pagalbinių duomenų tvarkytojų atliekamų asmens duomenų tvarkymo auditams, įskaitant patikrinimams vietoje

Duomenų tvarkytojas per duomenų valdytojo nurodytą protingą terminą neatlygintinai pateikia duomenų valdytojui visą informaciją, būtiną siekiant įrodyti, kad pagalbinis duomenų tvarkytojas vykdo Sąlygose nustatytas prievoles.

Jei reikia, duomenų valdytojas gali inicijuoti pagalbinio duomenų tvarkytojo auditą ar patikrinimą. Tai gali būti taikoma, jei duomenų valdytojas mano, kad duomenų tvarkytojas, prižiūrintis pagalbinį duomenų tvarkytoją, duomenų valdytojui nepateikė pakankamai dokumentų, kad būtų galima nustatyti, ar pagalbinis duomenų tvarkytojas atlieka duomenų tvarkymą pagal Sąlygas. Priimdamas sprendimą dėl audito ar patikrinimo, duomenų valdytojas gali atsižvelgti į atitinkamus pagalbinio duomenų tvarkytojo turimus sertifikatus.

Duomenų tvarkytojas, duomenų valdytojo prašymu, sudaro sąlygas bei padeda atlikti pagalbinio duomenų tvarkytojo veiklos, kuriai taikomos Sąlygos, auditą ar patikrinimą.

Duomenų valdytojas gali pats atlikti auditą (patikrinimą) arba įgalioti nepriklausomą auditorių. Auditas ar patikrinimas gali būti atliekamas tinkamai apie jį pranešus duomenų tvarkytojui ne vėliau kaip prieš 5 darbo dienas iki numatytos audito ar patikrinimo dienos.

Remdamasis audito ar patikrinimo rezultatais, duomenų valdytojas gali paprašyti duomenų tvarkytoją įpareigoti pagalbinį duomenų tvarkytoją imtis papildomų priemonių, kad būtų užtikrinta atitiktis Reglamentui (ES) 2016/679, galiojančioms Europos Sąjungos ar Lietuvos Respublikos duomenų apsaugos nuostatoms ir Sąlygoms.

Duomenų valdytojo dalyvavimas pagalbinio duomenų tvarkytojo audite ar patikrinime nekeičia fakto, kad duomenų tvarkytojui ir toliau tenka visa atsakomybė už pagalbinio duomenų tvarkytojo atitiktį Reglamentui (ES) 2016/679, galiojančioms Europos Sąjungos ar Lietuvos Respublikos duomenų apsaugos nuostatoms ir Sąlygoms.

7. Procedures for the Data Processor's personal data processing audits, including on-the-spot inspections carried out by the Data Controller

The Data Processor shall, within a reasonable period specified by the Data Controller, provide the Data Controller, free of charge, with all information necessary to demonstrate compliance with the obligations set out in the Clauses and, at the request of the Data Controller, shall create the conditions for and assist in performing an audit, including inspections, of the data processing activities subject to the Clauses, at reasonable intervals or when non-compliance with the requirements of the Clauses is identified. When deciding on an audit or inspection, the Data Controller may take into account the relevant certificates held by the Data Processor.

The Data Controller can perform the audit (inspection) itself or authorize an independent auditor. The audit (inspection) may include inspections at the premises or physical objects of the Data Processor and may be carried out with due notice to the Data Processor at least 5 working days before the scheduled date of the audit or inspection.

Based on the results of the audit or inspection, the Data Controller may request the Data Processor to take additional measures to ensure compliance with Regulation (EU) 2016/679, applicable data protection provisions of the European Union or the Republic of Lithuania, and the Clauses.

At the request of the supervisory authority (the State Data Protection Inspectorate), the Data Controller and the Data Processor shall provide the information specified by the supervisory authority, including the results of any audit or inspection.

8. Procedures for the Sub-processors' personal data processing audits, including on-the-spot inspections

The Data Processor shall, within a reasonable period specified by the Data Controller, provide the Data Controller, free of charge, with all information necessary to demonstrate the compliance of the Sub-processor with the obligations set out in the Clauses.

If necessary, the Data Controller may initiate an audit or inspection of the Sub-processor. This may apply if the Data Controller considers that the Data Processor supervising the Sub-processor has not provided the Data Controller with sufficient documentation to determine whether the Sub-processor is carrying out the processing in accordance with the Clauses. When deciding on an audit or inspection, the Data Controller may take into account the relevant certificates held by the Sub-processor.

The Data Processor shall, at the request of the Data Controller, create the conditions for and assist in performing an audit or inspection of the activities of the Sub-Processor subject to the Clauses.

The Data Controller can perform the audit (inspection) itself or authorize an independent auditor. The audit or inspection may be carried out with due notice to the Data Processor at least 5 working days before the scheduled date of the audit or inspection.

Based on the results of the audit or inspection, the Data Controller may request the Data Processor to oblige the Sub-processor to take additional measures to ensure compliance with Regulation (EU) 2016/679, applicable data protection provisions of the European Union or the Republic of Lithuania, and the Clauses.

The Data Controller's participation in the audit or inspection of the Sub-processor shall not change the fact that the Data Processor continues to bear full responsibility for the compliance of the Sub-processor with Regulation (EU) 2016/679, applicable data protection provisions of the European Union or the Republic of Lithuania, and the Clauses.