PREKIŲ PIRKIMO PARDAVIMO SUTARTIS

Nr. _____

UAB „Ignitis grupės paslaugų centras“, pagal Lietuvos Respublikos įstatymus įsteigta ir veikianti uždaroji akcinė bendrovė, juridinio asmens kodas 303200016, PVM mokėtojo kodas LT 100008194913, registruotos buveinės adresas Laisvės pr. 10, LT-04215 Vilnius, Lietuvos Respublika, apie kurią duomenys kaupiami ir saugomi VĮ Registrų centras,

25_GSC_IG_0002 (toliau – Pirkėjas), ir

Nossa Data LTD, pagal Jungtinės Karalystės įstatymus teisėtai įregistruota ir veikianti bendrovė, juridinio asmens kodas 12651742, PVM mokėtojo kodas GB385263181, registruotos buveinės adresas pirmas aukštas, 85 Great Portland g., Londonas, Didysis Londonas, Jungtinė Karalystė,

(toliau – Tiekėjas),

Pirkėjas ir Tiekėjas kiekvienas atskirai toliau vadinamas Šalimi, bendrai vadinami Šalimis, sudarė šią prekių pirkimo - pardavimo sutartį (toliau – Sutartis).

DROSIOS NUOSTATOS IR SUTARTIES OBJEKTAS

1.1. Tiekėjas įsipareigoja Sutartyje numatytomis sąlygomis perduoti ESG duomenų valdymo platformos prieigos licenciją (toliau – Prekės) Pirkėjui nuosavybės teise, o Pirkėjas įsipareigoja priimti Prekes ir sumokėti už jas Tiekėjui Sutartyje nurodytomis sąlygomis ir terminais.

1.2. Ši Sutartis sudaryta pasibaigus viešajam pirkimui, kuriame ekonomiškai naudingiausias pasiūlymas išrinktas pagal kainą.

2. PREKIŲ KIEKIS IR KAINA

2.1. Pagal šią Sutartį Pirkėjui tiekiamos Prekės, aprašytos Techninėje specifikacijoje.

2.2. Bendra Sutarties kaina yra 22 988.79 EUR (dvidešimt du tūkstančiai devyni šimtai aštuoniasdešimt aštuoni eurai 79 euro ct), įskaitant PVM. Bendrą Sutarties kainą sudaro:

CONTRACT FOR PURCHASE AND SALE OF GOODS

No. _____

UAB “Ignitis grupės paslaugų centras”, a private limited liability company duly registered and oper[illegible] laws of the Republic of Lithuania, leg[illegible] 303200016, VAT number LT100008194913, registered address Laisvės pr. 10, LT-04215 Vilnius, the Republic of Lithuania, the data of which is collected and stored by the State Enterprise Centre of Registers,

(hereinafter referred to as the ‘Buyer’), and

Nossa Data LTD, a company legally incorporated and operating under the laws of the United Kingdom, legal entity code 12651742, VAT number GB385263181, registered address First Floor, 85 Great Portland Street, London, Greater London, United Kingdom,

(hereinafter referred to as the ‘Supplier’),

the Buyer and the Supplier both hereinafter individually referred to as the Party and collectively as the Parties, have entered into the following Purchase and Sale Contract of Goods (hereinafter referred to as the ‘Contract’):

1. GENERAL PROVISIONS AND OBJECT OF THE CONTRACT

1.1. The Supplier undertakes to hand over the ESG data management platform access license (hereinafter referred to as the ‘Goods’) to the Buyer in terms and conditions set forth in the Contract by the right of ownership and the Buyer undertakes to accept the Goods and to pay for them to the Supplier in terms and conditions set forth in the Contract.

1.2. The present Contract is concluded after the public procurement has ended, where the most economically advantageous Tender was selected based on the price.

2. SCOPE AND PRICE OF THE GOODS

2.1. The Goods supplied to the Buyer on the basis of the present Contract are described in the Technical Specification.

2.2. Total Contract Price is EUR 22 988.79 (twenty-two thousand nine hundred eighty-eight euros 79 ct, including VAT. The Total Contract Price includes:

2.2.1. Prekių kaina – 18 999.00 EUR (aštuoniolika tūkstančių devyni šimtai devyniasdešimt devyni eurai 00 euro ct), neįskaitant PVM;

2.2.2. Pridėtinės vertės mokestis (PVM) – *21 %* – 3 989.79 EUR (trys tūkstančiai devyni šimtai aštuoniasdešimt devyni eurai 79 euro ct). PVM į Lietuvos Respublikos biudžetą sumoka Pirkėjas.

2.3. Vadovaujantis Viešųjų pirkimų tarnybos direktoriaus patvirtinta Kainodaros taisyklių nustatymo metodika, taikomas kainos apskaičiavimo būdas – fiksuota kaina.

2.4. Pirkėjas moka Tiekėjui fiksuotą kainą už faktiškai įsigytas Prekes.

2.5. Kainų perskaičiavimas vykdomas pagal metodiką, nurodytą Sutarties priede Nr. 3.

3. ŠALIŲ ĮSIPAREIGOJIMAI

3.1. **Pirkėjo pareigos:**

3.1.1. tinkamai ir sąžiningai vykdyti Sutartį;

3.1.2. Sutarties vykdymo metu bendradarbiauti su Tiekėju, teikiant Sutarties vykdymui pagrįstai reikalingą informaciją, kurios pateikimo būtinybė iškilo Sutarties vykdymo metu;

3.1.3. Tiekėjui tinkamai įvykdžius sutartinius įsipareigojimus, priimti Prekes bei už jas sumokėti Sutartyje numatyta tvarka;

3.1.4. suteikti reikiamus įgaliojimus Tiekėjui veikti Pirkėjo vardu (jei tokie įgaliojimai yra reikalingi);

3.1.5. tinkamai vykdyti kitus įsipareigojimus, numatytus Sutartyje ir galiojančiuose Teisės aktuose.

3.2. **Tiekėjo pareigos:**

3.2.1. tinkamai ir sąžiningai vykdyti Sutartį;

3.2.2. Sutartyje nustatytu laiku tiekti kokybiškas Prekes ir ištaisyti nustatytus trūkumus (jeigu tokių būtų);

3.2.3. perduodant Prekes, pateikti Pirkėjui visą būtiną dokumentaciją, įskaitant naudojimo ir priežiūros instrukcijas, bei nemokamai konsultuoti Pirkėją kitais, su Tiekėjo sutartiniais įsipareigojimais susijusiais klausimais;

3.2.4. nedelsiant raštu informuoti Pirkėją apie bet kurias aplinkybes, kurios trukdo ar gali sutrukdyti Tiekėjui tiekti Prekes Sutartyje nustatytais terminais bei tvarka;

3.2.5. savo sąskaita apsaugoti Pirkėją nuo bet kokių pretenzijų, nuostolių, atsirandančių dėl Tiekėjo veiksmų ar aplaidumo vykdant Sutartį bei atlyginti dėl savo kaltų veiksmų padarytą žalą Pirkėjui ir (ar) tretiesiems asmenims bei jų patirtus nuostolius;

3.2.6. užtikrinti iš Pirkėjo Sutarties vykdymo metu gautos ir su Sutarties vykdymu susijusios informacijos konfidencialumą ir apsaugą;

2.2.1. The price of Goods EUR 18 999.00 (eighteen thousand nine hundred ninety-nine euros 00 euro ct), excluding VAT;

2.2.2. Value-added tax (VAT) 21% – EUR 3 989.79 (three thousand nine hundred eighty-nine euros 79 euro ct).
VAT to the budget of the Republic of Lithuania shall be paid by the Buyer.

2.2. Pursuant to the Methodology for Establishment of Pricing Rules, approved by the Director of the Public Procurement Office (hereinafter referred to as the 'Methodology'), the price calculation method – fixed price shall apply.

2.4. The Buyer shall pay the Supplier a fixed price for the actually procured Goods.

2.5. Prices shall be recalculated according to the methodology provided in Annex 3 to the Contract.

3. OBLIGATIONS OF THE PARTIES

3.1. **The Buyer shall undertake to:**

3.1.1. perform the Contract in a proper and fair manner;

3.1.2. cooperate with the Supplier in the performance of the Contract, by providing the information, objectively necessary for the performance of the Contract, which became necessary in course of performance of the Contract;

3.1.3. accept the Goods and pay for them in accordance with the procedure established in the Contract once the Supplier properly implements their contractual obligations;

3.1.4. provide all necessary powers for the Supplier to act on behalf of the Buyer (if such powers are required);

3.1.5. duly fulfil other obligations provided for in the Contract and effective Legislations.

3.2. **The Supplier shall undertake to:**

3.2.1. perform the Contract in a proper and fair manner;

3.2.2. supply quality Goods within the time limits prescribed in the Contract and to rectify identified defects (if any);

3.2.3. when handing over the Goods, provide the Buyer with all necessary documentation, including instructions for use and maintenance, and consult the Buyer free of charge on other matters related to the Supplier's contractual obligations;

3.2.4. immediately notify the Buyer in writing of any circumstances, which hinder or could hinder the Supplier from supplying the Goods within the time limits and the procedure set out in the Contract;

3.2.5. protect the Buyer at own expense from any claims and/or losses occurring due to the actions or negligence of the Supplier in performing the Contract and to compensate to the Buyer and/or third persons damage and losses caused by the fault of the Supplier;

3.2.6. ensure the confidentiality and security of information obtained from the Buyer in course of performance of the

3.2.7. laikytis Lietuvos Respublikos civilinio kodekso bei kitų su Tiekėjo sutartinių įsipareigojimų vykdymu susijusių Lietuvos Respublikoje galiojančių teisės aktų nuostatų ir užtikrinti, kad Tiekėjo specialistai, darbuotojai bei atstovai jų laikytųsi. Tiekėjas garantuoja Pirkėjui ir/ar tretiesiems asmenims nuostolių atlyginimą, jei Tiekėjas ar jo specialistai, darbuotojai, atstovai nesilaikytų Lietuvos Respublikoje galiojančių teisės aktų reikalavimų ir dėl to Pirkėjui ir/ar tretiesiems asmenims būtų pateikti kokie nors reikalavimai ar pradėti procesiniai veiksmai.

3.2.8. susipažinti ir santykiuose su Pirkėju ir Sutarties vykdymui pasitelkiamomis trečiosiomis šalimis laikytis AB "Ignitis grupė" valdybos sprendimais patvirtintos Antikorupcinės politikos (toliau Sutartyje - Politika) ir Etikos kodekso (toliau – Kodeksas). Susipažinti su Politika bei Kodeksu ir (ar) šių dokumentų pakeitimais galima adresu www.ignitisgrupe.lt. Tiekėjas privalo užtikrinti, kad šio punkto ir aprašo reikalavimų laikytųsi Tiekėjas ir Sutarties vykdymui jo pasitelkiamų trečiųjų šalių darbuotojai ir kiti atstovai;

3.2.9. nedelsiant informuoti apie Sutarties galiojimo metu atsiradusias aplinkybes, dėl kurių Sutartis gali neatitikti Politikos, Kodekso nuostatų, nacionalinio saugumo, korupcijos prevencijos, ekonominių ir kitų tarptautinių sankcijų ar kitų viešiems interesų apsaugai skirtų teisės aktų reikalavimų;

3.2.10. vykdydamas Sutartį, turi laikytis šių aplinkosaugos reikalavimų: mažinti popieriaus sunaudojimą, atsisakyti nebūtino dokumentų kopijavimo ir spausdinimo, rengiama techninė dokumentacija, ataskaitos ir (ar) kiti su Sutarties vykdymu susiję dokumentai, prekių perdavimo–priėmimo aktai Pirkėjui turi būti pateikti tik elektroniniu formatu, o techninės dokumentacijos galutinės versijos ir (ar) kita dokumentacija, kuri turi būti pasirašoma bei prekių perdavimo–priėmimo aktai turi būti pasirašomi elektroniniu parašu. Išimtiniais atvejais su Sutarties vykdymu susiję dokumentai gali būti pateikiami fiziniu dokumentų formatu, jeigu toks formatas privalomas pagal teisės aktus ir (ar) Pirkėjas nurodo tokį būtinumą. Esant būtinybei spausdinti, naudojamas perdirbtas popierius, kuris atitinka reikalavimus, patvirtintus aktualios redakcijos Lietuvos Respublikos aplinkos ministro 2011 m. birželio 28 d. įsakymu Nr. D1-508 „Dėl Produktų, kurių viešiesiems pirkimams ir pirkimams taikytini aplinkos apsaugos kriterijai, sąrašo, Aplinkos apsaugos kriterijų

Contract, which is related with the performance of the Contract.

3.2.7. adhere to the provisions of the Civil Code of the Republic of Lithuania and other legislations effective in the Republic of Lithuania related to the performance of contractual obligations of the Supplier and to ensure the adherence thereof by the specialists, employees and representatives of the Supplier. The Supplier warrants the compensation of losses to the Buyer and/or third persons in the event where upon failure of the Supplier or specialists, employees and/or representatives thereof to adhere to the requirements of legislations effective in the Republic of Lithuania, the Buyer and/or third persons receive any claims or any proceedings are initiated against them.

3.2.8. familiarise with, and in its relations with the Buyer and the third persons engaged for the purpose of the performance of the Contract, comply with the provisions of the Anti-Corruption Policy (hereinafter referred to as the 'Policy') and the Supplier Code of Ethics (hereinafter referred to as the 'Code') approved by relevant resolutions of the Management Board of AB "Ignitis grupė" establishing the standards for good business practice, ethics and conduct.The Policy and the Code and/or the amendments thereto are available at http://www.ignitisgrupe.lt. The Service Provider shall ensure that the requirements of this paragraph will be complied with by employees, members of supervisory bodies and other representatives of both the Service Provider and the Third persons engaged for the performance of the Contract;

3.2.9. immediately inform about any circumstances occurring within the course of the validity period of the Contract, which could make the Contract inconsistent with the requirements for Policy, Code, national security, corruption prevention, economic and other international sanctions or other requirements of the legislations designed for protection of the public interest;

3.2.10. when performing the Contract, to adhere to the following environmental requirements: reduce paper consumption, avoid unnecessary copying and printing of documents, technical documentation, reports and/or other documents prepared in relation to the performance of the Contract, certificates of transfer and acceptance of the Services must be submitted to the Buyer only in electronic means, and the final versions of the technical documentation and/or other documentation which must be signed as well as the certificates of transfer and acceptance of the Services must be signed by electronic signature. In exceptional cases, the documents related to the performance of the Contract may be submitted in the physical format, if such a format is mandatory under legal acts and/or the Buyer indicates such necessity. If it must be printed, recycled paper which complies with the requirements approved by Order No D1-508 of the Minister of the Environment of the Republic of Lithuania of 28 June 2011 of the relevant version "On the list of products for which environmental protection criteria are applicable to public procurement and procurement, environmental protection criteria and environmental protection criteria that

ir Aplinkos apsaugos kriterijų, kuriuos perkančiosios organizacijos ir perkantieji subjektai turi taikyti pirkdami prekes, paslaugas ar darbus, taikymo tvarkos aprašo patvirtinimo“;

contracting authorities and contracting entities must apply when purchasing goods, services or works, approval of the description of the application procedure” shall be used;

3.2.11. Sąskaitas teikti teisės aktų nustatyta tvarka ir priemonėmis;

3.2.11. submit Invoices by using the tools and under the procedure established by the legislations;

3.2.12. garantuoti ir patvirtinti, kad tiek Sutarties sudarymo metu, tiek visą jos galiojimo laikotarpį Tiekėjas (jo pasitelkiami subtiekėjai, ūkio subjektai ar kitos trečiosios šalys) ir/ar jo (jų) akcininkas (-ai) ir/ar tiesioginis (-iai) ar netiesioginis (-iai) galutinis (-iai) naudos gavėjas (-ai) ir/ar jų valdomas (-i) subjektas (-ai) (toliau – Subjektai), nėra įtraukti į bet kokį Europos Sąjungos ir/ar Jungtinių Tautų ir/ar Didžiosios Britanijos ir/ar Jungtinių Amerikos Valstijų ir/ar Lietuvos Respublikos prekybinių, ekonominių, finansinių ar kitų sankcijų sąrašą (-us) ir/ar panašų sąrašą (toliau – Sankcijų sąrašai), o taip pat nei vienam iš Subjektų nėra pareikštas bet koks įtarimas, susijęs su dalyvavimu pinigų plovimo, teroristinės veiklos finansavimo ar mokestiniu sukčiavimu susijusioje veikloje ir/ar įsitraukimu į tokią veiklą. Tiekėjas Sutarties vykdymo metu įsipareigoja nedelsdamas raštu, bet ne vėliau nei per 1 (vieną) darbo dieną nuo nurodytų aplinkybių atsiradimo, pranešti Pirkėjui informaciją apie Subjektų įtraukimą į Sankcijų sąrašus, taip pat apie Subjektui pareikštus įtarimus dėl aukščiau nurodytų veiklų ir/ar įsitraukimo į tokias veiklas. Subjektų, kurių akcijomis prekiaujama vertybinių popierių biržoje, naudos gavėjui nustatyti taikomi Lietuvos Respublikos pinigų plovimo ir teroristų finansavimo įstatyme nustatyti kriterijai. Pirkėjas turi teisę reikalauti atlyginti tiesioginius nuostolius, patirtus Tiekėjui pažeidus šiame punkte numatytus įsipareigojimus informuoti ir/ar pateikus klaidingą ir melagingą informaciją apie Subjektų įtraukimą į Sankcijų sąrašus ir/ ar pareikštus įtarimus dėl pinigų plovimo, teroristinės veiklos finansavimo ar su mokestiniu sukčiavimu susijusios veiklos;

3.2.12. confirms and guarantees that both at the time of the conclusion of the Contract and for the entire period of its validity the Supplier (sub-suppliers, economic entities or other third parties) and/or its shareholder(s) and/or direct or indirect final beneficiary(s) and/or the entity(s) they manage (hereinafter "the Entities"), are not included in any list(s) and/or similar list of trade, economic, financial or other sanctions of the European Union and/or the United Nations and/or Great Britain and/or the United States of America and/or the Republic of Lithuania (hereinafter "the Sanctions Lists") nor any allegation is made to any of the Entities relating to participation in and/or involvement in money laundering, terrorist financing or tax fraud-related activities. Throughout the performance of the Contract. The Supplier shall immediately notify the Buyer in writing, but not later than within 1 (one) working day from the occurrence of the specified circumstances, about the inclusion of the Entities in the Sanctions Lists, as well as the suspicions made against the Entity regarding the above activities and/or involvement in such activities. The criteria established in the Law of the Republic of Lithuania on Money Laundering and Terrorist Financing shall apply to the determination of the beneficiary of the Entities whose shares are traded on the stock exchange. The Buyer has the right to claim compensation for direct losses incurred by the Supplier in violation of the obligations provided in this clause of the Contract to inform and/or provide misleading and false information about the inclusion of the Entities in the Sanctions Lists and/or allegations of money laundering, terrorist financing or activities related to tax fraud.

3.2.13. nenaudoti Pirkėjo ir Ignitis grupės įmonių ženklo (-ų) ir (ar) pavadinimo jokioje reklamoje, leidiniuose ar kitur be išankstinio raštiško Pirkėjo sutikimo;

3.2.13. not to use the Buyer’s and Ignitis Group companies’ trademark(s) and/or name in any promotional material, publications or elsewhere without a prior written consent of the Buyer;

3.2.14. visu Sutarties galiojimo laikotarpiu užtikrinti atitiktį Pirkimo sąlygų reikalavimams, įskaitant nacionalinio saugumo interesams bei kilmės reikalavimams, jei tokie reikalavimai buvo numatyti Pirkimo dokumentuose;

3.2.14. to ensure compliance with the requirements of the Procurement Conditions, including national security interests and origin requirements, if such requirements have been provided in the Procurement Documents, throughout the entire period of the Contract;

3.2.15. ne vėliau kaip iki 2025-09-30 sukurti vienkartinio prisijungimo (SSO) integraciją, kurios pagrindu būtų galima konfigūruoti „Entra ID“ per SAML. Šio įsipareigojimo pažeidimas laikomas esminiu Sutarties pažeidimu;

3.2.15. to create a single sign-on (SSO) integration that would enable the configuration of Entra ID via SAML not later than 30 September 2025. Violation of this obligation shall be considered a material breach of the Agreement;

3.2.16. tinkamai vykdyti kitus įsipareigojimus, numatytus Sutartyje ir galiojančiuose Lietuvos Respublikos teisės aktuose.

3.3. Visi kiti Šalių įsipareigojimai, neaptarti šiose sąlygose, reguliuojami Lietuvos Respublikos teisės aktų nustatyta tvarka.

3.2.16. properly implement other obligations established in the Contract and the effective legislations of the Republic of Lithuania.

3.3. All and any other obligations of the Parties, which have not been discussed in the present terms and conditions shall be regulated according to the procedure laid down by legislations of the Republic of Lithuania.

4. PREKIŲ KOKYBĖ

4.1. Prekės ir Prekių kokybė turi atitikti Sutartyje, Techninėje specifikacijoje nurodytus reikalavimus ir teisės aktų, reglamentuojančių Prekių kokybės, saugos, tiekimo reikalavimus bei standartus. Prekių trūkumais laikomi neatitikimai nurodytų dokumentų reikalavimams.

4.2. Pirkėjas per 5 (penkias) darbo dienas nuo Prekių perdavimo-priėmimo akto pasirašymo gali kreiptis į Tiekėją dėl Prekių kokybės trūkumų ir jų pašalinimo.

4.3. Prekių pastebėtiems trūkumams šalinti terminas numatytas Techninėje specifikacijoje.

4.4. Sutarties vykdymo metu Tiekėjas turi teisę keisti Prekių modelį ar (ir) gamintoją, tik gavęs rašytinį Pirkėjo sutikimą. Tiekėjas privalo pateikti Pirkėjui argumentuotą prašymą su įrodymais, kad keičiamos naujos Prekės visiškai atitinka Techninės specifikacijos ir Sutarties reikalavimus, yra ne prastesnės, o lygiavertės ar geresnės kokybės, nebus keičiami Prekių įkainiai (mažinti Prekių įkainius Tiekėjas turi teisę), pristatymo terminai ir kitos Sutarties sąlygos bei pateikti keičiamų naujų Prekių dokumentus. Šalys susitaria, kad atskiras susitarimas (gamintojo/modelio keitimo atveju) dėl Sutarties keitimo pasirašomas nebus. Lygiaverčiu dokumentu bus laikomas Tiekėjo prašymas bei rašytinis Pirkėjo sutikimas. Visi Tiekėjo pateikti dokumentai bei Pirkėjo sutikimas laikomi neatskiriama Sutarties dalimi.

4.5. Už nustatytų Prekių trūkumų nepašalinimą per Techninėje specifikacijoje nustatytą terminą Tiekėjas, Pirkėjui pareikalavus, moka Pirkėjui 0,05 procentų nuo trūkumų turinčių Prekių kainos dydžio delspinigius už kiekvieną uždelstą dieną, kurią vėluojama pašalinti trūkumus bei atlygina Pirkėjo dėl to patirtus tiesioginius nuostolius tiek, kiek jų nepadengia netesybos.

4. QUALITY OF GOODS

4.1. The Goods and the quality thereof shall comply with the requirements laid down in the Contract and in the Technical Specification, as well as the requirements and standards of legislations regulating the quality, security and supply of the Goods. Incompliances of the Goods with the said documents shall be considered as defects of Goods.

4.2. The Buyer may refer to the Supplier regarding the quality defects of the Goods and the elimination thereof within 5 (five) working days from the signature of the Certificate of Transfer and Acceptance of the Goods.

4.3. The deadline for elimination of observed defects of the Goods is prescribed in the Technical Specification.

4.4. The Supplier shall have the right to change the model and/or manufacturer of the Goods only under a written consent of the Buyer. The Supplier shall undertake to present a reasoned application to the Buyer containing evidence that the new substituting Goods fully meet the requirements of the Technical Specification and the Contract, that the Goods are of equal or better quality and that the price rates of the Goods (except for the right of the Supplier to reduce the price rates), their delivery terms and other terms and conditions of the Contract shall remain unchanged, as well as to provide the documents of the new substituting Goods. The Parties agree that a separate agreement regarding the amendment to the Contract (in case of substituting the manufacturer/model) shall not be signed. The application of the Supplier and the written consent of the Buyer shall be considered an equivalent document. All documents submitted by the Supplier and the consent of the Buyer shall form an integral part of the Contract.

4.5. For failure to eliminate the defects within the term prescribed in the Technical Specification, the Supplier shall, at the request of the Buyer, pay the Buyer the contractual penalties at the rate of 0.05 percent for each day by which the defect elimination term has been exceeded. The Supplier shall also compensate the direct losses to the Buyer incurred due to such delay to the extent to which they are not covered by the contractual penalties.

5. TIEKĖJO TEISĖ PASITELKTI TREČIUOSIUS ASMENIS (SUBTIEKĖJUS), JUNGTINĖ VEIKLA

5.1. Sutartis iš Tiekėjo pusės vykdoma jungtinės veiklos pagrindu: NE.

5. SUPPLIER'S RIGHT TO ENGAGE THIRD PERSONS (SUB-SUPPLIERS), JOINT VENTURE

5.1. The performance of the Contract on the part of the Supplier is carried out on the basis of joint venture: NO.

5.2. Kai Tiekėjas Pirkimo procedūrų metu atitikčiai Pirkimo sąlygose nustatytiems reikalavimams įrodyti rėmėsi kitų ūkio subjektų ekonominiais ir finansiniais pajėgumais, Tiekėjas ir ūkio subjektai, kurių pajėgumais Tiekėjas rėmėsi, prisiima solidarią atsakomybę už Sutarties įvykdymą.

5.3. Tiekėjas Sutarčiai vykdyti turi teisę pasitelkti Subtiekėjus tik tai Sutarties daliai, kurią nurodė Pasiūlyme. Tiekėjas Pasiūlyme nurodė Sutarties dalį, kuriai bus pasitelkiami Subtiekėjai: NE.

5.2. In cases, where during the Procurement procedure, the Supplier has relied upon the economic and financial capacities of other economic entities for compliance to the requirements indicated in the Procurement Conditions, the Supplier and economic entities, the capacities of which were relied upon by the Supplier, shall be jointly liable for the performance of the Contract.

5.3. The Supplier shall have the right to engage Sub-Suppliers for the performance of the Contract only for the share of the Contract indicated in the Tender. The Supplier has indicated in the Tender the share of the Contract to be delegated to the engaged Sub-Suppliers: *NO.*

6. PREKIŲ PRISTATYMO TERMINAI IR PERDAVIMO - PRIĖMIMO TVARKA

6.1. Prekės teikiamos nuotoliniu būdu per Techninės specifikacijos 4.1 p. nurodytą terminą.

6.2. Už vėlavimą pristatyti Prekes per Sutarties 6.1. nustatytą terminą Tiekėjas, Pirkėjui pareikalavus, moka Pirkėjui 0,05 procentų nuo vėluojamų pristatyti Prekių kainos dydžio netesybas už kiekvieną uždelstą dieną (tačiau bet kokiu atveju ne mažiau kaip 100,00 EUR (šimtą eurų) už vieną vėlavimo laikotarpį).

6.3. Prekių perdavimo – priėmimo aktas ir Sąskaita, jei nebuvo pateikta išankstinė Sąskaita, už faktiškai įsigytas prekes Pirkėjui pateikiami Prekių atsiėmimo (arba pristatymo) metu.

6. TERMS FOR DELIVERY OF GOODS, PROCEDURE OF TRANSFER AND ACCEPTANCE

6.1. The goods are provided remotely via the deadline specified in Technical Specification point no 4.1.

6.2. For failure to deliver the Goods within the time limits established in paragraph 6.1. of the Contract, at the request of the Buyer, the Supplier shall pay the Buyer the contractual penalties at the rate of 0.05 percent of the price of the *delivery* of which has been delayed for each day of the delay (however, no less than EUR 100,00 (one hundred euros) for one period of delay).

6.3. The Certificate of Transfer and Acceptance of the Goods and the Invoice for actually procured Goods shall be presented to the Buyer at the moment of collection (or delivery) of Goods, unless an advance invoice has already been presented.

7. ŠALIŲ ATSAKOMYBĖ

7.1. Šalys pareiškia, kad Sutartyje nustatytos netesybos yra laikomos teisingomis bei protingo dydžio, ir sutinka, kad jos nebūtų mažinamos, nepriklausomai nuo to, ar dalis prievolės yra įvykdyta. Šalys taip pat pripažįsta, kad minėtų netesybų dydis yra laikomas minimalia neginčijama nukentėjusiosios Šalies patirtų nuostolių suma, kurią kita Šalis turi kompensuoti nukentėjusiajai Šaliai dėl Sutarties pažeidimo (nesilaikymo), nereikalaujant tokių nuostolių dydį patvirtinančių įrodymų.

7.2. Už savo sutartinių įsipareigojimų nevykdymą ar netinkamą vykdymą Šalys atsako šioje Sutartyje ir teisės aktuose nustatyta tvarka. Nuostolių atlyginimas ir netesybų sumokėjimas neatleidžia Šalies nuo Sutarties nuostatų tinkamo vykdymo.

7.3. Pirkėjui pareiškus reikalavimą atlyginti patirtus nuostolius, netesybos įskaitomos į nuostolių atlyginimą. Netesybos taikomos nuo Sutartyje nurodytų sumų be PVM.

7. LIABILITY OF THE PARTIES

7.1. The Parties represent that the contractual penalties established in the Contract are fair and reasonable and the Parties agree not to reduce the contractual penalties, regardless of whether the obligation was partially performed or not. The Parties also acknowledge that the amount of the said contractual penalties shall be regarded an undisputable minimum amount of losses incurred by the injured Party, which must be compensated by the other Party due to the violation (incompliance) of the Contract, without requesting any proof confirming the amount of such losses.

7.2. For failure to perform their contractual obligations or undue performance thereof, the Parties shall be held liable according to the procedure laid down in the present Contract and legislations. The compensation of losses and payment of contractual penalties shall not relieve the Party from due performance of the provisions of the Contract.

7.3. Upon request of the Buyer for compensation of incurred losses, the contractual penalties shall be set-off against the compensation of losses. Contractual penalties shall be applied on the basis of the amounts indicated in the Contract, excluding VAT.

7.4. Sutarties pagrindu Šalies privalomos mokėti netesybos (jei jos nėra įskaitomos) turi būti sumokėtos per 10 (dešimt) kalendorinių dienų nuo joms apmokėti išrašytos sąskaitos – faktūros ar kito dokumento, kuriame pateikiamas reikalavimas sumokėti netesybas, gavimo dienos.

7.5. Jei Tiekėjas nevykdo ar netinkamai vykdo savo įsipareigojimus pagal Sutartį, jis pažeidžia Sutartį. Tiekėjui pažeidus Sutartį, Pirkėjas turi teisę naudotis bet kokiais teisėtais savo teisių gynimo būdais, numatytais Lietuvos Respublikos civiliniame kodekse ir Sutartyje, įskaitant, bet neapsiribojant:

7.5.1. reikalauti tinkamai vykdyti sutartinius įsipareigojimus;

7.5.2. reikalauti sumokėti Sutartyje nustatyto dydžio netesybas ir atlyginti nuostolius;

7.5.3. nutraukti Sutartį Sutartyje nustatyta tvarka.

7.4. The contractual penalties payable by a Party on contractual basis (if not set-off) shall be paid within 10 (ten) calendar days from the date of receipt of the invoice or another document presenting the requirement for payment of the contractual penalties.

7.5. In the event of the Supplier's failure to implement their obligations under the Contract or inadequate implementation thereof, this shall constitute a breach of the Contract. In the event of breach of the Contract by the Supplier, the Buyer shall be entitled to apply any lawful remedies established by the Civil Code of the Republic of Lithuania and the Contract, including, but not limited to:

7.5.1. requiring due performance of contractual obligations;

7.5.2. requiring the payment of contractual penalties of the amount established in the Contract, as well as compensation of losses;

7.5.3. termination of the Contract according to the procedure established hereunder.

8. NENUGALIMOS JĖGOS (FORCE MAJEURE) APLINKYBĖS

8.1. Šalis atleidžiama nuo atsakomybės už Sutarties nevykdymą, jei ji nevykdoma dėl nenugalimos jėgos (force majeure), t. y. aplinkybių, kurių ta Šalis negalėjo kontroliuoti bei protingai numatyti Sutarties sudarymo metu ir negalėjo užkirsti kelio šių aplinkybių ar jų pasekmių atsiradimui. Nenugalima jėga (force majeure) nelaikoma tai, kad Šalis neturi reikiamų finansinių išteklių arba Šalies kontrahentai pažeidžia savo prievoles. Apie nenugalimos jėgos (force majeure) aplinkybių atsiradimą Sutarties Šalys nedelsiant, bet ne vėliau kaip per 5 (penkias) darbo dienas nuo momento, kai sužinojo ar turėjo sužinoti apie tokių aplinkybių atsiradimą, raštu apie tai informuoti kitą Šalį, nurodyti nenugalimos jėgos (force majeure) aplinkybes, ir sutartinius įsipareigojimus, kurių ji negalės vykdyti. Šalis, laiku nepranešusi kitai Šaliai apie nenugalimos jėgos (force majeure) aplinkybes, negali jomis remtis kaip atleidimo nuo atsakomybės už Sutarties nevykdymą pagrindu ir atlyginti kitos Šalies nuostolius, susijusius su negautu ar ne Sutartyje nustatytu terminu gautu pranešimu.

8.2. Esant nenugalimos jėgos (force majeure) aplinkybėms Šalys atleidžiamos nuo savo sutartinių įsipareigojimų vykdymo visam minėtų aplinkybių buvimo laikotarpiui, bet ne ilgiau, kaip 2 (dviem) mėnesiams.

8.3. Jei nenugalimos jėgos aplinkybės tęsiasi ilgiau kaip 2 (du) mėnesius, bet kuri iš Šalių turi teisę vienašališkai, nesikreipdama į teismą, nutraukti šią

8. FORCE MAJEURE EVENTS

8.1. A Party shall be exempted from liability for non-performance of the Contract, in cases where the non-performance of the Contract occurs due to force majeure, i.e., the circumstances beyond control of such Party, which the Party could not have reasonably foreseen at the conclusion of the Contract and could not prevent the occurrence of such circumstances or consequences arising therefrom. The lack of necessary financial resources by the Party or the breach of obligations by the contractors of such Party shall not be regarded as force majeure events. The Parties to the Contract shall inform the other Party of the occurrence of the force majeure event in writing immediately, but no later than within 5 (five) working days from the moment such Party became aware or should have become aware of the occurrence of the force majeure event, indicating the force majeure circumstances and contractual obligations, which the Party will not be able to perform. Upon failure to notify the other Party of the force majeure event in a timely manner, the Party may not rely on such events as grounds for exemption from liability for non-performance of the Contract and shall compensate all losses incurred by the other Party due to the absence of or late notification received in breach of terms prescribed in the Contract.

8.2. In the event of force majeure events, a Party shall be excused from the performance of its contractual obligations for the entire period of existence of the said events, but for no longer than 2 (months).

8.3. Where the force majeure events last for more than 2 (two) months, any of the Parties shall have the right to terminate the Contract unilaterally without referring to the

Sutartį, apie tai įspėjusi raštu kitą Šalį prieš 5 (penkias) kalendorines dienas.

8.4. Nutraukus Sutartį, Šalys privalo ne vėliau kaip per 10 (dešimt) kalendorinių dienų nuo Sutarties nutraukimo dienos atsiskaityti viena su kita ir įvykdyti kitus iki nutraukimo momento kilusius įsipareigojimus.

court, by giving a written notice to the other Party thereof 5 (five) calendar days in advance.

8.4. Once the Contract is terminated, the Parties shall undertake to make settlements with each other and to fulfil their obligations, which arose before the moment of termination of the Contract no later than within 10 (ten) calendar days from the moment of termination of the Contract.

9. MOKĖJIMAI, PINIGINĖS PRIEVOLĖS IR SULAIKYMAI

9.1. Pirkėjas sumoka Tiekėjui iš anksto už visą licencijos galiojimo laikotarpį per 30 (trisdešimt) kalendorinių dienų nuo sąskaitos gavimo dienos.

9.2. Tiekėjas pristatęs Prekes nedelsiant, bet ne vėliau kaip per 2 (dvi) Darbo dienas nuo pristatytų Prekių perdavimo-priėmimo akto pasirašymo pateikia PVM sąskaitą – faktūrą ir pasirašytą Prekių perdavimo-priėmimo aktą Pirkėjui.

9. PAYMENTS, MONETARY OBLIGATIONS AND DETENTION

9.1. The Buyer pays the Supplier in advance for the entire license validity period within 30 (thirty) calendar days from the date of receipt of the invoice.

9.2. Upon delivery of the Goods, the Supplier shall immediately, but no later than within 2 (two) Working days from the signing of the Certificate of Transfer and Acceptance of the delivered Goods, submit a VAT invoice and a signed Cerrtificate of Transfer and Acceptance of the Goods to the Buyer.

9. SUTARTIES PASIRAŠYMAS, GALIOJIMAS IR NUTRAUKIMAS

10.1. Sutartis pasirašoma kvalifikuotais elektroniniais Šalių parašais.

10.2. Ši Sutartis įsigalioja nuo Sutarties pasirašymo dienos ir galioja iki visiško Šalių įsipareigojimų pagal šią Sutartį įvykdymo, bet ne ilgiau kaip 12 mėnesių.

10.3. Šalys turi teisę nutraukti šią Sutartį vienašališkai nesikreipdamos į teismą, apie tai raštu prieš 30 (trisdešimt) kalendorinių dienų informavusi kitą Šalį.

10.4. Sutartis gali būti nutraukta raštišku abiejų Šalių sutarimu.

10.5. Jei viena šalis pažeidžia Sutartį, nukentėjusioji Šalis privalo raštu pateikti pretenziją dėl netinkamo sutartinių įsipareigojimų vykdymo. Jei Sutartį pažeidusi Šalis ilgiau nei 30 (trisdešimt) kalendorinių dienų neatsako į pretenziją ir neištaiso trūkumų, nukentėjusioji Šalis turi teisę vienašališkai nutraukti Sutartį ir reikalauti nuostolių atlyginimo. Tokiu atveju minimaliais nuostoliais laikoma 10 (dešimt) procentų Prekių kainos dydžio suma, kuri sumokama nukentėjusiai Šaliai per 10 (dešimt) darbo dienų.

10.6. Bet kuriuo Sutarties nutraukimo atveju, Pirkėjas per 10 (dešimt) darbo dienų sumoka Tiekėjui už faktiškai pristatytas Prekes.

10.7. Pirkėjas turi teisę nutraukti Sutartį dėl esminio Sutarties pažeidimo iš Tiekėjo pusės, jei Tiekėjas, įskaitant bet kurį su Tiekėju susijusį asmenį, duoda arba

10. SIGNING, VALIDITY AND TERMINATION OF THE CONTRACT

10.1. The Parties shall sign the Contract by: qualified electronic signatures.

10.2. The present Contract shall enter into force from the moment of signature thereof and shall remain effective until complete fulfilment of the contractual obligations of the Parties under the present Contract, however, no longer than 12 months.

10.3. The Parties shall have the right to terminate the present Contract unilaterally without referring to court by giving notice thereof to the other Party 30 (thirty) calendar days in advance.

10.4. The Contract may be terminated by a written agreement between both Parties.

10.5. In case of breach of the Contract by a Party, the injured Party shall undertake to present a written claim regarding undue performance of contractual obligations. If the injuring Party fails to reply to the claim and to rectify defects for more than 30 (thirty) calendar days, the injured Party shall have the right to terminate the Contract unilaterally and to require compensation of losses. In such cases, the minimum amount of losses shall be 10 (ten) percent of the price of Goods, which shall be paid to the injured Party within 10 (ten) working days.

10.6. In any case of termination of the Contract, the Buyer shall pay the Supplier for actually delivered Goods within 10 (ten) working days.

10.7. the Buyer shall be entitled to terminate the Contract due to a substantial breach of the Contract by the Supplier, if the Supplier, including any entity associated with the

pasiūlo (tiesiogiai arba netiesiogiai) bet kuriam Pirkėjo ar Ignitis grupės įmonių darbuotojui bet kokią naudą daikto, piniginio atlygio, komisinių, paslaugų arba kitos materialios ar nematerialios naudos forma, kaip paskatą arba apdovanojimą už bet kurio su šio Pirkimo ar Sutartimi susijusio veiksmo atlikimą arba susilaikymą jį atlikti, arba už palankumo arba nepalankumo parodymą, arba susilaikymą juos parodyti (kyšį) bet kuriam su šia Sutartimi susijusiam asmeniui. Pirkėjui nutraukus Sutartį šiuo pagrindu, Tiekėjas privalo atlyginti Pirkėjui visas patirtas išlaidas, susijusias su Sutarties vykdymo užbaigimu, bei kompensuoti visus dėl Sutartis nutraukimo patirtus nuostolius.

10.8. Paaiškėjus Sutarties 3.2.12 punkte nurodytoms aplinkybėms, Pirkėjas turi teisę sustabdyti Sutarties vykdymą sankcijų galiojimo laikotarpiui ar vienašališkai nutraukti Sutartį raštu informavęs Tiekėją per 1 (vieną) darbo dieną nuo pranešimo apie Sutarties sustabdymą ar vienašališką nutraukimą išsiuntimo dienos, gavęs informaciją apie Subjektų įtraukimą į Sankcijų sąrašus ir/ ar Subjektui pareikštus įtarimus dėl pinigų plovimo, teroristinės veiklos finansavimo ar su mokestiniu sukčiavimu susijusios veiklos. Nutraukus Sutartį ar sustabdžius jos vykdymą šiame Sutarties punkte nurodytu pagrindu, Šalys neturi prievolės viena kitai mokėti baudų, atlyginti žalą ar išmokėti kokias nors kompensacijas, susijusias su Sutarties nutraukimu ar jos sustabdymu, išskyrus Sutartyje nurodytus atvejus.

10.9. Atsižvelgiant į tai, jog Ignitis grupės įmonėms priklauso strateginę reikšmę nacionaliniam saugumui turinčios įmonės bei valdomi įrenginiai, o energetikos sektorius priskiriamas prie nacionaliniam saugumui užtikrinti strategiškai svarbių ūkio sektorių, Pirkėjas pasilieka teisę Sutarties vykdymo metu patikrinti Tiekėjo ir (arba) jo pasitelktų Asmenų atitiktį Lietuvos Respublikos teisės aktams, reglamentuojantiems privalomus nacionalinio saugumo ir kitų strateginių interesų užtikrinimo kriterijus / principus ir (arba) dėl VPĮ 45 straipsnio 2^1 dalyje / PĮ 58 straipsnio 4^1 dalyje ir (arba) VPĮ 37 straipsnio 9 dalyje / PĮ 50 straipsnio 9 dalyje, ir (arba) VPĮ 47 straipsnio 9 dalyje numatytiems reikalavimams. Tuo atveju, jei Sutarties galiojimo metu paaiškėja, jog Tiekėjas neatitinka šių kriterijų / nuostatų / principų ir nustatytų neatitikimų neištaiso per Pirkėjo nurodytą terminą, Pirkėjas įgyja teisę, įspėjęs prieš 10 (dešimt) Dienų, vienašališkai nutraukti Sutartį, neatlygindamas jokių nuostolių, apimant bet neapsiribojant, nuostolius dėl minimalių Pirkimo objekto kiekių išpirkimo.

10.10. Jeigu Tiekėjas pažeidžia Sutarties 3.2.15 punkte nustatytus įsipareigojimus ir tokio pažeidimo neištaiso per Pirkėjo nurodytą terminą, Pirkėjas turi teisę vienašališkai nutraukti Sutartį dėl Tiekėjo kaltės. Nutraukus Sutartį šiuo pagrindu, Tiekėjas privalo Pirkėjui grąžinti Sutarties 2.2.1 p. nurodytą sumą

Supplier, gives or offers any form of an item, pecuniary compensation, commissions, services or other tangible or intangible benefits (directly or indirectly) to any employee of the Buyer or the Companies of Ignitis Group as an incentive or reward for any action or omission taken in relation to this Procurement or the Contract, or for showing favour or disfavour or refraining from doing so (bribe) to any entity associated with this Contract. In the event of termination of the Contract by the Supplier on these grounds, the Supplier shall compensate all costs incurred by the Buyer in relation to finishing of implementation of the Contract as well as compensate all and any losses incurred as a result of termination of the Contract.

10.8. Where the circumstances referred to in paragraph 3.2.12 of the Contract become apparent, the Buyer has the right to suspend the performance of the Contract for the period of validity of sanctions or unilaterally terminate the Contract by notifying the Supplier in writing within 1 (one) working day from the date of dispatch of the notice of suspension or unilateral termination of the Contract upon receipt of information about the inclusion of the Entities in the Sanctions Lists and/or suspected money laundering, terrorist financing or tax fraud activities against Entity. The Parties shall not be obliged to pay each other fines, compensate for damages or pay any compensation related to the termination or suspension of the Contract on the basis specified in this clause of the Contract.

10.9. Taking into account that the companies of Ignitis Group own companies and manage facilities strategically important to national security, and the energy sector is classified as a strategically important for national security, the Buyer reserves the right to, during the performance of the Contract, verify the compliance of the Supplier and/or the persons engaged with the legal acts of the Republic of Lithuania regulating the mandatory criteria/principles for ensuring national security and other strategic interests and/or the requirements laid down in Article 45(2^1) of the LPP / Article 58(4^1) of the LP and/or Article 37(9) of the LPP / Article 50(9) of the LP, ans/or Article 47(9) of the LPP. In an event it becomes known within the validity of the Contract that the Supplier fails to meet those criteria, provisions or principles, and the Supplier fails to eliminate such deficiencies within a term specified by the Buyer, the Buyer shall be entitled to unilaterally terminate the Contract without an obligation to compensate any losses, including but not limited to, losses due to the redemption of the minimum quantities of the Object of the Procurement, by informing the Supplier thereof 10 (ten) Days in advance.

10.10. If the Supplier violates the obligations set forth in paragraph 3.2.15 of the Contract and fails to remedy such violation within the time limit specified by the Buyer, the Buyer shall be entitled to unilaterally terminate the Contract due to the Supplier's fault. Upon termination of the Contract on this basis, the Supplier shall be obliged to refund to the Buyer the

proporcingai nesuteiktų Paslaugų daliai už likusius mėnesius, sumokėti Sutartyje numatytas netesybas bei atlyginti kitus Pirkėjo nuostolius, kurių nepadengia sumokėtos netesybos.

amount specified in paragraph 2.2.1 of the Contract in proportion to the part of the Services not provided for the remaining months, pay the penalties specified therein, and compensate the Buyer for other losses not covered by the penalties paid.

11. KONFIDENCIALI INFORMACIJA

11.1. Šalys susitaria laikyti šią Sutartį, išskyrus jos sudarymo faktą ir teisės aktų pagrindu privalomą viešinti informaciją, ir visą jos pagrindu viena kitai perduodamą ar kitokiu būdu Sutarties vykdymo metu sužinotą / užfiksuotą / nufilmuotą ir pan. informaciją paslaptyje neterminuotai, neatsižvelgiant į tai, ar ta informacija pateikiama žodžiu ar raštu. Šalys susitaria neatskleisti konfidencialios informacijos jokiai trečiajai šaliai be išankstinio raštiško kitos Šalies sutikimo, o taip pat nenaudoti konfidencialios informacijos asmeniniams ar trečiųjų šalių poreikiams, išskyrus atvejus, kai tokia informacija privalo būti atskleista Įstatymo ar kitų teisės aktų nustatyta tvarka ar turi būti atskleista teisės, finansų ar kitos srities specialistui / patarėjui, ar paskolos davėjui.

11. CONFIDENTIAL INFORMATION

11.1. The Parties do hereby agree to keep this Contract confidential indefinitely, except for the fact of conclusion thereof and the information required to be made public on the grounds of the legislations, and all information communicated orally or in writing to each other on the basis of the Contract as well as other information discovered/recorded/filmed, etc. in any other manner within the course of performance of the Contract. The Parties hereunder do hereby agree not to disclose any confidential information to any third persons without a prior written consent of the other Party, and also not to use any confidential information for personal or third-person needs, except for cases when such information must be disclosed under the procedure established by legislation or to a specialist/advisor in the area of law, finance or other area, or to a creditor.

11.2. Visa Pirkėjo Tiekėjui suteikta bei Sutarties vykdymo metu sukurta / sužinota informacija yra laikoma konfidencialia, išskyrus viešai prieinamą informaciją ir Pirkimo sąlygose, visais kitais atvejais Pirkėjas turi patvirtinti raštu, kad tam tikra pateikta informacija nėra konfidenciali.

11.2. All information provided by the Buyer to the Supplier as well as other information developed/discovered within the course of performance of the Contract shall be considered as confidential, except for publicly available information and the Procurement Conditions; in all other cases, the Buyer shall confirm in writing that certain provided information is not confidential.

11.3. Šalis, pažeidusi Sutartyje numatytą konfidencialumo pareigą, įsipareigoja pagal argumentuotą kitos Šalies reikalavimą sumokėti 3 000,00 eurų (trijų tūkstančių eurų 00 euro ct) be pridėtinės vertės mokesčio baudą ir atlyginti visus kitos Šalies patirtus nuostolius, kiek jų nepadengia numatyta bauda.

11.3. The Party infringing the obligation of confidentiality specified in the present Contract, on the basis of a reasonable request of the other Party, shall undertake to pay a fine amounting to EUR 3,000.00 (three thousand euros, 00 ct), exclusive of value-added tax, and to compensate for all losses incurred by the other Party to the extent not covered by the established fine.

11.4. Visą informaciją, gautą Sutarties vykdymo metu, Pirkėjas gali naudoti savo ir / ar bet kurios Ignitis grupės įmonės ar AB „Ignitis grupė“ netiesiogiai ar tiesiogiai kontroliuojančios įmonės naudai ir tikslais, ir tai nebus laikoma Sutarties (konfidencialumo) pažeidimu.

11.4. The Buyer may use the complete information obtained in the course of the execution of the Contract for own benefit and purpose and/or that of any company of AB “Ignitis grupė” or an entity directly or indirectly controlled by AB “Ignitis grupė”, and that shall not be a breach of the Contract (in terms of confidentiality).

12. KITOS SĄLYGOS

12.1. Visi pranešimai, prašymai, pretenzijos ir bet kokia kita informacija tarp Šalių pagal šią Sutartį perduodama raštu ir laikoma tinkamai pateikta, jei įteikiama asmeniškai, siunčiama per kurjerį, registruotu paštu, Sutarties rekvizituose nurodytu elektroniniu paštu ar kitomis priemonėmis, nurodytomis Sutarties rekvizituose.

12. MISCELLANEOUS

12.1. All notices, requests, claims and other information between the Parties hereunder shall be presented in writing and shall be deemed to have been duly presented where they have been served personally, delivered by courier, dispatched by registered post, email address provided in the Contract or by other means indicated in the Contract.

12.2. Tiekėjui yra žinoma, kad AB „Ignitis grupė“ yra išplatinusi finansines priemones, kurios yra įtrauktos į

12.2. The Supplier is familiar with the fact that AB “Ignitis grupė” has issued financial instruments, which are available

prekybą reguliuojamose rinkose NASDAQ OMX Vilnius ir Londono biržose. Atsižvelgiant į tai, AB „Ignitis grupė“ yra emitentas, kuriam, be kitų teisės aktų reikalavimų, taip pat taikomos ir Piktnaudžiavimo rinka reglamento (ES) Nr. 596/2014 nuostatos. Kadangi emitentas gali disponuoti viešai neatskleista informacija (angl. inside information), visiems šią informaciją žinantiems asmenims draudžiama neteisėtai ja pasinaudoti atliekant prekybos AB „Ignitis grupė“ finansinėmis priemonėmis veiksmus arba perduodant šią informaciją bet kuriam asmeniui, kuris neturi teisės su ja susipažinti. Tiekėjas pripažįsta ir sutinka, kad jis ir jo darbuotojai žino apie aptartą reguliavimą ir sutinka visapusiškai laikytis Piktnaudžiavimo rinka reglamento (ES) Nr. 596/2014 nuostatų, tame tarpe, jei taikoma, pareigos sudaryti viešai neatskleistą informaciją žinančių asmenų (angl. *insider list*) sąrašą.

to trade in the regulated markets of NASDAQ OMX Vilnius and London Stock Exchange. Considering the above, AB “Ignitis grupė” acts as an issuer that is subject to, including other relevant legal acts, provisions of the Market Abuse Regulation (EU) No 596/2014. The issuer can dispose of inside information, therefore, all persons who have access to it are prohibited to abuse it when trading financial instruments of AB “Ignitis grupė” or provide such information to any person who does not have the right to access it. The Supplier hereby acknowledges and confirms that it and its employees are familiar with the aforementioned regulation and agrees on all accounts to comply with the provisions of Market abuse regulation (EU) No 596/2014, including, if applicable, the obligation to compile an insider list.

12.3. Kiekviena šalis privalo per 5 (penkias) darbo dienas pranešti kitai Šaliai apie Sutartyje nurodyto adreso, rekvizitų, kontaktinių asmenų pasikeitimą. Iki informavimo apie adreso pasikeitimą, visi šioje Sutartyje nurodytu adresu išsiųsti pranešimai ir kita korespondencija laikomi įteiktais tinkamai.

12.3. Each Party shall undertake to notify the other Party of changes in the address, contact details or contact persons indicated in the Contract within 5 (five) working days. All notices and other correspondence sent to the address indicated in the Contract before the notice of change in the contact details, shall be deemed to have been duly served.

12.4. Šalis neįgyja teisės perduoti savo įsipareigojimų pagal šią Sutartį trečiajam asmeniui be raštiško kitos Šalies sutikimo.

12.4. The Party shall not acquire the right to delegate their contractual obligations under the present Contract to a third person without a written consent of the other Party.

12.5. Sutartis gali būti keičiama rašytiniu Šalių susitarimu, jeigu keitimas neprieštarauja Sutarties arba viešuosius pirkimus reglamentuojančių teisės aktų nuostatoms.

12.5. The Contract may be amended by a written agreement between the Parties, if such amendment thereto is not contrary to the provisions of the Contract or legislations regulating public procurement.

12.6. Vykdant Sutartį, sąskaitos faktūros teikiamos tik elektroniniu būdu. Elektroninės sąskaitos faktūros, atitinkančios Europos elektroninių sąskaitų faktūrų standartą, kurio nuoroda paskelbta 2017 m. spalio 16 d. Komisijos įgyvendinimo sprendime (ES) 2017/1870 dėl nuorodos į Europos elektroninių sąskaitų faktūrų standartą ir sintaksių sąrašo paskelbimo pagal Europos Parlamento ir Tarybos direktyvą 2014/55/ES (OL 2017 L 266, p. 19) (toliau – Europos elektroninių sąskaitų faktūrų standartas), teikiamos, priimamos ir apdorojamos VPĮ 22 straipsnio 3 dalyje / PĮ 34 straipsnio 3 dalyje nustatyta tvarka.

12.6. In course of the performance of the Contract, the invoices shall be presented electronically. E-Invoices, which meet the European Electronic Invoicing Standard, the reference of which was published in the Commission Implementing Decision (EU) 2017/1870 of 16 October 2017 on the publication of the reference of the European standard on electronic invoicing and the list of its syntaxes pursuant to Directive 2014/55/EU of the European Parliament and of the Council (OL 2017 L 266, p.19) (hereinafter referred to as the ‘European Electronic Invoicing Standard’), shall be presented by means chosen by the Supplier. Invoices shall be submitted, accepted and processed following the procedure laid down in Article 22(3) of the LPP / Article 34(3) of the LP.

12.7. Visus Šalių tarpusavio santykius, atsirandančius iš šios Sutarties ir neaptartus jos sąlygose, reglamentuoja Lietuvos Respublikos įstatymai ir kiti teisės aktai.

12.7. All mutual relations between the Parties, arising from the present Contract, which, however, were not discussed hereunder, shall be governed by the laws and other legislations of the Republic of Lithuania.

12.8. Visus ginčus dėl šios Sutarties vykdymo Šalys įsipareigoja spręsti derybomis. Jeigu Šalys šių ginčų negali išspręsti derybomis, jie sprendžiami Lietuvos Respublikos teismuose teisės aktų nustatyta tvarka.

12.8. All disputes arising from the performance of the present Contract shall be resolved by means of negotiation. In the event where the Parties are unable to resolve the disputes by means of negotiation, the disputes shall be resolved before the courts of the Republic of Lithuania according to the procedure laid down by legislations.

12.9. Ne rečiau kaip kartą per metus Tiekėjas įsipareigoja pateikti (i) vidaus kontrolės užtikrinimo ataskaitas informacijos saugos valdysenai pagal IEC/ISO 27001:2022 (angl. International Organization for Standardization) standartą arba lygiavertį arba Pirkėjui, aukščiau nurodytu periodiškumu, sudaro sąlygas informacijos saugos valdysenos audito atlikimui; (ii) vidaus kontrolės užtikrinimo ataskaitas IT valdysenai pagal SOC (angl. Service Organization Control), arba pagal ISAE – 3402 (angl. International Standard on assurance Engagements) arba lygiavertį arba Pirkėjui, aukščiau nurodytu periodiškumu, sudaro sąlygas IT valdysenos audito atlikimui.

12.9. The Supplier undertakes to provide, at least once a year, (i) internal control assurance reports on information security governance in accordance with the IEC/ISO 27001:2022 (International Organization for Standardization) standard, or equivalent, or to enable the Buyer to carry out an audit of information security governance at the frequency specified above;(ii) internal control assurance reports on IT governance in accordance with SOC (Service Organization Control) or ISAE - 3402 (International Standard on assurance Engagements) or equivalent or shall enable the Buyer to audit IT governance at the above frequency.

12.10. Tiekėjas taip pat įsipareigoja nedelsiant, bet ne vėliau kaip per 24 valandas pranešti Pirkėjui apie visus kibernetinius incidentus, susijusius su Pirkėjo tinklų ir informacinėmis sistemomis, kurias vysto ir/ar prižiūri Tiekėjas, kai tik Tiekėjas sužino apie atitinkamą kibernetinį incidentą, ir ne vėliau kaip per 20 dienų nuo įvykusio kibernetinio incidento, pateikti Pirkėjui kibernetinio incidento tyrimo ataskaitą.

12.10. The Supplier also undertakes to notify the Buyer immediately, but not later than within 24 hours, of all cyber incidents involving the Buyer's networks and information systems developed and/or maintained by the Supplier, as soon as the Supplier becomes aware of the cyber incident and to provide the Buyer a report of the investigation of the cyber incident not later than within 20 days of the occurrence of the cyber incident.

12.11. Kai pagal teisės aktus Sutartis turi būti paprastos rašytinės formos, ji gali būti sudaroma tiek surašant vieną šalių pasirašomą (rašytiniu parašu) dokumentą, tiek ir apsikeičiant raštais, telegramomis, telefonogramomis, telefakso pranešimais ar kitokiais telekomunikacijų galiniais įrenginiais perduodama informacija, jeigu yra užtikrinta teksto apsauga ir galima identifikuoti jį siuntusios šalies parašą.

12.11. Where, according to the legislations, the Contract has to be concluded in a simple written form, the Contract may be concluded both by drawing up a single document signed by both parties (in physical signature) and by exchanging certificates, telegrams, telexes, fax messages or the information otherwise transmitted through telecommunication devices, if the security of text has been ensured and the signature of the sending Party may be identified.

12.12. Jei Sutartis sudaroma ją pasirašant fiziniais Šalių parašais, pasirašoma tiek Sutarties egzempliorių, kiek yra Sutarties Šalių. Jei Sutartis sudaroma ją pasirašant kvalifikuotais elektroniniais parašais, Šalys pasirašo vieną Sutarties egzempliorių, perduodamą viena kitai naudojantis telekomunikacijų galiniais įrenginiais. Jei Sutartis sudaroma ją pasirašant skirtingais parašų formatais, Šalys apsikeičia pasirašytais Sutarties egzemplioriais, naudodamosi atitinkamomis apsikeitimo priemonėmis.

12.12. If the Contract is concluded by signing physical signatures of the Parties, the amount of copies shall be signed equal to the number of the Parties of the Contract. If the Contract is concluded by signing it using qualified electronic signatures, the Parties shall sign a single copy, transmitted to each other by telecommunication terminal equipment. If the Contract is concluded by signing it using different formats of signature, the Parties shall exchange the signed copies of the Contract using the relevant exchange measures.

12.13. Kiekvienas šios Sutarties priedas yra neatskiriama jos dalis. Kiekviena Šalis gauna po vieną kiekvieno Sutarties priedo egzempliorių.

12.13. Every Annex to the present Contract forms an integral part thereof. Each Party shall be given one copy of each Annex to the Contract.

12.14. Prie Sutarties pridedami šie priedai:

12.14. Annexes to the Contract are as follows:

12.14.1. Priedas Nr. 1 – Kontaktiniai adresai pranešimams siųsti ir asmenys, atsakingi už sutarties vykdymą, 1 lapas;

12.14.1. Annex 1 – Contact details for Sending of Notices and Persons Responsible for Performance of the Contract, 1 page;

12.14.2. Priedas Nr. 2 – Techninė specifikacija.

12.14.2. Annex 2 – Technical Specification.

12.14.3. Priedas Nr. 3 – Kainos perskaičiavimo sąlygos, 1 lapas.

12.14.3. Annex 3 – Conditions for Recalculation of the Price, 1 page.

12.14.4. Priedas Nr. 4 – Excel lentelė „NFR_template“.

12.14.4. Annex 4 – Excel table "„NFR_template“.

13. ŠALIŲ REKVIZITAI

Tiekėjas
Nossa Data LTD

_____
(pareigos, vardas, pavardė, parašas)

_____
(Sutarties pasirašymo data)

Pirkėjas
UAB „Ignitis grupės paslaugų centras“

_____
(pareigos, vardas, pavardė, parašas)

_____
(pareigos, vardas, pavardė, parašas)

13. DETAILS OF THE PARTIES

Supplier
Nossa Data LTD

_____
(CEO & Company Director, Julianne Flesher, signature)

_____
(*date of signature of the Contract*)

Buyer
UAB ”Ignitis Grupės Paslaugų Centras”

_____
(*position, full name, signature*)

_____
(*position, full name, signature*)

(Sutarties pasirašymo data)	(*date of signature of the Contract*)

Sutarties priedas Nr. 1

KONTAKTINIAI ADRESAI PRANEŠIMAMS SIŲSTI IR ASMENYS, ATSAKINGI UŽ SUTARTIES VYKDYMĄ

1. KONTAKTINIAI ASMENYS

a. Pirkėjo atstovų, kurie bus atsakingi už šios Sutarties vykdyma. užsakymu teikima kontaktai:

b. Tiekėjo atstovų, kurie bus atsakingi už šios Sutarties vykdymą, užsakymų gavimą kontaktai:

Supplier Representative for Signing:

Pranešimai siunčiami:
Užsakymai teikiami:

Sutarties galiojimo metu Pirkėjas turi teisę keisti pranešimų ar (ir) Užsakymų pateikimo būdą ir komunikacijos kanalus, apie tai raštu pranešdamas Tiekėjui.

Tiekėjas
Nossa Data LTD

Pirkėjas

UAB „Ignitis grupės paslaugų centras“

(pareigos, vardas, pavardė, parašas)

(pareigos, vardas, pavardė, parašas)

Annex 1 to the Contract

CONTACT ADDRESSES FOR SENDING OF NOTICES AND PERSONS RESPONSIBLE FOR PERFORMANCE OF THE CONTRACT

1. CONTACT PERSONS

a. Contact details of the representatives of the Buyer, which will be responsible for the performance of the present Contract and for the placement of orders:

b. Contact details of the representatives of the Supplier, which will be responsible for the performance of the present Contract and the receipt of orders:

Supplier Representative for Signing:

Notices shall be sent:
Orders shall be placed:

Throughout the period of the Contract, the Buyer shall have the right to change the manner of submission of notices and/or placement of Orders as well as communication channels notifying the Supplier of such change beforehand in writing.

Supplier
Nossa Data LTD

Buyer

UAB „Ignitis grupės paslaugų centras“

(position, full name, signature)

(position, full name, signature)

Priedas Nr. 3

Perskaičiavimo sąlygos

Kaina Sutarties galiojimo laikotarpiu bus perskaičiuojami (-a) tokiomis sąlygomis:

1. Pirmas perskaičiavimas atliekamas ne anksčiau kaip po 6 mėn. nuo Sutarties įsigaliojimo dienos, vėlesni perskaičiavimai – praėjus ne mažiau kaip 6 mėn. nuo paskutinio perskaičiavimo dienos;
2. Perskaičiavimas atliekamas, jeigu pagal Valstybės duomenų agentūros duomenis Metinės infliacijos dydis pasiekia 10 ar daugiau procentų arba Metinės defliacijos dydis pasiekia -10 ar mažiau procentų ribą (duomenų šaltinis - https://osp.stat.gov.lt/pagrindiniai-salies-rodikliai);
3. Perskaičiavimas atliekamas pagal žemiau pateiktą formulę:

$$C_{pn} = S_n \times (1 + (I - X)/100)$$

C_{pn} – perskaičiuota (-i)Kaina EUR be PVM;

S_n – Sutartyje numatyta (-i)Kaina; EUR be PVM;

I – naujausias paskelbtas Metinės infliacijos arba defliacijos dydis procentais (defliacijos atveju įrašomas su minuso ženklu);

X - defliacijos atveju (-10), infliacijos atveju 10.

4. Perskaičiavimas atliekamas tik Suinteresuotai Šaliai raštu kreipusis į kitą Šalį dėl kainos / įkainių perskaičiavimo:
   - 4.1 Kai Suinteresuota Šalis yra pirkėjas – pirkėjas pateikia pranešimą dėl perskaičiavimo kartu su perskaičiuota (-ais) kaina / įkainiais kitai Šaliai suderinti;
   - 4.2 Kai Suinteresuota Šalis yra tiekėjas – tiekėjas pateikia pirkėjui prašymą dėl perskaičiavimo. Pirkėjas perskaičiuoja kainą / įkainius ir raštu pateikia perskaičiuotą (-us) kainą / įkainius kitai Šaliai ne vėliau kaip per 10 darbo dienų nuo tiekėjo kreipimosi dėl perskaičiavimo dienos.
5. Tiekėjas per 3 darbo dienas turi patvirtinti perskaičiuotą (-us) kainą / įkainius arba raštu pateikti pastabas dėl kainos / įkainių perskaičiavimo. Tiekėjui per 3 darbo dienas raštu nepatvirtinus perskaičiuotos (-ų) kainos / įkainių arba raštu nepateikus pastabų, yra laikoma, kad perskaičiavimui pritarta, o pirkėjo pateiktas pranešimas apie pakeistą (-us) kainą / įkainius įsigalioja, jei pranešime nenurodyta kita, vėlesnė data, ir laikomas neatskiriama Sutarties dalimi. Tiekėjui per nurodytą terminą pateikus pastabas dėl perskaičiavimo, pirkėjas jas išnagrinėja per 3 darbo dienas ir, joms esant pagrįstoms, patikslina perskaičiuotą (-us) kainą / įkainius bei raštu pateikia patikslintus perskaičiuotą (-us) kainą / įkainius tiekėjui pakartotinai suderinti šiame punkte nustatyta tvarka.
6. Už Prekes, užsakytas (-us) iki perskaičiavimo įsigaliojimo, pirkėjas apmoka taikant iki tol galiojusią (-us) kainą / įkainius, o už Prekes / Paslaugas / Darbus, užsakytas (-us) po perskaičiavimo įsigaliojimo, tiekėjui bus apmokama taikant perskaičiuotą (-us) kainą / įkainius.
7. Vadovaujantis Viešųjų pirkimų tarnybos direktoriaus patvirtinta Kainodaros taisyklių nustatymo metodika, esant poreikiui, patikslinama (didėja arba mažėja) Sutarties vertė.

Annex No. 3

Conditions for recalculation

Price will be recalculated during the term of the Contract under the following terms:

1. The first recalculation shall take place no earlier than in 6 months after the date of entry into force of the Contract, and subsequent recalculations shall take place no later than in 6 months after the date of the last recalculation;

2. The recalculation is performed if the Annual Inflation Rate reaches 10 per cent or more or the Annual Deflation Rate reaches the threshold of -10 per cent or less according to the data of the State Data Agency (data source: https://osp.stat.gov.lt/pagrindiniai-salies-rodikliai);

3. The recalculation shall be carried out according to the formula below:

$$C_{pn} = S_n \times (1 + (I - X)/100)$$

C_{pn} – recalculated Price EUR excl. VAT;

S_n – provided in Contract Price; EUR excl. VAT;

I – the latest published Annual Inflation Rate or Deflation Rate in percentage (in the case of deflation, entered with a minus sign);

X - in case of deflation (-10), in case of inflation 10.

4. The recalculation shall only be performed after the Interested Party has contacted the other Party with a request for the recalculation of the price/rates:

4.1 Where the Interested Party is the buyer, the buyer shall submit a request for recalculation along with the recalculated price/rates to the other Party for approval;

4.2 Where the Interested Party is the supplier, the supplier shall submit a request for recalculation to the buyer. The buyer shall recalculate the price/rates and submit the recalculated price/rates in writing to the other Party no later than 10 business days after the date of the Supplier's request for recalculation.

5. The Supplier shall have 3 business days to confirm the recalculated price/rates or to comment in writing on the recalculation of the price/rates. If the Supplier fails to approve or comment in writing on the recalculated price/rates within 3 business days, the recalculated price/rates shall be deemed to have been accepted and the notice of the recalculated price/rates presented by the buyer shall, unless the notice specifies a different, later date, become effective and shall constitute an integral part of the Contract. If the Supplier submits comments on the recalculation within the specified time limit, the buyer shall examine them within 3 business days and, if justified, adjust the recalculated price(s)/rates and submit the adjusted recalculated price(s)/rates in writing to the Supplier for re-approval in accordance with the procedure set out in this clause.

6. The buyer shall pay for the Goods ordered prior to the effective date of the recalculation at the then prevailing price/rates and for the Goods/Services/Works ordered after the effective date of the recalculation, the Supplier shall be paid at the recalculated price/rates.

7. The Contract value shall be adjusted (upwards or downwards) as necessary in accordance with the Methodology for the Determination of the Pricing Rules approved by the Director of the Public Procurement Office.

TECHNINĖ SPECIFIKACIJA

1. SĄVOKOS IR SUTRUMPINIMAI

1.1. **Pirkėjas –** AB „Ignitis grupė“.

1.2. **Tiekėjas –** ūkio subjektas – fizinis asmuo, privatusis juridinis asmuo, viešasis juridinis asmuo, kitos organizacijos ir jų padaliniai ar tokių asmenų grupė, su kuriuo Pirkėjas sudaro Sutartį.

1.3. **Sutartis –** sutartis, sudaroma tarp Pirkėjo ir Tiekėjo dėl Pirkimo objekto.

1.4. **Prekė –** ESG duomenų valdymo platformos prieigos licencija.

2. PIRKIMO OBJEKTAS

2.1. Perkama ESG duomenų valdymo platformos prieigos licencija neribotam naudotojų skaičiui 12 mėnesių laikotarpiui.

2.2. **CDP Premium**

a. CDP šablonas sistemoje
b. 3 kitų pasirinktų įmonių atsakymai – atsakymai susieti su CC, W, F, jei įmanoma
c. Visiems respondentams prieinama informacija apie gaires ir vertinimą, įskaitant žymes prie esminių kriterijų klausimų
d. IFRS S2 suderinimas
e. Praėjusių metų atsakymai susieti su dabartiniu šablonu
f. Praėjusių metų duomenų iš CDP portalo užpildymas
g. Duomenų patikrinimas ir API įkėlimas į CDP portalą, kokybės užtikrinimo patikrinimai

2.3. **ESRS trūkumų analizė ir atskleidimo paketas**

a. Sistemoje esantys šablonai visiems ESRS duomenų taškams, kaip paskelbta EFRAG
b. AI orientuota trūkumų analizė, lyginanti organizacijos atskleidimus (galima įkelti tiek viešų ar privačių dokumentų, kiek norima)
c. Susieta prieiga prie EFRAG priedų dokumentų
d. Reglamentų atnaujinimai, kai EFRAG ir ES paskelbia papildomas gaires, pvz., XBRL, priedo informaciją, audito reikalavimus, EFRAG klausimų ir atsakymų atsakymus, atskleidimo pavyzdžius

2.4. **Individualizuoti ESRS šablonai (iš viso 10 per metus)**

a. Papildomi šablonai, skirti Grupės įmonėms ESO, GEN, IGN, KKJ, REN, VKJ ir (arba) kiti individualizuoti šablonai
b. Gali būti įtraukti arba pašalinti duomenų taškai, remiantis DMA rezultatais, arba įtraukti arba pašalinti ESRS tarpdisciplininiai duomenų taškai (pvz., GRI, ISSB), jei yra reikšmingų duomenų, kurie nėra įtraukti į ESRS

TECHNINĖ SPECIFIKACIJA

1. DEFINITIONS AND ABBREVIATIONS

1.1. **Buyer –** AB „Ignitis grupė“.

1.2. **Supplier –** an economic entity - a natural person, a private legal entity, a public legal entity, other organizations and their subdivisions or a group of such persons with whom the Buyer signs the Contract.

1.3. **Contract –** a Contract concluded between the Buyer and the Supplier regarding the Procurement Object.

1.4. **Good –** ESG data management platform access license

2. PROCUREMENT OBJECT

2.1. ESG data management platform access license is purchased for unlimited users for a period of 12 months.

2.2. **CDP Premium**

a. In-app templates to CDP
b. 3 peer responses - answers mapped where available for CC, W, F
c. Guidance and Scoring information available for all responders, including flags on Essential Criteria questions
d. IFRS S2 Alignment
e. Previous answers mapped to current template
f. CDP Data Pre-fill, where done so by CDP
g. Data verification and API upload to CDP platform, quality assurance checks

2.3. **ESRS Gap Analysis and Disclosure Package**

a. In-app templates for all ESRS Data Point as published by EFRAG
b. AI focused gap analysis versus your disclosure (Can upload as many public or private documents as you like)
c. Linked access to EFRAG appendix documents
d. Regulation updates as EFRAG and the EU publish additional guidelines e.g. XBRL, Appendix information, Audit requirements, EFRAG Q&A Responses, example disclosure

2.4. **Custom ESRS Templates (10 total per year)**

a. Additional templates accounting for groups such as ESO, GEN, IGN, KKJ, REN, VKJ, and/or other custom templates
b. Can include adding or removing datapoints based on DMA outcomes or adding or removing ESRS cross-cutting datapoints (e.g. GRI, ISSB) where you have material data not covered by the ESRS

2.5. **Ability to request the templates below at no additional cost:**

a. Top Employer Questionnaire
b. EU Taxonomy

2.5. **Galimybė be papildomų išlaidų užsisakyti šiuos šablonus:**

a. Top Employer klausimynas
b. ES taksonomija
c. NTAI klausimynas
d. UNGC COP

1. PREKIŲ TEIKIMO VIETA

1.1. Licencija suteikiama nuotoliniu būdu.

2. PREKIŲ PATEIKIMO TVARKA IR TERMINAI

2.1. Licencijos aktyvavimo kodai pateikiami po sutarties pasirašymo, ne vėliau kaip per 30 kalendorinių dienų nuo Sutarties įsigaliojimo dienos.

3. KOKYBĖ IR TRŪKUMŲ PAŠALINIMAS

3.1. Trūkumais laikoma prieigos teisės nebuvimas licencijos galiojimo metu.

3.2. Pirkėjo nustatytiems trūkumams šalinti nustatomas 1 (vienos) darbo dienos terminas.

4. APMOKĖJIMO SĄLYGOS

4.1. Pirkėjas sumoka Tiekėjui iš anksto už visą licencijos galiojimo laikotarpį per 30 (trisdešimt) kalendorinių dienų nuo sąskaitos gavimo dienos.

5. PATEIKIAMI DOKUMENTAI

7.1. Tiekėjas privalo pateikti licencijų aktyvavimo kodus, taip pat privalo būti pateikti 5 naudotojų prisijungimo vardai bei slaptažodžiai.

c. NTAI questionnaire
d. UNGC COP

3. PREKIŲ TEIKIMO VIETA

3.1. License is provided remotely.

4. PROCEDURE AND TERMS OF DELIVERY OF GOODS

4.1. License activation codes are provided after signing the contract, no later than within 30 calendar days from the date of entry into force of the contract.

5. QUALITY AND REMEDY OF DEFECTS

5.1. The lack of access right during the validity of the license is considered as a defect.

5.2. A deadline of 1 (one) working day is set for eliminating defects identified by the Buyer.

6. PAYMENT CONDITIONS

6.1. The Buyer pays the Supplier in advance for the entire license validity period within 30 (thirty) calendar days from the date of receipt of the invoice.

7. DOCUMENTS TO BE SUBMITTED

7.1. The supplier must provide license activation codes, as well as 5 user login names and passwords.

Nr.	Reikalavimas	English	Reikalavimo tipas / Requirement category	Komentarai
NFR-1.1	Paslaugų teikėjo informacijos saugumas turi būti valdomas vadovaujantis ISO/IEC 27001 informacijos saugumo valdymo standartu (toliau - Standartas)	The Service Provider's information security must be managed in accordance with ISO 27001information security management standards.	Reikalavimai paslaugų teikėjui / Requirements for Service Provider	Yes, this can be found here: https://certcheck.ukas.com/certification/793a814b-dc9e-595a-ae6e-f991030441bb
NFR-1.2	Paslaugų teikėjas turi turėti patvirtintą informacijos saugumo politiką (toliau – Politiką) pagal Standarto reikalavimus.	The Service Provider must have an approved information security policy.	Reikalavimai paslaugų teikėjui / Requirements for Service Provider	Yes, Nossa Data has an Information Security Policy that can be provided upon request.
NFR-1.3	Paslaugų teikėjas turi turėti paskirtą už informacijos saugą atsakingą asmenį.	The Service Provider must have a designated person responsible for information security.	Reikalavimai paslaugų teikėjui / Requirements for Service Provider	Yes, the Data Protection Officer, Irina Dumitrescu.
NFR-1.4	Paslaugų teikėjo darbuotojai turi būti supažindinti su informacijos saugumo reikalavimais bei jais vadovautis. Paslaugų teikėjas, Užsakovui pareikalavus privalo pateikti įrodymus, patvirtinančius apie Paslaugų teikėjo darbuotojų susipažinimą su informacijos saugos reikalavimais.	The employees of the Service Provider must be familiar with information security requirements and must adhere to them. The Service Provider, upon request from the Client, must provide evidence confirming that the employees are familiar with these requirements.	Reikalavimai paslaugų teikėjui / Requirements for Service Provider	Yes, Nossa Data can provide upon request.
NFR-1.5	Paslaugų teikėjas ne rečiau kaip vieną kartą per vienerius metus, turi atlikti informacinio saugumo rizikų vertinimą, apimantį visas teikiamas paslaugas. Visoms rizikoms, kurių lygis yra nepriimtinas turi būti parengtas ir Paslaugų teikėjo vadovybės patvirtintas rizikų valdymo priemonių planas. Paslaugų teikėjas, Užsakovui pareikalavus, privalo pateikti ne vėliau kaip prieš vienerius metus atlikto informacinio saugumo rizikų vertinimą, apimantį Užsakovui teikiamas paslaugas.	The Service Provider must conduct an information security risk assessment, covering all provided services, at least once a year. Risk management action plan must be prepared and approved by the Service Provider's management for all unacceptable risks. The Service provider, upon request from the Client, must provide the results of an information security risk assessment, covering the services provided to the Client.	Reikalavimai paslaugų teikėjui / Requirements for Service Provider	02 Risk Assessment: RA-03 Nossa Data will establish a risk assessment program designed to assess the organization's enterprise-level risk on an annual basis or upon significant changes to the environment requiring an update to the risk assessment. This risk assessment will specify Nossa Data's objectives and enable the identification and assessment of risks related to these objectives. As part of the risk assessment process, the organization will document the risk assessment results in Nossa Data's risk registry and/or plan of action and milestones, and will respond to the results in accordance with the organization's risk tolerance.
NFR-1.6	Paslaugų teikėjas turi turėti patvirtintą informacijos valdymo (klasifikavimo, žymėjimo ir naudojimo) tvarką pagal Standarto reikalavimus.	The Service Provider must have an approved information management (Classification, Marking and Use) procedure.	Reikalavimai paslaugų teikėjui / Requirements for Service Provider	Yes, per the System Development Life Cycle (SDLC) Policy
NFR-1.7	Paslaugų teikėjas turi turėti patvirtintas fizinės saugos politiką ir planus, užtikrinančius tinkamą, informacinių išteklių, kuriuose saugoma Užsakovo informacija, fizinę apsaugą, pagal Standarto reikalavimus	The Service Provider must have approved physical security policies and plans to ensure the proper physical protection of the information resources in which the Customer's information is stored.	Reikalavimai paslaugų teikėjui / Requirements for Service Provider	03 Physical Access Control: PE-03 Nossa Data has implemented physical access controls to safeguard the organization's facilities and the equipment therein from unauthorized physical access, tampering, and theft. Physical access controls may include logs, guards, or physical barriers to prevent movement from any publicly accessible areas of a facility to non-public (restricted) areas of the facility.
NFR-1.8	Paslaugų teikėjas turi turėti patvirtintą saugaus informacijos laikmenų utilizavimo tvarką pagal Standarto reikalavimus. Apie laikmenų, kuriose yra Užsakovo informacija, naikinimą turi būti informuojamas Užsakovas ir jam turi būti pateikiamas laikmenų naikinimo protokolas.	The Service Provider must have an approved procedure for the secure information media disposal. The Customer shall be informed of the destruction of media containing the Customer's information and shall be provided with a media destruction report.	Reikalavimai paslaugų teikėjui / Requirements for Service Provider	Yes, can be provided upon request.
NFR-1.9	Paslaugų teikėjas turi turėti parengtas elektroninio pašto, interneto, kompiuterio ir kitų informacinių išteklių naudojimo instrukcijas, taikomas Paslaugų teikėjo darbuotojams, kuriose nurodytos leistino naudojimo ribos.	The Service Provider must have acceptable terms of e-mail, Internet, computer and other information resources usage applicable to the Service Provider's staff, which specify the permitted usage limits.	Reikalavimai paslaugų teikėjui / Requirements for Service Provider	Yes, confirmed.
NFR-1.10	Paslaugų teikėjas turi turėti formalizuotas keitimų ir konfigūracijų valdymo tvarkas ir procesus, apimančius ir teikiamas Klientui paslaugas, užtikrinančius Sistemos pakeitimų planavimą, registravimą ir klasifikavimą, įtakos vertinimą, tvirtinimą, testavimą, vykdymą, atstatymą ir informavimą.	The Service Provider must have documented changes and configuration management procedures and processes, which includes Customer services, to ensure the planning, registration and classification of the System changes, impact assessment, validation, testing, execution, restore and communication.	Reikalavimai paslaugų teikėjui / Requirements for Service Provider	Identifying and recording of significant changes; Planning and testing of changes; Assessment of impacts of change; Formal approval of changes; Verification of security requirements being met; Communication of changes; Fall-back procedures; Emergency change processes; Formal responsibilities to ensure control over changes; and Maintained audit logs of change information.
NFR-1.11	Paslaugų teikėjo informacijos saugumo valdymo sistema (ISVS), rizikų valdymo priemonės ir Klientui teikiamos Paslaugos turi būti kasmet vertinamos nepriklausomų auditorių.	The Service Provider Information Security Management System (ISMS), risk management and Services provided to the Customer must be audited annually by independent auditors.	Reikalavimai paslaugų teikėjui / Requirements for Service Provider	Yes, Nossa Data has independent auditors required as a part of it's ISO-27001 cerification.
NFR-1.12	Paslaugų teikėjas turi turėti patvirtintą saugumo incidentų valdymo tvarką, apimančią ir teikiamas Paslaugas, pagal Standarto reikalavimus.	The Service Provider must have an approved security incident management procedures, which include Customer services.	Reikalavimai paslaugų teikėjui / Requirements for Service Provider	Yes, can be provided upon request.
NFR-1.13	Paslaugų teikėjas turi turėti paskirtą informacijos saugos auditorių, kuris negali būti atsakingas ir už informacijos saugumo priemonių įgyvendinimą, t.y. kontrolės ir sistemos priežiūros funkcijos turi būti atskirtos.	The Service Provider must have an information security auditor who can not be responsible for the implementation of information security policy. Auditing and system maintenance functions must be separated.	Reikalavimai paslaugų teikėjui / Requirements for Service Provider	Yes, this is a responsbility held by the company's CTO, Irina Dumitrescu.
NFR-1.14	Taikomas keitimų ir klaidų taisymo procesas (pataisymai, atnaujinimai, klaidų taisymo paketai) ir versijų valdymas.	Patch and change management (patches, updates and service packs deployed swiftly) and release management must be performed.	Debesijos paslaugos, kai padidintas prieinamumas ar konfidencialumas / Cloud Services with higher availability or confidentiality	Patches are deployed swiftly without service interruption. In the rare unlikely occurence of potential interruption, users would be notified.
NFR-1.15	Programinės įrangos kūrimo ciklo procese turi būti taikomos saugaus programavimo (Angl. Secure Coding) kontrolė spriemonės, aparašytos ISO/IEC 27001 standarte (peržiūros, automatiniai testai, pažeidžiamumų skenavimas ir t.t.).	Secure Coding controls as described in ISO/IEC 27001 (reviews, automated tests, vulnerability scanning, etc.) must be applied in the software development lifecycle.	Reikalavimai paslaugų teikėjui / Requirements for Service Provider	Yes, Nossa Data has an audited ISO 27001 certification confirming this.
NFR-1.16	Tiekėjas turi vykdyti nuolatinį veiklos tęstinumo valdymo testavimą resursams (žmogiškiesiems ir technologiniams), susijusiems su paslaugos teikimu.	The Service Provider must regulary carry out business continuity management tests.	Reikalavimai paslaugų teikėjui / Requirements for Service Provider	Yes, as outlined in Nossa Data's Contingency Planning Policy.
NFR-1.17	Bet kokie Sistemos duomenys ar su Sistema susiję duomenys negali būti perduoti jokiai trečiai šaliai be Užsakovo raštiško sutikimo / leidimo.	Any data from the System or with the System may not be transferred to any third party without the permission / authorization of the Client.	Reikalavimai paslaugų teikėjui / Requirements for Service Provider	Yes, confirmed.
NFR-1.18	Užsakovui turi būti atskleistos bet kokios su Paslaugos teikimo susijusios šalys, jei jos yra ar planuojamos pasitelkti. Saugos ir kvalifikaciniai reikalavimai taip pat yra taikomi visoms paslaugų teikėjo pasitelktoms susijusioms šalims (subrangovams).	The Service Provider must inform the Customer about any related parties involved in the service, if they are or will be used. Safety and qualification requirements also apply to all related parties (subcontractors) engaged by the service provider.	Reikalavimai paslaugų teikėjui / Requirements for Service Provider	Yes, Nossa Data can commit to this and currently does not use subcontractors on this service.
NFR-1.19	Paslaugų teikėjo darbuotojai, kuriems suteikiama prieiga prie Kliento informacijos, privalo pasirašyti konfidencialumo susitarimus.	The Service Provider's employees, who have access to the Customer's information, must sign confidentiality agreements.	Reikalavimai paslaugų teikėjui / Requirements for Service Provider	Yes.
NFR-1.20	Paslaugų teikėjas privalo užtikrinti, kad duomenų laikmenos su Užsakovo informacija nebus perduota tretiesiems asmenims.	The Service Provider must ensure that data storage containing the Client's information will not be transferred to third parties	Reikalavimai paslaugų teikėjui / Requirements for Service Provider	Yes, confirmed.
NFR-1.21	Paslaugos teikėjas privalo užtikrinti, kad Užsakovui skirti resursai (virtualios tarnybinės stotys, virtualus tinklas ir t. t.t.) bus atskirtas nuo kitiems Paslaugų teikėjo klientams skirtų resursų.	Securely Isolating the customer's data (e.g. virtual storage areas, tagging, etc.)	Reikalavimai paslaugų teikėjui / Requirements for Service Provider	Nossa Data segments our environments into a development environment, a staging environment and a production environment. The three environments are connected to entirely different networks within different VPCs and with separate authentication systems, loads balancers, etc, reflecting essential the same architecture three times. Production data can only be queried by authenticated clients and is always filtered by the client's associated company. We hold data in a relational database identified by company and company report ownership. We also separate users by user roles. We always filter all data retrievals by the company it is owned by and this logic is always thoroughly tested through (1) unit tests; (2) end-to-end tests; (3) QA sessions on feature launches in a testing environment. The application uses a single database, along with supplementary data in AWS S3. We have role-based access controls to ensure data is not leaked between tenants (companies) which has high test coverage. Access checks based on database IDs rather than company names.
NFR-1.22	Paslaugų teikėjas turi taikyti principą "Būtina žinoti" t. y. Paslaugų teikėjo darbuotojai turi turėti tik tas prieigos teises, kurios yra būtinos vykdyti tiesiogines funkcijas.	The Service Provider must apply the principle "Need-to-Know", meaning that the employees of the Service Provider should have only the access rights that are necessary to perform their direct functions.	Reikalavimai paslaugų teikėjui / Requirements for Service Provider	Yes, Nossa Data employees are given access to restricted and privileged data on a least privileged basis. This access is reviewed by Management regularly. All production systems access is logged, including any changes made by either developers or business teams.
NFR-1.23	Užsakovui turi būti suteikta galimybė stebėti matuojamus paslaugų lygio parametrus, kurie nustatyti sutartyje.	Customer must be able to monitor measurable parameters as agreed in the SLA	Reikalavimai paslaugų teikėjui / Requirements for Service Provider	Yes, the BCM plan includes: Defined essential business functions; Critical vendors analysis; Defined SLAs; The Contingency Planning procedure.
NFR-1.24	Teikėjas įsipareigoja informuoti Užsakovą apie įvykusį saugos incidentą, dėl kurio buvo pažeistas Užsakovo informacijos vientisumas ar konfidencialumas arba buvo/yra trikdoma teikiama Paslauga nedelsiant, bet ne vėliau kaip per 24 valandas.	Service Provider undertakes to inform the Customer of any security incident that has compromised the integrity or confidentiality of the Customer's information or has disrupted/is disrupting the provided Service immediately, but no later than within 24 hours.	Reikalavimai paslaugų teikėjui / Requirements for Service Provider	Yes, confirmed.
NFR-1.25	Paslaugų teikėjas įsipareigoja teikti Užsakovui visą su įvykusiu kibernetiniu incidentu susijusią informaciją: išsamus incidento, įskaitant jo sunkumą ir poveikį, aprašymas, incidento įvykimo priežastis, taikomos incidento poveikio mažinimo priemonės, žurnaliniai įrašai ir kita su incidentu susijusi Užsakovo paprašyta informacija. Informacija Užsakovui turi būti pateikiama ne vėliau kaip per 1 mėnesį nuo incidento nustatymo momento.	The Service Provider undertakes to provide the Customer with all information related to the occurred cyber incident: a detailed description of the incident, including its severity and impact, the cause of the incident, the measures taken to mitigate the impact of the incident, logs, and any other incident related information requested by the Customer. The information to the Customermust be provided no later than 1 month after the incident identification date.	Reikalavimai paslaugų teikėjui / Requirements for Service Provider	Yes, confirmed.
NFR-1.26	Tiekėjas turi reguliariai informuoti Užsakovą apie saugos rodiklius, IT saugos valdymo sistemos pasikeitimus, saugos incidentus, IS peržiūrų ir įsibrovimo testavimo rezultatus.	Service Providers should regularly notify cloud users about security measures, changes to the IT security management system, security incidents, the results of IS reviews and penetration tests.	Reikalavimai paslaugų teikėjui / Requirements for Service Provider	Details about penetration test results can be provided upon request.
NFR-1.27	Tiekėjas turi reguliariai vykdyti įsibrovimo testavimus.	Service Provider must regulary do penetration tests.	Reikalavimai paslaugų teikėjui / Requirements for Service Provider	Yes, Nossa Data performs penetration tests annually per the ISO-27001 audit.
NFR-1.28	Tiekėjas garantuoja, kad atitinka duomenų apsaugos teisinius reikalavimus, taikomus Lietuvoje ir / ar Europos Sąjungoje.	Service Provider guarantees data protection under Lithuania and / or EU law.	Reikalavimai paslaugų teikėjui / Requirements for Service Provider	Yes, per GDPR requirements available here: https://products.privasee.io/privacy-portal/64d261d0a914ba0013be0d4c
NFR-1.29	Paslaugos teikėjas turi užtikrinti, kad Paslaugos teikimui būtų naudojama tik legali programinė įranga bei visos sistemos aplikacinės ir infrastruktūrinės platformos/bibliotekos būtų su naujausiomis saugos pataisomis, bei užtikrinti, kad aplikacinių ir infrastruktūrinių platformų/bibliotekų versijos būtų palaikomos gamintojų.	The Service Provider must ensure that only legal software is used providing the services. All system application and infrastrukcture platforms/libraries must be up to date with the latest security patches. Additionaly, it must be ensured that the versions of application and infrastructure platforms/libraries are supported by the manufacturer.	Reikalavimai paslaugų teikėjui / Requirements for Service Provider	Yes, confirmed.
NFR-1.30	Užsakovas arba jo įgalioti paslaugų teikėjai turi teisę atlikti Paslaugos teikėjo atitikties šiems saugos reikalavimams auditą. Paslaugos teikėjas įsipareigoja sudaryti sąlygas tokiam auditui atlikti sutarties laikotarpiu ar įvykus dideliam incidentui.	The Client or its authorized service providers have the right to audit the Service Provider's compliance with these security requirements. The Service Provider undertakes to facilitate such an audit during the contract period or in the event of a major incident.	Reikalavimai paslaugų teikėjui / Requirements for Service Provider	Third-party attestation report review; Vendor risk assessment review; Organizational or independent third-party analysis; Organizational or third-party testing; Vendor information security incidents review;. Vendor audit trails and records of information security events, operational problems, failures, tracing of faults and disruptions in service review; Monitor vendor service performance levels against vendor service agreements; and Monitor vendor service capabilities to ensure that agreed service continuity levels are maintained following major service failures or disasters. Yes, if the need is justified upon request, we can do our best to accommodate rights for this audit, but Nossa Data will also need to assess the necessity of the request and the resources required to ensure Nossa Data's capacity is not unfairly constrained.

NFR-1.31	Paslaugų teikėjo duomenų centruose turi būti naudojamos saugumo priemonės prieš kenkimo programinę įrangą (antivirusinė PĮ, Trojan detektorius, anti-spam ir kt.).	Security measures must be used against malware (anti-virus, Trojan detection, anti-spam, etc.) in the Service Provider data centres.	Debesijos infrastruktūros paslaugos / Infrastructure as a Cloud Services	Yes to prohibit unauthorized software use; Implement controls to prevent and detect use of unauthorized software; Implement controls to prevent and detect from known and suspected malicious websites; Implement technical vulnerability management to reduce risk of exploits from vulnerabilities; Conduct regular reviews of software and data content to detect and investigate unauthorized changes; Install and regularly update malware detection and repair software and on a routine basis scan files received over networks, scan mail attachments or downloads, and scan web pages for malware; Define responsibilities in handling malware protection, training on their use, reporting, and recovering from attacks; Develop contingency plans to recover from attacks; Regularly collect information about new malware; Verify information related to malware to ensure it is coming from qualified sources; and Isolate environments where catastrophic impacts may result.
NFR-1.32	Paslaugos teikėjo duomenų centras turi atitikti ne mažesnius nei Tier 3 reikalavimus.	The Service Provider's data center must meet at least Tier 3 requirements.	Debesijos paslaugos / Cloud Services	Yes - Nossa Data services are in AWS.
NFR-1.33	Paslaugų teikėjo duomenų centre turi būti taikoma dviejų faktorių autentifikacija.	There must be used two-factor authentication for access to the Service Provider data centre.	Debesijos paslaugos / Cloud Services	Yes, confirmed.
NFR-1.34	Nuotolinis duomenų centrų administravimas turi būti vykdomas saugiais kanalais (pvz., SSH, TLS/SSL, IPSec, VPN)	Remote administration must be done via a secure communication channel (e. g. SSH, TLS/SSL, IPSec, VPN)	Debesijos paslaugos / Cloud Services	Yes, Nossa Data requires a VPN on at all times.
NFR-1.35	Turi būti naudojamas šifruotas ryšys (SSL/TLS arba lygiavertis) tarp Paslaugų tiekėjo ir Užsakovo	Encrypted communication (e. g. TLS/SSL or alternative) between Cloud Service provider and Cloud Service user must be used	Debesijos paslaugos / Cloud Services	Approved encryption technologies such as Transport Layer Security (TLS) (e.g., TLSv1.2 or higher), Secure Shell (SSH), Secure Socket Layer (SSL), and many other secure data encryption protocols will be utilized when accessing the specified system component.
NFR-1.36	Turi būti naudojamas šifruotas ryšys (SSL/TLS arba lygiavertis) tarp Paslaugų teikėjo nutolusių lokacijų.	Encrypted communication (e. g. TLS/SSL or alternative) between Cloud Service locations must be used	Debesijos paslaugos / Cloud Services	Approved encryption technologies such as Transport Layer Security (TLS) (e.g., TLSv1.2 or higher), Secure Shell (SSH), Secure Socket Layer (SSL), and many other secure data encryption protocols will be utilized when accessing the specified system component.
NFR-1.37	Turi būti naudojamas šifruotas ryšys (SSL/TLS arba lygiavertis) su trečiomis šalimis, kurios reikalingos Paslaugų teikėjui.	Encrypted communication (e. g. TLS/SSL or alternative) must be used with third party providers where these are required for the provider's own offering	Debesijos paslaugos / Cloud Services	Nossa Data will produce, control, and distribute symmetric cryptographic keys using NIST FIPSvalidated or NSA-approved key management technology and processes. Key generation will be seeded from an industry-standard random number generator (RNG).
NFR-1.38	Turi būti daromos reguliarios virtualių serverių, įskaitant jų konfigūraciją, atsarginės kopijos.	Regular backups of virtual servers, including their configuration must be performed.	Debesijos paslaugos / Cloud Services	Yes, confirmed.
NFR-1.39	Duomenys privalo būti visiškai ištrinti Užsakovo pareikalavimu.	Data must be fully and reliably deleted by the customer's request	Debesijos paslaugos / Cloud Services	Yes, this can be done at the client's request.
NFR-1.40	Debesų kompiuterijoje veikiančios Sistemos Administratorių tapatumui patvirtinti turi būti naudojamos dviejų veiksnių tapatumo patvirtinimo priemonės.	Cloud System administrators must be authenticated by two-factor authentication controls.	Debesijos paslaugos / Cloud Services	Yes, confirmed.
NFR-1.41	Sistema turi būti apsaugotos nuo kenkėjiškos programinės įrangos antivirusinės programos pagalba.	The System must be protected form malicious software by using antivirus software.	Debesijos paslaugos / Cloud Services	Yes, confirmed.
NFR-1.42	Autentifikacijai naudoti saugius autentifikacijos protokolus bei standartus (OpenID, JWT, Oauth ar MTLS)	Secure authentication protocols and standards must be used (OpenID, JWT, Oauth or MTLS)	Debesijos paslaugos / Cloud Services	Yes, our authentication system implements secure protocols and standards: - JWT tokens for stateless authentication with configurable expiration - Secure password hashing and session management - Comprehensive audit logging and brute-force protection
NFR-1.43	Duomenys, perduodami tarp integruotų Grupės sistemų, turi būti šifruojami. Šifravimui turi būti naudojama ne žemesnis nei *TLS v1.2* arba *IPSec* tunelis.	Data transitted between integrated systems must be encrypted. Encryption should use not less than TLS v1.2 or an IPSec tunnel.	Debesijos paslaugos / Cloud Services	Nossa Data will protect the confidentiality and integrity of transmitted information. Nossa Data will implement cryptographic mechanisms to prevent unauthorized disclosure of information and detect changes to information during transmission. Nossa Data will maintain the confidentiality and integrity of information during preparation for transmission and during reception. Nossa Data will implement cryptographic mechanisms to protect external messages unless they are otherwise protected by defined alternative physical controls. Nossa Data will ensure rules related to personally identifiable information (PII) processing are enforced in and out of the systems where applicable. Approved encryption technologies such as Transport Layer Security (TLS) (e.g., TLSv1.2 or higher), Secure Shell (SSH), Secure Socket Layer (SSL), and many other secure data encryption protocols will be utilized when accessing the specified system component.
NFR-1.44	Duomenų šifravimui turi būti naudojami skaitmeniniai sertifikatai išduoti patikimų sertifikavimo tarnybų.	Digital sertificates issued by trusted certification authorities must be used for data encryption.	Debesijos paslaugos / Cloud Services	Approved encryption technologies such as Transport Layer Security (TLS) (e.g., TLSv1.2 or higher), Secure Shell (SSH), Secure Socket Layer (SSL), and many other secure data encryption protocols will be utilized when accessing the specified system component.
NFR-1.45	Ryšių su išorinėmis sistemomis šifravimui naudojamų SSL/TLS raktų ilgiai turi būti ne trumpesni nei 2048 bitai. (komunikacija su išore galima taikyti)	For encryption of connection with external systems SSL/TLS key lenght must be 2048 bits or longer	Debesijos paslaugos / Cloud Services	Yes, via AWS Certificate manager our public key is: RSA 2048, with the signature algorithm SHA-256 with RSA
NFR-1.46	Sistemos Tinklo perimetro ugniasienės, turi turėti IDS/IPS.	The perimeter firewalls of the System network must have IDS/IPS.	Debesijos paslaugos / Cloud Services	Nossa Data has network firewalls between external and internal networks, deploying AWS WAF. Nossa Data also establishes a baseline of anticipated data flows, network usage, and network operations for users and systems. Further details can be found in the 02 Boundary Protection and Firewalls: SC-07 section of the System Protection Policy. AWS GuardDuty is also deployed. Our approach to security on the AWS stack is slightly different from the traditional IDS / IPS components, listing below the features we believe relevant from our AWS GuardDuty and AWS WAF components: AWS GuardDuty: - Enabled with comprehensive threat detection - EKS Runtime Monitoring enabled - EKS Audit Logs monitoring enabled - RDS Login Events monitoring enabled - S3 Data Events monitoring enabled AWS WAF (Web Application Firewall) has multiple rulesets including: - Common Rule Set (protects against OWASP Top 10) - IP Reputation List (blocks known malicious IPs) - Known Bad Inputs Rule Set - SQL Injection protection - Linux-specific protection - Admin protection - Applied to both ALB ingress and CloudFront distributions Security Groups (acting as distributed firewalls): - Network-level access control at instance level - Stateful firewall rules for EKS cluster and nodes VPC Network Segmentation:
NFR-1.47	Sistemos ir jos komponentų programinė įranga turi būti periodiškai atnaujinama. Sistemos ir jos komponentų programinės įrangos versijos peržiūrimos ir / arba atnaujinamos ne rečiau kaip kartą per metus.	The System and its components software must be updated periodically. Software versions of the system and its components are reviewed and/or updated at least once a year.	Debesijos paslaugos / Cloud Services	Yes, confirmed.
NFR-1.48	Paslaugų teikėjo duomenų centruose turi būti tinkamai įgyvendintas tinklų segmentavimas (t. y. valdymo potinklis atskirtas nuo duomenų perdavimo tinklo).	Network segmentation must be done in Service Provide's datacenters.	Debesijos paslaugos, kai padidintas prieinamumas / Cloud Services with higher availability	We use AWS VPC's and Security Groups in conjunction with AWS EKS in order to segment our network and control access.
NFR-1.49	Paslaugų teikėjo duomenų centruose turi būti naudojama apsauga nuo paskirtstyto atsisakymo aptarnauti *(angl. Distributed Denial-of-Service, DDoS)*	Protection against DDoS attacks must be used in the Service Provider data centers	Debesijos paslaugos, kai padidintas prieinamumas ar konfidencialumas / Cloud Services with higher availability or confidentiality	Nossa Data has implemented AWS architecture controls to prevent DDoS attacks, which includes a firewall and load balancer specifically designed to mitigate such threats. These network-level controls are part of our defense strategy to ensure the availability of our products and services.
NFR-1.50	Turi būti vykdomas automatinis Kliento programinės įrangos pažeidžiamumų testavimas.	Automated checking of customer applications for application vulnerabilities, particularly before going live.	Debesijos programinės įrangos paslaugos / Software as a Cloud Services	Nossa Data is committed to taking the following steps in the event of detecting a vulnerability in the Services, either through penetration testing or from other methods of discovery: (i) implementing reasonable and appropriate measures designed to detect, prevent, and remediate any identified vulnerabilities and potential threats to the security, integrity, and availability of the Services; (ii) The usage of the Common Vulnerability Scoring System (CVSS) v3.1 to evaluate and prioritize each discovered vulnerability's cybersecurity risk. Vulnerabilities are checked internally by being deployed to a staging environment for testing before going live.
NFR-1.51	Teikėjo palaikymas turi apimti Sistemos programinės įrangos klaidų ar netikslumų registravimą ir kaupimą.	Service Provider support should include registration and accumulation of system software errors or inaccuracies.	Incidentų šalinimas ir palaikymas	Yes, confirmed.
NFR-1.52	Fizinė duomenų saugojimo vieta turi būti Europos Sąjungoje, Jungtinėje Karalystėje arba transatlantinės integracijos kriterijus atitinkančiose šalyse.	The physical location of data (at rest and for processing) must be in the Europe Union, UK or countries, meeting the criteria of transatlantic integration.	Debesijos paslaugos / Cloud Services	Yes, aws-eu-west-2
NFR-1.53	Sistema turi užtikrinti apsaugą, nuo neteisėto prisijungimo prie vidinio kompiuterinio tinklo, pasinaudojant Sistemos programine įranga ar jos moduliais.	The System shall ensure protection against unauthorized access to the internal computer network within system and its modules	Saugumas ir žurnalizavimas/Security and logging	Yes, this is ensured additionally with VPN requirements for employees with access.
NFR-1.54	Sistemos vartotojams, įskaitant privilegijuotus vartotojus, turi būti panaikinta galimybė ištrinti ar keisti žurnalinių įrašų informaciją.	The System shall not allow system users, including administrators, to delete or edit action logs.	Saugumas ir žurnalizavimas/Security and logging	Yes, confirmed.
NFR-1.55	Žurnaliniai įrašai privalo palaikyti Syslog standartą, kad galėtų būti kaupiami nutolusiame žurnalinių įrašų serveryje arba pateikiami. Tuo atveju, jeigu sistemos žurnaliniai įrašai yra kito standarto, saugojami rangovo debesijos duomenų bazėje - incidento atveju sistemos prižiūrėtojas privalo nedelsiant, ne vėliau nei per 24val pateikti su Incidentu susijusius žurnalinius įrašus.	The System logging must support Syslog standard which is required for integration with used logging system.	Saugumas ir žurnalizavimas/Security and logging	n/a
NFR-1.56	Sistemoje turi būti tinkamu formatu fiksuojami šie įvykiai: • Sistemos ir jos modulių, įskaitant audito funkciją, įjungimas, išjungimas ar perkrovimas. • Sėkmingi ir nesėkmingi bandymai prisijungti ir atsijungti. • Visi naudotojų vykdomi veiksmai, apimant veiksmus su duomenimis, naudotojų ar jų grupių bei administratorių teisių naudotis sistemos ištekliais pakeitimus, sistemos parametrų, laiko ir / ar datos pakeitimus ir kitus veiksmus. •Naudotojo paskyros pokyčiai (paskyros sukūrimas, ištrynimas, Administratoriaus teisių suteikimas). •Sistemos tinklo duomenų srauto įrašai (NetFlow, IPFIX, sFlow). •Sistemos saugos įrangos sugeneruoti saugos įvykiai.	The following events must be recorded in the System in an appropriate format: • Enabling, disabling, or reloading the System and its modules, including the audit function. • Successful and unsuccessful attempts to log in and log out. • All actions performed by users, including actions with data, changes in the rights of users or their groups and administrators to access system resources, changes in system parameters, time and / or date, and other actions. •Changes in user accounts (creation of account, deletion, provision of admin rights). •System network flow events (NetFlow, IPFIX, sFlow) •Security equipment generated security logs. • Other events specified by the Customer.	Saugumas ir žurnalizavimas/Security and logging	Yes, confirmed, and we store these events for as long as relevant.

NFR-1.57	Kiekvienas žurnalinis įrašas turi apimti šiuos veiksmus: veiksmą atlikusio naudotojo vardą (prisijungimo identifikatorių), kompiuterio, iš kurio jungtasi informaciją (IP adresas), atliktą veiksmą (turi būti fiksuojamas naudotojo sąsajoje atliktas veiksmas), objektą, su kuriuo atliktas veiksmas, identifikatorių, įvykio rūšį / pobūdį, veiksmo arba įvykio datą ir tikslų laiką, įvykio rezultatą ir kitą informacijos saugai svarbią informaciją (suderintą su Užsakovu). **Reikalavimas apima ir privilegijuotų vartotojų veiksmus.**	Each log entry must include the following actions: the name of the user who performed the action (login identifier), computer IP address, performed action, the identifier of the object on which the action was performed, event type, date and time, event result and any other information critical for information security. The requirement also covers the actions of privileged users.	Saugumas ir žurnalizavimas/Security and logging	Yes confirmed, per the Identification and Authentication Policy.
NFR-1.58	Sistemos administratorius turi galėti peržiūrėti konkrečių audito įrašų informaciją. Sistemos diegimo įgyvendinimo metu Paslaugų teikėjas turės nustatyti ir suderinti, kokia informacija turės būti pateikiama.	Easy review of certain audit records shall be enabled for system administrator. During System installation, the Service Provider shall have to determine and agree with the Customer which information must be provided.	Saugumas ir žurnalizavimas/Security and logging	Yes, confirmed. Information provided confirmed with the client.
NFR-1.59	Sistemoje turi būti realizuota galimybė automatiškai, konfigūruojamu periodiškumu perduoti Sistemos kaupiamus žurnalinius įrašus į esamoje Užsakovo IT infrastruktūroje veikiantį informacijos ir įvykių valdymo (SIEM) sprendimą, suderintą diegimo projekto analizės ir projektavimo metu.	The System shall allow automatic transfer of System's stored logs at adjustable regularity to the Security Information and Event Management tool used in the existing infrastructure of Contracting Authority, as agreed during implementation project analysis and design phases.	Saugumas ir žurnalizavimas/Security and logging	Optional
NFR-1.60	Žurnaliniai įrašai turi būti saugomi ne trumpiau kaip 90 kalendorinių dienų	Logs must be stored for at least 90 days.	Saugumas ir žurnalizavimas/Security and logging	Yes, confirmed.
NFR-1.61	**Sistemoje neturi būti galimybės saugoti ir registruoti jautrios ir / ar konfidencialios informacijos apie sistemos vartotojus, tokios kaip vartotojo slaptažodis, asmens kodas atviru tekstu.**	The System shall prevent saving and recording sensitive and/or confidential information on system users, such as user password, personal code, in open text.	Saugumas ir žurnalizavimas/Security and logging	Information sharing agreements shall identify the requirements deemed necessary for protecting confidential information; and agreements between Nossa Data and vendors or suppliers contain requirements to address information security risks associated with the services and products being provided to Nossa Data. The only user PII we store are full name and email, required for authentication. These are stored in plaintext in our encrypted database. Passwords are always hashed, we never store a password in plaintext. Confidential information pertaining to the company is stored in plaintext in our encrypted database.
NFR-1.62	Sistemoje administratoriui turi būti galimybė šalinti pasirinktus jautrius ir / ar konfidencialius duomenis, kurių nėra privaloma kaupti / kurie nėra reikalingi tolimesniam sėkmingam Sistemos darbui (pvz. asmeninę naudotojų informaciją).	System shall allow system administrators to delete the selected sensitive and/or confidential data whose storage is not obligatory / which is not required for further successful System operation (such as personal information of users).	Saugumas ir žurnalizavimas/Security and logging	Yes, confirm. Assistance with back-end deletion can also be provided upon request.
NFR-1.63	Sistemoje turi būti galimybė įjungti ir išjungti auditavimą (Audit Trail) nestabdant ar kaip kitaip neįtakojant nepertraukiamo sistemos veikimo.	The System shall allow switching on/off the Audit Trail without stopping or otherwise interfering continuous system operation.	Saugumas ir žurnalizavimas/Security and logging	Yes, confirmed.
NFR-1.64	Kiekvienas sistemos komponentas turi turėti atskirą žurnalizavimo konfigūraciją.	Each system module or component must support its individual logging configuration	Saugumas ir žurnalizavimas/Security and logging	Yes, confirmed. Identification and Authentication Policy can also be provided upon request.
NFR-1.65	Sistema turi turėti bent 3 skirtingus žurnalizavimo lygius: - įspėjimai ir klaidos - visos klaidos, išskilusios sistemoje dėl jos veiklos ar integracijų - informacinis - pradžia ir pabaiga kiekvienos transakcijos, integracijos su kitais sistemos komponentais ir sistemomis - debug - detalus visų veiksmų žurnalas, kuris pateikia visus input ir output parametrus, procedūras, sąsajas, DB iškvietimus, logines operacijas.	System must support at least 3 levels of logging: - warnings & errors - all errors and warning due to system performance or integrations must be logged; - informational - beginning and ending of each transaction, log entries with other system components and other systems; - debug - all details to reveal internals of business logic and connectivity. This includes IN, OUT parameters of procedure, web service, DB calls, all conditional decisions, etc.	Saugumas ir žurnalizavimas/Security and logging	Yes, system supports these where relevant based on user actions.
NFR-1.66	Žurnalų įrašai turi turėti unikalų identifikatorių, pagal kurį būtų galima identifikuoti ir surišti transakcijas tarp sistemų (end to end)	Log entries must have identifiers which allow to track unique transactions across all the Systems (end to end)	Saugumas ir žurnalizavimas/Security and logging	Yes, log entries have unique identifiers, but transactions do not take place on the system.
NFR-1.67	Sistemos fiksuojami žurnaliniai įrašai turi būti saugomi atskiroje, specializuotoje ir tam pritaikytoje techninėje ar programinėje įrangoje.	System log records must be stored on separate, specialized, and appropriately designed hardware or software.	Saugumas ir žurnalizavimas/Security and logging	Nossa Data uses aws-eu-west-2 for storage requirements.
NFR-1.68	Visų Sistemos architektūros modelio lygių sisteminis laikas turi būti sinchronizuotas su laiko žymių serveriu *(angl. Network Time Protocol, NTP)* **ne mažiau kaip vienos sekundės tikslumu.**	The System time for all System level architectural models must be synchronized with the Network Time Protocol.	Saugumas ir žurnalizavimas/Security and logging	Nossa Data utilizes its cloud provider services to synchronize system clocks within and between system components. Nossa Data's cloud provider ensures their internal system clocks are compliant with ISO-27001.
NFR-1.69	Sistemoje turi būti galimybė nustatyti žiemos / vasaros laiką (angl. Daylight Saving Time) ir atitinkamai automatiškai pakeisti taikomą laiką, nedarant įtakos Sistemos veiklai.	The System must be able to set the Daylight Saving Time and automatically change the applicable time without affecting the operation of the System.	Saugumas ir žurnalizavimas/Security and logging	Time is automatically adjusted to the user's location.
NFR-1.70	Sistemos komponentai turi būti stebimi kenkėjišką programinę įrangą aptinkančia programine įranga.	Antivirus software must be centrally managed.	Saugumas ir žurnalizavimas/Security and logging	Yes, confirmed. It is managed by Nossa Data's CTO.
NFR-1.71	Sistemoje nenaudojami fiziniai ir / arba loginiai prievadai turi būti išjungti.	Unused physical and logical ports in the system must be disabled.	Saugumas ir žurnalizavimas/Security and logging	Employees perform all their work on Nossa Data issued laptops, which are all enrolled in Jumpcloud MDM. We ensure via Jumpcloud that all USB ports are disabled and do not allow any data transfers. Only specific ports (e.g. 443 for https) are enabled.
NFR-1.72	Sistemoje naudojami fiziniai ir loginiai prievadai, protokolai turi būti dokumentuoti.	Physical and logical ports and protocols used in the System must be documented.	Saugumas ir žurnalizavimas/Security and logging	We disable all USB ports, disabling data transfers. We allow employee laptops access to ports for power and monitor only. All employee laptops have strong passwords enforced, and a 5 minute auto-lock window. Only specific ports (e.g. 443 for https) are enabled.
NFR-1.73	Perduodami įvykiai iš Komponento į centralizuotą įvykių registrą ir arba SIEM, turi būti šifruoti patikimais šifravimo algoritmais.	Logs transmitted to Client's SIEM must be encrypted using reliable encryptio algorithms.	Saugumas ir žurnalizavimas/Security and logging	Optional
NFR-1.74	**Šifravimui naudojama programinė ir aparatinė įranga turi gebėti saugiai sutrikti (angl.** *fail securely*).	Software and harware used for encryption must be able to fail securely.	Saugumas ir žurnalizavimas/Security and logging	Importing and exporting of hardware and software that performs or is designed to perform cryptographic functions; Restricting of usage of encryption where applicable; Utilizing mandatory and discretionary methods for country access to encrypted information by hardware and software providing content confidentiality; and Confirming compliance with requirements (e.g., FIPS 140-2 standards) as applicable. Yes: our data is stored encrypted and requires the encryption key to be working.
NFR-1.75	Šifravimo algoritmas turi neturėti žinomų pažeidžiamumų sistemos diegimo ir viso sistemos eksploatacijos metu.	The encryption algorithm must not have known vulnerabilities during system deployment	Saugumas ir žurnalizavimas/Security and logging	We use standard industry-wide encryption algorithms not known to have any vulnerabilities. Our approach to security focuses on using the best industry standard, as this gets some of the most attention for potential vulnerabilities from security researchers.
NFR-1.76	Sistemos pažeidžiamumai turi būti matuojami pagal tarptautinę CVSS klasifikavimo skalę https://web.nvd.nist.gov/view/vuln/search). Kritinė reikšmės pažeidžiamumai - tokie pažeidžiamumai kuriems yra priskirti 9,0-10,0 balų pagal tarptautinę CVSS klasifikavimo skalę. Svarbios reikšmės pažeidžiamumai - tokie pažeidžiamumai, kuriems yra priskirti 7,0-8,9 balai pagal tarptautinę CVSS klasifikavimo skalę. Vidutinės reikšmės pažeidžiamumai -tokie pažeidžiamumai, kuriems yra priskirti 4 - 6,9 balai pagal tarptautinę CVSS klasifikavimo skalę. Žemos reikšmės pažeidžiamumai - tokie pažeidžiamumai, kuriems yra priskirti 0,1 - 3,9 balai pagal tarptautinę CVSS klasifikavimo skalę.	System vulnerabilities are measured using the international CVSS grading scale https://web.nvd.nist.gov/view/vuln/search. Critical Vulnerabilities are those vulnerabilities that are assigned 9.0-10.0 points according to the international CVSS classification scale. Important vulnerabilities are those vulnerabilities that are assigned 7,0-8,9 points according to the international CVSS classification scale. Medium-level vulnerabilities are those vulnerabilities that are assigned 4,0-6,9 points according to the international CVSS classification scale. Low-level vulnerabilities are those vulnerabilities that are assigned 0,1-3,9 points according to the international CVSS classification scale.	Saugumas ir žurnalizavimas/Security and logging	Nossa Data is committed to taking the following steps in the event of detecting a vulnerability in the Services, either through penetration testing or from other methods of discovery: (i) implementing reasonable and appropriate measures designed to detect, prevent, and remediate any identified vulnerabilities and potential threats to the security, integrity, and availability of the Services; (ii) The usage of the Common Vulnerability Scoring System (CVSS) v3.1 to evaluate and prioritize each discovered vulnerability's cybersecurity risk; (iii) expediting remediations accordingly as a business priority, based on their severity. Yes we use the CVSS severity rating to assess the SLA of our cybersecurity vulnerabilities. Nossa Data is committed to taking the following steps in the event of detecting a vulnerability in the Services, either through penetration testing or from other methods of discovery: (i) implementing reasonable and appropriate measures designed to detect, prevent, and remediate any identified vulnerabilities and potential threats to the security, integrity, and availability of the Services; (ii) The usage of the Common Vulnerability Scoring System (CVSS) v3.1 to evaluate and prioritize each discovered vulnerability's cybersecurity risk; (iii) expediting remediations accordingly as a business priority, based on their severity. The SLAs are as follows: Critical Severity: remediation assumed to be delivered immediately, no later than within 3 business days; High Severity: remediation assumed to be delivered within 5 business days; Medium Severity: remediation assumed to be delivered within 30 business days; Low Severity: remediation assumed to be delivered within 45 business days.
NFR-1.77	Tiekėjas privalo per dieną nuo pažeidžiamumo nustatymo dienos parengti pataisą, skirtą kritiniam pažeidžiamumui pašalinti, arba pažeidžiamumo mažinimo planą. Tiekėjas privalo per savaitę nuo pažeidžiamumo nustatymo dienos parengti pataisą, kad būtų pašalintas itin svarbus pažeidžiamumas, arba pažeidžiamumo mažinimo planą. Tiekėjas turi atlikti kitų pažeidžiamumų pašalinimo pataisas, reguliariai atnaujindamas sistemą ar sistemos komponentus.	The Supplier must make a patch for elimination, or vulnerability mitigation plan of Critical Vulnerability per day after vulnerability was identified. The Supplier must make a patch for elimination, or vulnerability mitigation plan of High Criticality Vulnerability per one week after vulnerability was identified. The Supplier must make a patch for elimination of other Vulnerabilities with a regular system or system components update.	Saugumas ir žurnalizavimas/Security and logging	Nossa Data will establish a Vulnerability Monitoring and Scanning Program designed to monitor and scan for internal and external vulnerabilities in systems and hosted applications at least monthly (or more randomly) to identify, quantify, and prioritize vulnerabilities. Nossa Data will also ensure that all findings from vulnerability scans are analyzed and documented on a monthly basis and are remediated in accordance with the organization's risk tolerance. Nossa Data will also ensure that effective vulnerability management processes are in place that include: ● The identification of associated risks and the actions to be taken once a potential technical vulnerability has been identified; ● The technical vulnerability monitoring process should be regularly monitored and evaluated in order to ensure its effectiveness and efficiency; ● The prioritization of remediation of vulnerabilities on systems at high risk; ● A defined procedure to address the situation where a vulnerability has been identified but there is no suitable countermeasure. In this situation, the organization should evaluate risks relating to the known vulnerability and define appropriate detective and corrective actions; ● Defined and established roles and responsibilities associated with technical vulnerability management, including vulnerability monitoring, asset tracking, and any coordination responsibilities required; and ● Alignment of the change management process and the incident response process
NFR-1.78	Sistemoje naudotojas turi patvirtinti savo tapatybę slaptažodžiu arba kita Sistemos reikalavimuose numatyta autentiškumo patvirtinimo priemone. Sistemoje pateikiamą informaciją gali matyti ir veiksmus atlikti tik autentifikavęsi naudotojai.	System user must confirm his/her identity by password or using other authentication mean according to System requirements. Only authenticated users shall see the information provided in the System and will be able to perform actions.	Vartotojų autentikavimas, autorizavimas ir valdymas/Users authentication authorization and administration	Yes, confirmed.
NFR-1.79	Sistemos naudotojų autentifikavimas, autorizavimas ir naudotojų valdymas turi būti realizuotas vaidmenų (angl. Role Based Access Control - RBAC) pagrindu. Naudotojų kūrimas, autorizavimas, autentifikavimas ir teisių valdymas turi būti valdomas centralizuotai visiems Sistemos architektūros modelio lygiams.	System authorization mechanism shall be implemented on the basis of Role-based Model and managed centrally for all levels of System architecture model. User creation, authorisation, authentication and rights management shall be centrally managed for all levels of the System Architecture Model.	Vartotojų autentikavimas, autorizavimas ir valdymas/Users authentication authorization and administration	Yes confirmed. Nossa Data also implements the least privileges to employees based upon their roles within the organization.
NFR-1.80	Sistemoje turi būti galimybė valdyti naudotojų prieigos teises suteikiant skirtingas roles ar teisių grupes, vadovaujantis principu – „būtina žinoti"	The System must have the capability to manage user access rights by assigning different roles or permission groups, folowing the principle "need-to-know".	Vartotojų autentikavimas, autorizavimas ir valdymas/Users authentication authorization and administration	Yes, confirmed. There are different levels of access based on level of access required.
NFR-1.81	Sistemoje pagal įvedamo teksto pradžią neturi būti galimybės automatiškai užpildyti jautrių ir / ar konfidencialių informacijos laukų, pvz. įvedus pirmus tris slaptažodžio simbolius Sistema negali automatiškai užpildyti likusių slaptažodžio simbolių.	System shall prevent autofilling of sensitive and/or confidential data fields after beginning of the text is entered, for example, when three first password characters are entered, the System shall not autofill the rest password characters.	Vartotojų autentikavimas, autorizavimas ir valdymas/Users authentication authorization and administration	There is no autofilling of sensitive and/or confidential data fields. Inputs have to be manually typed in and are then tracked for users to find.
NFR-1.82	Sistemoje turi būti realizuota duomenų mainų sąsaja su Ignitis grupės Microsoft Active Directory Domain Services Ignitis grupės įmonių naudotojų autentifikavimui Sistemoje.	Autentification of system users must be implemented using Ignitis Group's MS Active Directory.	Vartotojų autentikavimas, autorizavimas ir valdymas/Users authentication authorization and administration	Currently not possible and seen as something that is potentially possible once SSO is implemented
NFR-1.83	Turi būti galimybė prisijungti prie Sistemos be pakartotinio naudotojo duomenų suvedimo (angl. *Single Sign-On*) , jei naudotojas autentifikavosi Ignitis grupės Microsoft Active Directory Domain Services profilio dėka.	The System shall allow Single Sign-On, if user has authenticated him/herself through Client's Microsoft Active Directory Domain Services profile.	Vartotojų autentikavimas, autorizavimas ir valdymas/Users authentication authorization and administration	SSO will be available at Nossa Data within 2025.

NFR-1.84	Suspendavus naudotoją Ignitis grupės Microsoft Active Directory Domain Services paslaugoje, naudotojas turi būti suspenduotas Sistemoje.	When the user is suspended in the Client's Microsoft Active Directory Domain Services service, the user has to be suspended in the System as well.	Vartotojų autentikavimas, autorizavimas ir valdymas/Users authentication authorization and administration	Currently not possible and seen as something that is potentially possible once SSO is implemented
NFR-1.85	Sistemoje turi būti galimybė naudotojui priskirti daugiau nei vieną rolę, išskyrus administravimui priskirtą rolę. Sistemoje administravimo funkcijai atlikti turi būti sukuriama/naudojama atskira unikali paskyra pagal Ignitis grupės paskyrų kūrimo taisykles.	The System shall allow assigning more than one role to a user. A separate unique account must be created/used in the system for the administration function in accordance with the Ignitis group account creation rules.	Vartotojų autentikavimas, autorizavimas ir valdymas/Users authentication authorization and administration	Nossa Data has set user permissions per user in accordance with Ignitis Group requests. From the definition of a "role" a user can only have one level of access. However, the Topic Lead level of access is built to have access in a customisable way, whereby an admin can modify a user's access to be different on different ESG reports.
NFR-1.86	Sistemos naudotojas turi galėti peržiūrėti tik tokią informaciją ir naudotis tik tokiomis funkcijomis, kurios yra nustatytos priskirtomis prieigos teisėmis (pvz., jei Sistemos naudotojas nori peržiūrėti informaciją, Sistema turi pranešti, kad naudotojas neturi teisių peržiūrėti tam tikrų duomenų ar kitais būdais apriboti informacijos peržiūrą ir pan.).	System user shall be able to view only such information and use only such functions that are assigned to access rights (e.g.., if System user wants to view certain information, the System shall notify that the user has no rights to view certain data or otherwise restrict information display, etc.).	Vartotojų autentikavimas, autorizavimas ir valdymas/Users authentication authorization and administration	This depends on the level of access of a user. Some users will not be able to see any questions where admins explicitly do not want them to see information.
NFR-1.87	Sistemos funkcionalumas turi leisti nedelsiant sustabdyti arba nustatyti galiojimo terminą konkretaus naudotojo ar naudotojų grupės rolėms/prieigos teisėms (t. y. rolės/prieigos teisės nedelsiant/arba suėjus nustatytam terminui turi tapti negaliojančios).	The System shall allow stopping of role validity and automatic cancelation of associated functions and access for role user.	Vartotojų autentikavimas, autorizavimas ir valdymas/Users authentication authorization and administration	Yes, confirmed.
NFR-1.88	Sistemoje turi būti galimybė kurti naujus, keisti ir šalinti esamas roles bei jų prieigos teises. Pakeitus esamų rolių teises, šios turi būti realiu laiku pritaikomos naudotojams, kuriems priskirtas su pakeitimu susijusi rolė.	The System shall allow to create new, modify and delete existing roles and their access rights. When rights of existing roles are modified, these in real time have to be applied to users assigned with such role.	Vartotojų autentikavimas, autorizavimas ir valdymas/Users authentication authorization and administration	Yes, confirmed. Nossa Data can allow for this for Colalborators and Topic Leads invited to the system.
NFR-1.89	Kiekvienas sistemos naudotojas turi būti unikaliai identifikuojamas ir autentifikuojamas.	All accounts of the System must be uniquely identified and authenticated	Vartotojų autentikavimas, autorizavimas ir valdymas/Users authentication authorization and administration	Nossa Data must ensure that parties accessing organizational systems are assigned unique usernames and authenticators.
NFR-1.90	Sistemos administratorius turi turėti galimybę užblokuoti visus vieno ar kelių kitų naudotojų veiksmus, pateikiant naudotojo sąsajoje informaciją, kad veiksmų su Sistema tam tikru metu atlikti nėra galimybės.	System administrator must have possibility to block activities of one or more users by providing notification in user's interface that no activity in the System can be performed during certain period.	Vartotojų autentikavimas, autorizavimas ir valdymas/Users authentication authorization and administration	Yes, confirmed. Admin users can block activities and set timelines for Collaborator users.
NFR-1.91	**Sistemos administratorius turi turėti galimybę atjungti (angl.** *force stop* **) iš Sistemos pasirinktą prisijungusį naudotoją, t.y. turi būti galimybė nutraukti pasirinkto naudotojo darbo sesiją su Sistema.**	System's administrator must have possibility to force stop selected logged-in user, i.e. the System shall have the capability to terminate selected user's work session in the System.	Vartotojų autentikavimas, autorizavimas ir valdymas/Users authentication authorization and administration	Yes, confirmed.
NFR-1.92	Sistemoje turi būti galimybė automatiškai užrakinti (angl. Lock arba Lock Screen) ir / arba užbaigti naudotojų darbo sesiją, jei neveikimo laikas viršija nustatytą trukmę (15 minučių).	The System shall have automatic Lock or Lock Screen and/or user work session termination function when inactive period exceeds preset duration (15 minutes).	Vartotojų autentikavimas, autorizavimas ir valdymas/Users authentication authorization and administration	Inactive sessions will be terminated after a defined period of time. Session tokens are refreshed for active sessions, but they expire after 7 days of inactivity. This can be reduced depending on future client requests.
NFR-1.93	Sistemoje turi būti galimybė nustatyti naudotojų darbo sesijų trukmę.	The System shall allow setting duration of user work session.	Vartotojų autentikavimas, autorizavimas ir valdymas/Users authentication authorization and administration	Yes, confirmed.
NFR-1.94	Turi būti užtikrinta, kad vienu metu ir tuo pačiu prisijungimo vardu į Sistemą gali jungtis tik vienas autenfikuotas vartotojas. Vieningo prisijungimo (angl. Single Sign-On) funkcionalumas traktuojamas kaip viena ir ta pati sesija.	The System shall allow only one work session at the same time for one unique user. Single Sign-On functionality is treated as one and the same session.	Vartotojų autentikavimas, autorizavimas ir valdymas/Users authentication authorization and administration	SSO is planned for deployment in 2025.
NFR-1.95	Jei tiekėjo pateiktame funkcionalume bus numatyta, kad prie informacinės sistemos galės jungtis išoriniai (ne vidinio tinklo) naudotojai, jų prisijungimui turi būti taikomi šie minimalūs reikalavimai: 1. Slaptažodžiai privalo būti sudaryti iš mažųjų ir didžiųjų raidžių, skaičių ir/arba specialiųjų simbolių. 2. Vartotojų slaptažodis turi būti sudarytas iš mažiausiai 8 simbolių, administratorių slaptažodžiai privalo būti sudaryti iš mažiausiai 12 simbolių. 3. Slaptažodis privalo būti reguliariai keičiamas, t. y. ne rečiau kaip 90 dienų laikotarpyje. 4. Laikini arba pradiniai slaptažodžiai privalo būti pakeisti pirmo prisijungimo metu. 5. Slaptažodžiai negali būti naudojami tokie patys, kokie buvo naudoti 6 mėnesių laikotarpyje. 6. Buvę 6 slaptažodžiai negali būti pakartotiniai naudojami to pačio vartotojo. 7. Didžiausias leistinas mėginimų įvesti teisingą slaptažodį skaičius yra 5 kartai. 8. Slaptažodžiai saugomi sistemose privalo būti užšifruoti. Šifravimui naudojamas vienpusio šifravimo algoritmas. 9. Draudžiama techninėje ir programinėje įrangoje naudoti gamintojo nustatytus slaptažodžius, jie turi būti pakeisti į atitinkančius reikalavimus. 10. Draudžiama naudoti prisijungimo duomenų saugojimą naršyklėse 11. Keičiant slaptažodį, vartotojas privalo pateikti seną ir naują slaptažodį.(minimo funkcijai). 12. Draudžiama įvedamą slaptažodį rodyti įvedimo lauke (privaloma maskuoti).	In case the functionality provided by the Service Priovider will allow login to the information system for outside users (external network), the following minimum requirements shall be applied for their login: 1. Passwords shall consist of small and capital letters, numbers and/or special characters. 2. User's password shall consist of at least 8 characters, administrator's password shall consist of at least 12 characters. 3. A password has to be regularly changed, with maximum period of 90 days. 4. Temporary or initial passwords have to be changed during the first login. 5. Passwords can not be used the same which were used within the period of 6 months. 6. The former 6 passwords can not be reused by the same user. 7. The maximum correct password attempts shall be 5. 8. Passwords stored in the systems have to be encrypted. Unidirectional encryption algorithm shall be used. 9. Use of manufacturer's set passwords in hardware and software is prohibited, they have to be changed according to requirements. 10. User must provide old and new password during password change. 11. User has to be asked for additional authentication when email address is changed (applicable if IS uses email address for password remind function). 12. Password display in input field is prohibited (it has to be masked).	Vartotojų autentikavimas, autorizavimas ir valdymas/Users authentication authorization and administration	Enforce the following password composition and complexity rules: o A minimum password length of eight (15) alphanumeric characters for nonprivileged users; Appropriate password complexity, including the use of both upper- and lowercase letters, at least one (1) special character (e.g., $%^&*()_+|~-=\`{}[]:";'<>?,./) or at least one (1) number (e.g., 0-9); Prohibition of the use of consecutive identical numeric or alphabetic characters; o Prohibition of passwords that are vulnerable to dictionary attacks; and o Prohibition of passwords containing the user's name, date of birth, or telephone number; Change or refresh passwords: o Every 90 days, o When compromised, o After the first login o5: & 6: Unmet o7: The maximum password attempts before locking an account is 6. o8: Hashes of passwords are stored on the system, not the original password o9: Yes, confirmed. o10: If a user forgets a password, in this situation a user will have to confirm forgetting a password through a verified email. o11: Email address changes require communications with Nossa Data. o12: Yes, confirmed.
NFR-1.96	Sistema turi būti apsaugota nuo dešimities naujausių per tinklą vykdomų atakų (angl. TOP 10), kurių sąrašas skelbiamas Atviro tinklo programų saugumo projekto *(angl. The Open Web Application Security Project (OWASP))* interneto svetainėje www.owasp.org	The system must be secured against the most recent attacks over the network. The list is published in The Open Web Application Security Project website (www.owasp.org)	Vartotojų autentikavimas, autorizavimas ir valdymas/Users authentication authorization and administration	Nossa Data follows secure coding practices as a core part of their Software Development Lifecycle (SDLC). The organisation emphasizes "coding for security, not functionality" as a fundamental approach for all software developers. This includes removing, disabling, and not implementing insecure services, protocols, or ports that could compromise system security. The Engineering Team documents the functions of new services or protocols, controls changes, and reviews potential consequences to mitigate risks. Developers are required to follow a structured project management framework with well-defined change management policies and procedures, ensuring security is integrated throughout the development process Nossa Data's internal documentation lists all coding principles that we are following. These are based on the OWASP secure coding practices, with a few additional guidelines specific to our systems. An initial review of the codebase is being performed, where we ensure these coding principles are followed. All new features go through a checklist to ensure they are following these principles. Engineering Leadership reviews these principles annually or after any large system change.
NFR-1.97	Privalomas funkcionalumas HTTP sesijos apsaugai: 1. Apsaugoti lankytojo/vartotojo visą sesiją TLS (TLS versija ne senesnė nei v1.3); 2. Neįtraukti sesijos ID į URL adresą arba nesiųsti jo siunčiamos užklausos antraštėje (angl. „Referrer header“); 3. Užtikrinti, kad sesijos ID yra ilgas, sudėtingas, sugeneruotas iš atsitiktinių skaičių ir negali būti lengvai atspėjamas; 4. Draudžiama saugoti sesijos ID; 5. Sesijos ID turi būti šifruojamas ne mažesniu kaip 128 bitų ilgio raktu; 6. Pakeičiamas sesijos ID įeigu yra perjungimas į SSL; 7. PĮ neprriima sesijos ID, kuris yra jau naudojamas kito vartotojo; 8. Išvalomas sesijos objektas vartotojui išsiregistravus arba sesijai nustojus galioti.	Obligatory functionality for HTTP session protection: 1. Protect the entire visitor's/user's session with a help of TLS (The version of TLS must be v1.3 or newer); 2. Do not include session ID into URL address and/or do not send it in the Referrer header; 3. Ensure long, complex, generated from random numbers, not easily guessed session ID; 4. Saving of session ID is prohibited; 5. Session ID has to be encrypted by a key of length at least 128 bits; 6. Session ID has to be changed in case of transfer to SSL; 7. The software has to reject ID, which is already used by another user; 8. Session object has to be deleted when user signs out or when the session is terminated.	WEB svetainė/WEB portal	1. Yes, confirmed. 2. Yes, confirmed. 3. Yes, confirmed. 4.
NFR-1.98	Draudžiama naudoti podėlio *(angl. cache)* **funkcionalumą puslapiuose, kuriuose vyksta vartotojo autentifikacija.**	Use of cache functionality is prohibited for authenticated pages.	WEB svetainė/WEB portal	We store authentication tokens in the user's browser cache and they have an expiration after 7 days unless renewed by activity or login. Reference: https://www.notion.so/nossadata/Expiration-time-outs-info-19148e316031800b9897f4241b058b62
NFR-1.99	Duomenys, turintys įtakos saugumui (pvz., slaptažodžiai) turi būti saugomi serverio, o ne kliento pusėje.	Security-relevant data (e.g. passwords, connection strings) must be stored server-side.	WEB svetainė/WEB portal	Passwords are not stored, only password hashes are stored in the AWS-hosted database.
NFR-1.100	Podėlis kliento pusėje yra išjungtas tuose tinklalapiuose, kur vedama jauti informacija (pvz., naudojant antraštes (angl. headers) „Cache-Control: no-store“ ir „Pragma: no-cache“).	Client-side caching is disabled on pages containing sensitive information (e.g. using "Cache-Control: no-store" and "Pragma: no-cache" headers).	WEB svetainė/WEB portal	Yes, confirmed.
NFR-1.101	Programų išeities tekstas, talpinamas tarnybinėse stotyse, turi būti nepasiekiamas neautorizuotiems naudotojams.	Server-side source code is protected from being downloaded by unauthorised users.	WEB svetainė/WEB portal	Source code is only shared between Nossa Data engineers, and stored in private repositories.
NFR-1.102	Programiniame kode draudžiama išsaugoti vartotojo vardą slaptažodį; autentifikavimui skirtus raktus / ženklus (angl. Token) ir kt.	It is prohibited to store login name, password, keys/tokens, etc. in the source code.	WEB svetainė/WEB portal	Nossa Data controls access to source code through multiple mechanisms. Developers use a structured process for code review and submission, with branch protection rules in place. Access to code repositories is restricted and logged, with engineers requiring additional yearly secure coding training. Code repositories are subject to branch protection rules, and any changes to these systems are tracked and logged.
NFR-1.103	Sesijos nutraukimo (angl. logout) mechanizmai prieinami iš visų terminalų, prie kurių vyksta autentifikavimas ir autorizavimas.	Logout mechanisms are available to users from all screens that are protected by authorisation to terminate the associated session or connection.	WEB svetainė/WEB portal	Yes, confirmed.
NFR-1.104	Nuolatinės (nenutrūkstamos) sesijos arba slapukai be galiojimo datos yra draudžiami.	Persistent authentication sessions or cookies are disallowed.	WEB svetainė/WEB portal	n/a
NFR-1.105	Visi konkrečios sesijos duomenys turi būti saugomi kaip sesijos kintamieji, o ne kaip slapukai kliento įrenginyje.	All data must be stored in session variables instead of client-side cookies.	WEB svetainė/WEB portal	Some data is stored in client-side cookies: Expiry-based auth token, and various third party utilities as per our privacy policy. Regular session auth tokens expire after 7 days, access link tokens are valid for 24 hours.
NFR-1.106	Sesijos identifikatoriai ir slapukai turi būti niekada nesiunčiami į web serverį kaip HTTP GET parametrai.	Session identifiers and cookies are never sent to the web server as HTTP GET parameters.	WEB svetainė/WEB portal	Yes, confirmed.
NFR-1.107	Kai naudotojas prisijungia, turi būti sukuriamas naujas unikalus sesijos identifikatorius.	A new session identifier must be created when a user logs on.	WEB svetainė/WEB portal	Yes, confirmed.
NFR-1.108	Naudotojui vedant slaptažodį, Sistema vedamo slaptažodžio neturi rodyti atviru tekstu.	Passwords on the user's screen are obscured so that they cannot be viewed by 'shoulder surfing'.	WEB svetainė/WEB portal	Yes, confirmed.
NFR-1.109	Visų įvesties duomenų patikrinimas (validavimas) turi būti vykdomas patikimoje sistemoje (pvz., tarnybinėje stotyje, o ne kliento įrangoje).	All input validation is conducted on a trusted system (i.e. server-side, not client-side).	WEB svetainė/WEB portal	Yes, confirmed.
NFR-1.110	Visi įvesties duomenys turi būti patikrinti pagal: diapazoną, ilgį, formatą ir duomenų tipą.	All input has been validated for expected range, length, format and data type.	WEB svetainė/WEB portal	Yes, confirmed, per requirements of each ESG framework.

NFR-1.111	Duomenų įvesties formos, kurios prieinamos išorės naudotojams, pildymas turi būti apsaugotas nuo pildymo automatizuotomis priemonėmis, pvz., reCAPTCHA, No CAPTCHA ir pan.	Data entry forms that are accessible to external users must be protected against automation filling in, such as reCAPTCHA, No CAPTCHA, etc.	WEB svetainė/WEB portal	n/a; data entry forms are not sent externally. We do not have reCAPTCHA on the login page, however, we do have DDoS protection and additionally lock accounts if multiple login attempts are made (e.g. to protect against password cracking attempts).
NFR-1.112	Sistemai turi būti taikomos apsaugos priemonės nuo bandymų automatizuotai atspėti paskyros slaptažodį (angl. „brute force attack“). Bandymai turi būti registruojami.	The system must be protected against automatic brute force attacks. Tests must be recorded.	WEB svetainė/WEB portal	Nossa Data will has a suitable authentication technique to substantiate the claimed identity of a user. Nossa Data will develop the following log-on procedure in order to not provide any assistance to unauthorized users: System or application identifiers will not be displayed until the log-on process has been successfully completed; Restricting any help messages provided during the log-on procedure that would aid an unauthorized user; Log-on information will only be validated on completion of all input data; No indication will provided to the users regarding the part of the data that is correct or incorrect as part of an error condition arising; Protection against brute force log-on attempts will be implemented.
NFR-1.113	Sistema turi užtikrinti duomenų konfidencialumą, t. y. turi leisti asmenims matyti tik tuos duomenis, kuriuos jie gali matyti, turi būti uždraustas naršymas Sistemos svetainės aplankuose (angl. Directory browsing).	The system must ensure the confidentiality of the data, i.e. must allow people to view only the data they are allowed to view. Browsing in Directory browsing is prohibited.	WEB svetainė/WEB portal	Yes. Admin users can dictate what data is seen by each user.
NFR-1.114	Sistemoje turi būti įgyvendintos kontrolės priemonės leidžiančios prisijungimą prie Sistemos administravimo dalies tik iš Užsakovo pateiktų IP adresų.	Access to the System Administration console must be limited by IPs provided by the Customer.	WEB svetainė/WEB portal	This can be provided upon request.
NFR-1.115	Sistemoje turi būti galimybė valdyti robotų ribojimo protokolą (angl. Robots Exclusion Protocol - robots.txt) nurodant, kurias Sistemos dalis leisti pasiekti paieškų robotams, o kurias draustį. Sistema turi užtikrinti automatinį šio protokolo valdymą be papildomo administratoriaus įsikišimo, kai informacija padaroma nebepublikuojama ar jos pateikimui uždedamas draudimas.	The system must have the ability to control the robots exclusion protocol (robots.txt), indicating which parts of the system allow access to search robots and which are prohibited. The system must ensure automatic management of this protocol without additional intervention by the administrator when information is no longer published or its prohibition is placed.	WEB svetainė/WEB portal	Yes, by preventing disclosure of the directory structure in the robots.txt file by placing directories not intended for public indexing into an isolated parent directory.
NFR-1.116	Interneto svetainėje turi būti patalpintas failas „security.txt“ su Skaitmeninės saugos kontaktine informacija standartinėje vietoje (pvz., www.svetainė.lt/security.txt)	A file named "security.txt" with Client's Digital Security contact information should be hosted on the website in the standard location (e.g. www.website.com/security.txt)	WEB svetainė/WEB portal	This can be done upon request.

Sistemoms, kuriose tvarkomi asmens duomenys yra taikomi ADA1, ADA2, ADA3 reikalavimai:

ADA1 – saugos reikalavimai turi būti užtikrinami visose sistemose, kuriose tvarkomi (įskaitant ir saugojimą) bet kokie asmens duomenys (pvz. kontaktinis telefonas, pareigos, vardas, pavardė, ir pan.);	ADA1 – security requirements must be ensured in all systems that process (including storage) any personal data (e.g. contact phone number, position, name, surname, etc.);
ADA2 – saugos reikalavimai turi būti užtikrinami Sistemose, kuriose tvarkomi klientų (tapatybės, sutarčių, įsiskolinimų, nuosavybės, mokėjimų ir pan.) asmens duomenys, darbuotojų duomenys, kiek tai susiję su atliekamomis darbo funkcijomis, užduotimis, pavedimais;	ADA2 – security requirements must be ensured in Systems that process personal data of customers (identity, contracts, debts, property, payments, etc.), employee data, as far as it is related to the work functions, tasks, and orders performed;
ADA3 – saugos reikalavimai turi būti užtikrinami Sistemose, kurios naudojamos darbuotojų duomenų tvarkymui (darbo santykių administravimo tikslu), ir/arba sistemoje tvarkomi specialiųjų kategorijų asmens duomenys (sveikatos, biometriniai duomenys, duomenys apie asmenų teistumą), ir/arba sistemoje vykdomas sistemingas ir išsamus asmens savybių vertinimas, grindžiamas automatizuotu tvarkymu, įskaitant profiliavimą.	ADA3 – security requirements must be ensured in Systems that are used for the processing of employee data (for the purpose of administering employment relations), and/or the system processes special categories of personal data (health, biometric data, data on criminal records of individuals), and/or the system carries out a systematic and comprehensive assessment of personal characteristics based on automated processing, including profiling.

Taikymas	Prieigų kontrolė	Access control and authentication	ADA1	ADA2	ADA3	KUR turi būti įkelta
	Privilegijuotiems vartotojams (pvz., sistemų administratoriams) prisijungimui prie asmens duomenų tvarkymo sistemų turi būti taikomas dviejų veiksnių autentifikavimas. Visais atvejais, kai į tokias sistemas jungiamasi ne iš vidinio kompiuterių tinklo, turi būti naudojamas dviejų veiksnių autentifikavimas. Autentifikavimo veiksniais gali būti slaptažodžiai, saugumo žetonai, USB raktai su slapta žyma, biometriniai duomenys ir kt.	Privileged users (such as system administrators) must use two-factor authentication when connecting to personal data processing systems. In all cases where access to such systems is not from an internal network, two-factor authentication must be used. The authentication factors could be passwords, security tokens, USB sticks with a secret token, biometrics etc.			x	NFR
	Techniniai žurnalų įrašai (angl. logs)	**Logging and monitoring**				KUR turi būti įkelta
OF PREM	Techninių žurnalų įrašai turi būti įgyvendinti kiekvienai IT sistemai, naudojamai asmens duomenims tvarkyti. Techninių žurnalų įrašuose turi būti matoma visa įmanoma prieigų prie asmens duomenų informacija (pvz., data, laikas, peržiūrėjimo, keitimo, panaikinimo veiksmai). Saugojimo terminas – ne trumpiau kaip 6 mėnesiai.	Log files should be activated for each system/application used for the processing of personal data. They should include all types of access to data (view, modification, deletion). Storage term – at least 6 months.	x	x	x	NFR
	Duomenų bazių apsauga	**Data base security**				
	Duomenų bazėse ir taikomųjų programų tarnybinėse stotyse turi būti tvarkomi tik tie asmens duomenys, kurie yra reikalingi darbui, atitinkančiam duomenų tvarkymo tikslus.	Database and applications servers should only process the personal data that are actually neededs to process in order to achieve its processing purposes	x	x	x	NFR
	Duomenų bazėse turi būti taikomi pseudonimizavimo metodai, atskiriant tiesioginius identifikatorius nuo esamų sąsajų su kitais duomenimis.	Pseudonymization techniques should be applied through separation of data from direct identifiers to avoid linking to data subject without additional information		x	x	FR
	Duomenų saugojimas ir duomenų subjektų teisių įgyvendinimas:	**Data retention and enforcement of data subjects' rights**				
	Sistemoje turėtų būti įdiegtas funkcionalumas, kad pasibaigus duomenų saugojimo terminui, šie duomenys iš sistemos turėtų būti trinami arba nuasmeninami.	The system should have functionality – after data retention period data should be deleted from system or anonimyzed	x	x	x	FR
	Sistemoje turi būti galimybė automatiškai sugeneruoti ataskaitą, kokie pavienio asmens duomenys tvarkomi sistemoje	The system must be able automatically generate a report of what personal data is processed in the system	x	x	x	FR
	Sistemoje turi būti galimybė ištrinti/nuasmeninti pavienio kliento asmens duomenis, jeigu jų saugoti nėra teisinio pagrindo.	The system must be able to delete / personalize the personal data of an individual customer if there is no legal basis for their storage.	x	x	x	FR

Nr.	Reikalavimas	English	Reikalavimo tipas / Requirement category	NFR/Sutartis/Tech spec
NFR-3.1	Turi būti galimybė daryti rezervines kopijas visiems saugomiems duomenims tiek veikiančioje, tiek neveikiančioje Sistemoje (angl. online and offline).Duomenų rezervinis kopijavimas turi būti atliekamas ne rečiau nei kas 24 val, turi būti galimybė atsatyti ne senesnius nei 24 val. duomenis, paskutinė rezervinė kopija turi būti saugoma ne trumpiau nei sutartas dienų skaičius.	It must be possible to back up all stored data both online and offline.Data must be backed up at least every 24 hours, it must be possible to back up data older than 24 hours, and the last backup must be kept for number of days agreed in the agreement.	Atsarginės kopijos ir atstatymas/Backup and Restore	Daily snapshots are taken, with backups available in more than one AWS region.
NFR-3.2	Sistemos vidinė architektūra turi būti pritaikyta palaikyti Sistemos prieinamumą ne mažiau kaip 99,95 proc. laiko visus metus.	The internal architecture of the System must be designed to support system availability of at least 99.95% of the time throughout the year.	Prieinamumas ir patikimumas/Availability and Reliability	Yes, SLO is 99.99%.
NFR-3.3	Įvykus incidentui, dėl kurio Sistemos programinė įranga perleidžiama iš naujo (pvz., elektros energijos tiekimo sutrikimas, kt.), programinės įrangos paleidimas turi įvykti automatiškai be žmogaus įsikišimo, negali dingti į Sistemą suvesti ir incidento metu apdorojami duomenys ar programinės įrangos konfigūracijos duomenys (reikalavimas negalioja portalų / paskyrų užpildymo laukuose įvestiems, bet incidento metu dar neišsaugotiems duomenims).	In case of incident causing System restart (such as loss of the power), software shall be restarted automatically without human interference. Data entered into the System and processed during the incident, as well as, software configuration data shall not be lost. This requirement is not applied for data entered GUI, but not saved before the incident.	Prieinamumas ir patikimumas/Availability and Reliability	Yes, confirmed. If a user had been typing an answer that cannot be saved, they will be prompted to save it locally until it can be saved again.
NFR-3.4	Turi būti galima dirbti su Sistema, kol vykdomi kiti darbai, pvz., atliekamų paketinių užduočių veiksmai, registravimai, naudotojo veiksmai, išskyrus Sistemos administratoriaus veiksmus, neturi blokuoti kito naudotojo veiksmų ir neturi daryti įtakos Sistemos greitaveikai ir pan.	It must be possible to work with the System while performing other tasks, such as actions performed by batch tasks, registrations, actions by the user, with the exception of the actions of the SYSTEM administrator, do not block the actions of another user and should not affect the speed of the SYSTEM, etc.	Prieinamumas ir patikimumas/Availability and Reliability	Yes, correct.
NFR-3.5	Tiekėjas turi pasiūlyti sprendimą Sistemos ir jos komponentų stebėjimui, kuris turėtų galimybę integruotis į pirkėjo turimas monitoringo ir stebėjimo sistemas Zabbix.	The Supplier shall propose a solution for the monitoring of the System and its components, which would be able to integrate into the buyer's currently owned monitoring systems Zabbix.	Prieinamumas ir patikimumas/Availability and Reliability	n/a
NFR-3.6	Sistema turi palaikyti automatinio techninių pajėgumų plėtimą, prijungiant papildomą techninę įrangą (angl. Auto-scaling) ir apkrovos balansavimo funkciją, kad išlaikytų našumo standartus net esant dideliam duomenų srautui.	The system should be capable of auto-scaling and load balancing to maintain performance standards, even under heavy traffic conditions.	Plečiamumas/Scalability	developers use a process for reviewing, testing and submitting code into the development environment. This is followed by infrastructure testing, submission into the staging environment, quality assurance testing, followed by a production deployment. Our Software Development Lifecycle procedures provide full guidelines for developers. We set up branch protection rules requiring code reviews, including for deployments to staging and

Nr.	Taikymas	Reikalavimas	English	Reikalavimo tipas / Requirement category	NFR/Sutartis/Tech spec
NFR-4.1	Visiems	Sistemos aplinkos (vystymo, testavimo ir darbinė aplinkos) turi būti atskiros viena nuo kitos.	The System environments (development, testing, and work environment) must be separate from each other	Kokybės užtikrinimas ir diegimas/Quality assurance and deployment	Yes, this is the case at Nossa Data.
NFR-4.2	Visiems	Sistema turi turėti automatizuotą procesą, kuris keitimus iš vienos sistemos aplinkos perdiegtų į kitą. Turi būti galimybė perkelti visus pakeitimus įskaitant , bet neapsiribojant: - procesus; - duomenis; - konfigūraciją; - parametrus.	System must have automated processes to deploy changes from one environment to other. It must be possible to deploy all changes including but not limited to: - processes; - data; - configuration; - parameters.	Kokybės užtikrinimas ir diegimas/Quality assurance and deployment	Yes, per the system protection policy.
NFR-4.3	SaaS	Užsakovas turi būti informuotas apie būsimus diegimus ir kartu su pranešimu gauti būsimo diegimo testavimo ataskaitas.	The Customer must be informed about upcoming releases and testing reports to be provided.	Kokybės užtikrinimas ir diegimas/Quality assurance and deployment	Yes, confirmed.
NFR-4.4	Visiems	Pokyčio diegimas turi būti atliekamas tokiu būdu, kad nereikalautų sistemos stabdymo (angl. downtime).	The deployment/release of the changes into the system should be executed in the way that it doesn't require system downtime.	Kokybės užtikrinimas ir diegimas/Quality assurance and deployment	Yes, this is the case. In the rare case that downtime may be expected, this would occur outside working hours and with warning to the customer.
NFR-4.5	Visiems	Sistemoje turi būti numatyti skaitmenizuoto verslo proceso kokybės rodiklių išvedimo taškai, kuriuos būtų galima perduoti į bendrą „Ignitis“ naudojamą verslo procesų stebėsenos sistemą.	Digital business proceses quality metrics must be available and provided in a way that would integrate to „Ignitis“ metrics monitoring system.	Kokybės užtikrinimas ir diegimas/Quality assurance and deployment	Metrics can be provided upon request. Specifics have not been requested to understand metrics needed.
NFR-4.6	SaaS	Rangovas įsipareigoja diegti tik ištestuotus pokyčius.	The vendor comits to release only tested releases.	Kokybės užtikrinimas ir diegimas/Quality assurance and deployment	Yes, tested in a staging environment before deployment.

Nr.	Reikalavimas	English	Reikalavimo tipas / Requirement category	NFR/Sutartis/Tech spec	
NFR-5.1	Sistemoje turi būti mobiliesiems įrenginiams pritaikyta programėlė suderinama su iOS ir Android mobiliosiomis operacinėmis sistemomis.	The system must have a mobile application compatible with iOS and Android mobile operating systems.	Mobilus įrenginiai/Mobile devices	n/a	Teikiama rangovui tokiu atveju, jeigu yra poreikis mobiliai programelei
NFR-5.2	Sistemoje turi būti galimybė rūšiuoti įrašus, dokumentų sąrašus pagal datą ir kitus pasirinktus parametrus.	The System must be able to sort entries, document lists by date and other selected parameters.	Naudojimo patogumas / Usability	Yes, confirmed.	
NFR-5.3	Sistemos naudotojo sąsajos turi būti atsparios klaidoms: 1. Sistemos naudotojo sąsajos turi tikrinti įvedamų duomenų logikos korektiškumą. 2. Sistemos naudotojo sąsajos turi padėti išvengti klaidos situacijų bei klaidų duomenų įvedimo metu (pvz., prie duomenų įvedimo laukų turi būti nurodomi duomenų įvesties formato paaiškinimai). 3. Sistemos naudotojo sąsajose klaidų pranešimai turi būti taip pateikiami ir būti tokio turinio, kad kokybiškai prisidėtų prie klaidos ištaisymo (pvz., klaidos pranešimas turi nurodyti, kur yra klaida ir kaip ją ištaisyti). 4. Sistemos naudotojo sąsajose klaidų indikacija turi būti pateikiama šalia klaidą sukėlusio elemento (pvz., neturi būti pažymėti laukai su klaidingai įvestais duomenimis). 5. Jeigu Sistema gali pati ištaisyti klaidas, Sistemos naudotojo sąsajose turėtų būti pateikiama tokia informacija, ir leidžiama nuspręsti, ar pasinaudoti tokia pagalba (pvz., turi būti pateikiami automatiniai laukų užpildymo pasiūlymai). 6. Sistemos naudotojo sąsajose įvedamos informacijos tikrinimas turėtų būti atliekamas dinamiškai. 7. Sistemos naudotojo sąsajose užfiksuotų klaidų taisymui reikalingas veiksmų kiekis turi būti minimalus.	System UI interfaces must be error-proof: 1. The system user interfaces must verify the correctness of the input logic if such verification is feasible. 2. The system user interfaces must help prevent error situations and errors when entering the data (for example, the data input fields must contain explanations of the data input format). 3. Error messages must be presented in such a way and contribute qualitatively to the error (for example, the error message must indicate where the error is and recommend how to fix it). 4. In the system user interface, the error indication must be displayed next to the error causing the item (for example, fields with incorrectly entered data must not be marked). 5. If the system can correct itself for errors, the system user interface should contain the following information and it is allowed to decide whether to use such assistance (for example, automatic field bidding must be provided). 6. The system should check the information entered in the user interfaces in a dynamic manner. 7. The system needs to minimize the amount of activity required to correct errors detected in the user interface.	Naudojimo patogumas / Usability	Yes, all of these conditions can be satisfied. Example use cases include; Percentages that must be under 100% cannot be inputted at over 100%; letters cannot be inputted where characters must be numeric; the incorrect number of decimal places will not be accepted; error notifications will occur during many of these conditoins.	
NFR-5.4	Sistema turi palaikyti UCS koduotes (minimum UTF8) ir lietuvių kalbos abėcėlės rašmenis. Grafinė sistemos sąsaja turi būti pritaikyta daugiakalbystei įskaitant lietuvių ir anglų kalbas.	System shall support UTF8 and characters of Lithuanian alphabet. Graphical interface must support Multilanguage including Lithuanian and English.	Naudojimo patogumas / Usability	System is a web-based application. These characters are supported by the web browsers suitable for use with Nossa Data (Chrome, Edge, Firefox).	
NFR-5.5	Sistema turi užtikrinti importuojamų duomenų integralumą šiomis taisyklėmis: - Ar aptikus klaidas importuojamuose duomenyse, sėkmingai importuojami visi ne klaidingai pateikti duomenys; - Ar aptikus klaidas importuojamuose duomenyse, nėra importuojami jokie duomenys. - Ar aptikus klaidas importuojamuose duomenys, suimportuoti teisingus ir atskirai pateikti klaidingus bei įvardinti jų klaidas Detalios duomenų importavimo taisyklės turės būti suderintos Sistemos diegimo metu.	System shall ensure integrity of the imported data by the rules: - if there are errors in import data, correct records will be imported, OR - if there are errors in import data, no data will be imported, OR - if there are errors in import data, correct records will be imported and wrong records presented separated with cause of failure indicated. Exact rules for particular import procedure will be agreed during implmenetation.	Naudojimo patogumas / Usability	Yes, confirmed. This is only applicable in Nossa Data's CDP upload process.	
NFR-5.6	Sistema turi veikti pagal greitaveikos reikalavimus, kai su ja vienu metu dirbs x tiesiogiai prisijungusių vartotojų (atidarytų sesijų). Iš jų vienu metu gali aktyviai atlikinėti veiksmus.	The System shall meet fast response requirements with 800 directly logged in users (open sessions) simultaneously. 800 of them can actively perform actions.	Sistemos darbas/Performance	Yes, confirmed, can be tested by simulating open sessions.	
NFR-5.7	Visos naudotojams skirtos funkcijos turi būti atliekamos naudojant GUI. Su galimybe tam tikras funkcijas atlikti komandų pagalba.	All functions must be performed using the GUI, not just the menu. With the ability to perform certain functions with command line or hot keys help.	Naudojimo patogumas / Usability	n/a	
NFR-5.8	Klaidų pranešimai turi būti suformuluoti taip, kad Sistemos naudotojui būtų aišku (ne tik klaidos kodas), kas atsitiko.	Error messages must be worded in such a way that the SYSTEM will make clear to the user what has happened and what actions they should continue to do in order to continue their work.	Naudojimo patogumas / Usability	Yes, confirmed.	
NFR-5.9	Sistema turi užtikrinti korektišką klaidų, kurias sukėlė neteisingi naudotojo veiksmai, valdymą.	System must support error checking and data control for users caused actions.	Naudojimo patogumas / Usability	Yes, errors are flagged to the team of software engineers upon system activity (users not being able to log in, page crashing, etc.).	
NFR-5.10	Sistemos naudotojui atlikus neteisingą (neleidžiamą) komandą arba nekorektiškai įvedus duomenis, Sistema turi naudotojui rodyti atitinkamus pranešimus darbalaukyje.	System must show notifications explaining incorrect user action or wrong data.	Naudojimo patogumas / Usability	Yes, this is provided for particular actions (example: error icon when trying to edit a completed report).	
NFR-5.11	Sistema turi mokėti patikrinti, ar visi įvedamo / keičiamo / importuojamo įrašo privalomi laukai yra įvesti.	The System shall check if entered/modified/imported data obligatory fields are filled.	Naudojimo patogumas / Usability	Yes, confirmed.	
NFR-5.12	Sistema turi būti pritaikyta naudojimui mobiliais įrenginiais. Sistema turi palaikyti "responsive design" ir pritaikyta įvairaus tipo su skirtinga skiriamąja geba (resolution) arba turi turėti tam skirtą aplikaciją.	The system must be adapted for use with mobile devices. The system has to be responsive design and adapted to different types of resolution (resolution) or have a dedicated application.	Mobilus įrenginiai/Mobile devices	n/a	
NFR-5.13	Sistemoje turi būti galimybė naudotojui pasikeisti numatytą naudotojo sąsajos kalbą neperdiegiant ar neperkraunant sistemos.	The System shall allow user to change the default user interface language without system reinstallation or restarting.	Naudojimo patogumas / Usability	Yes, as an online software, this is simply performed with browser capabilities seemlessly.	
NFR-5.14	Sistemos naudotojo sąsajos turi būti suderinamos su šiomis naršyklėmis: • Mozilla Firefox (nuo 44 iki Sistema diegimo etapo pradžios vėliausios išleistos versijos, Microsoft Windows, Apple Mac OS X, Linux OS); * Google Chrome (nuo 45 iki Sistema diegimo etapo pradžios vėliausios išleistos versijos, Microsoft Windows OS) * Microsoft Edge	The System UI must be compatible with the following browsers: • Mozilla Firefox (from 44 to the start of the System installation phase, the latest release, Microsoft Windows, Apple Mac OS X, Linux OS); * Google Chrome (from 45 to the start of the System installation phase of the latest release of Microsoft Windows OS) * Microsoft Edge	Naudojimo patogumas / Usability	Yes, Nossa Data can operate on all of these.	
NFR-5.15	Sprendimas turi užtikrinti aukštą prieinamumą ir ne mažesnį kaip 99,9 % veikimo laiką, kurį palaiko keičiamo dydžio infrastruktūra tam, kad būtų apdorojami kintantys darbo krūviai ir nesumažėtų našumas.	The SaaS solution must ensure high availability with a minimum uptime of 99.9%, supported by scalable infrastructure to handle fluctuating workloads without degradation in performance.	Sistemos darbas/Performance	Core Nossa Data third party dependency services have an SLA of at least 99.9%.	
NFR-5.16	Naudotojo sąveikos reakcijos laikas piko metu neturi viršyti 2 sekundžių, siekiant užtikrinti sklandžią vartotojo patirtį.	Response times for user interactions should remain under 2 seconds during peak usage, ensuring a seamless experience.	Sistemos darbas/Performance	Yes, confirmed. Platform slowness is also monitored continuously.	
NFR-5.17	Sprendimo tiekėjas įsipareigoja priimti užsakovo nusiskundimus dėl sistemos greitaveikos kaip defektus, išnagrinėti juos bei pašalinti greitaveikos sutrikimą sukelenčias priežastis/atlikti sistemos ar infrastruktūros pagerinimus arba pateikti užsakovui protingumo kriterijais pagrįstus paaiškinimus, kodėl greitaveikos sutrikimai negali būti pašalinti	The Solution Provider undertakes to accept the Customer's complaints about system performance as defects, to investigate them and to remedy the causes of the performance degradation/improve the system or the infrastructure to remove performance degradation, or to provide the Customer with an explanation, based on reasonable criteria, as to why the performance degradation cannot be remedied	Sistemos darbas/Performance	Yes, Nossa Data tracks all client feedback using internal communications and tools to track these, providing updates to the client upon updates.	

Nr.	Reikalavimas	English	Reikalavimo tipas / Requirement category	NFR/Sutartis/Tech spec
NFR-6.1	Siūlomas Sprendimas ar Sistema privalo atitikti daugiapakopę (angl. multitenant) architektūrą leidžiančia teikti paslaugas iš jungtinės infrastruktūros keliems Sistemos naudotojams/nuomininkams (angl. tenant).	The Solution or System must support multitenant architecture which a single instance of software runs on a server and serves multiple tenants	Sistemos architektūra/Technology Architecture	
NFR-6.2	Sistema turi būti realizuota ne mažiau kaip pagal trijų lygių programų architektūros modelį (duomenų bazės lygis, aplikacijų lygis, naudotojo sąsajos lygis). Sistemoje turi būti galimybė konfigūruoti ir plėsti kiekvieną iš šių lygių individualiai, nepriklausomai nuo kitų lygių.	The Solution or System must be implemented at least in accordance with the three-level architecture model (database level, application level, user interface level). The System must be able to configure and extend each of these levels individually, regardless of other levels.	Sistemos architektūra/Technology Architecture	Nossa Data has nonproduction environments (e.g., development, test, quality assurance, staging) and ensures that they are logically separated from the production environment. Access rights to the production environment will be configured for separation of duties to ensure that the development team is prevented from implementing changes independently.
NFR-6.3	Sistema turi turėti standartizuotą web integravimosi sąsają (API) per kurią būtų galima skaityti, kurti, redaguoti ir trinti objektus, ar įrašus.	The Systems must be implemented in service-oriented architecture and have the ability to integrate with the ESB by standard API.	Sistemos architektūra/Technology Architecture	n/a
NFR-6.4	Siūlomas sprendimas ar/ir Sistema turi būti grįsta standartiniu konfigūruojamu produktu (angl. COTS, https://en.wikipedia.org/wiki/Commercial_off-the-shelf). Programinė įranga turi būti standartiniai produktai, t. y. parduodami kaip standartinė licencijuojama programinė įranga, turinti nepriklausomą nuo konkrečių pavienių užsakovų vystymo planą ir gyvavimo ciklą	The Solution or System must be based on a standard configurable product (COTS, https://en.wikipedia.org/wiki/Commercial_off-the-shelf). The software must be standard products, ie. y. sold as standard licensed software with independent development plans for individual customers and lifecycle	Sistemos architektūra/Technology Architecture	This solution is an off-the-shelf solution, with configurability enabled and discussed ahead of the contract drafting.
NFR-6.5	Sistemoje turi būti galimybė išsaugoti atributų, laukų, kitų sistemos leidžiamų modifikacijų keitimo istoriją	System shall log changes to standard and customized attributes	Sistemos architektūra/Technology Architecture	Yes, confirmed. Updates to new features are also regularly shared with the client.
NFR-6.6	Sistema turėtų būti įgyvendinta remiantis į paslaugas orientuota architektūra (angl. Service-Oriented Architecture, SOA) ir užtikrinti paslaugų moduliarumą, plečiamumą ir pernaudojamumą. Kiekviena verslo funkcija turėtų būti pateikiama kaip atskira sąveiki paslauga, leidžianti sklandžiai integruoti ir palaikyti ryšį tarp skirtingų komponentų. Paslaugos turėtų būti laisvai susietos ir bendrauti standartizuotais protokolais, kad jas būtų galima lengvai prižiūrėti, atnaujinti ir plėsti ateityje.	The system should be implemented based on a Service-Oriented Architecture (SOA) to ensure modularity, scalability, and reusability of services. Each business function should be encapsulated as a distinct, interoperable service, allowing for seamless integration and communication between different components. Services should be loosely coupled and communicate via standardized protocols, enabling easy maintenance, updates, and future expansion.	Sistemos architektūra/Technology Architecture	Yes, confirmed.
NFR-6.7	Sistema turi turėti standartinius sprendimus ir protokolus duomenų mainų sąsajų su kitomis sistemomis realizavimui.	System must have standard solutions, protocols, APIs for data exchange with other systems.	Sistemos architektūra/Technology Architecture	Yes, Nossa Data where relevant in the client's chosen solutions operates with standard solutions, protocols, and APIs to transmit data.

NFR-6.8	Sistemoje turi būti galimybė palaikyti kelių skirtingų organizacinių (pvz., įmonės, padalinio, departamento, skyriaus ir pan.) vienetų duomenis vienu metu: -Turi būti galimybė bendrai naudoti atskirų organizacinių vienetų išteklius bei atskirų organizacijų duomenų bazių duomenis; -Turi būti galimybė matyti tiek skirtingų organizacinių vienetų suvestinius duomenis už visus organizacinius vienetus, tiek kiekvieno organizacinio vieneto duomenis atskirai. (gal performuluot į prieėjimą prie tam tikrų duoemnų rinkinių pagal roles)	The System must be able to support the data of several different organizational units (e.g., company, department, department, department, etc.) simultaneously: -To be able to share the resources of individual organizational units and data from individual organizations databases; - It should be possible to see aggregate data of different organizational units for all organizational units and data for each organizational unit separately.	Sistemos architektūra/Technology Architecture	Yes, this is reflected by the different user types that can access the software, all accessing different information based on level of security and chosen departmental topics by the Admin user.
NFR-6.9	Sistemos operacijos duomenų bazėje gali būti atliekamos tik per Sistemos aplikacijos sluoksnį, t.y. tiesioginis SQL komandų vykdymas duomenų bazėje turi būti neleidžiamas.	System operations in the database can only be performed through the application layer of the system, i.e. The direct execution of SQL commands in the database must be denied.	Sistemos architektūra/Technology Architecture	Engineers can perform SQL commands directly if necessary, however this is a discouraged practice that is kept as a back-up plan for critical scenarios only.
NFR-6.10	Sistemoje turi būti priemonės, užtikrinančios vieningą duomenų suvedimą (angl. Single Data Entry), t.y. suvedus tam tikrą duomenų reikšmę, pvz., adresą, tam pačiam IS objektui dubliuojančių reikšmių suvedimas nebūtų galimas.	The system must have tools for Single Data Entry, i.e. when a certain value of the data, such as an address, is entered, the duplication of values for the same IS object would not be possible.	Sistemos architektūra/Technology Architecture	Where relevant for particular ESG questionnaires, Nossa Data has value check in place to reduce risk of incorrect data.
NFR-6.11	Duomenų bazių valdymo sprendimas turi užtikrinti vidines duomenų vientisumo užtikrinimo funkcijas, turėti duomenų atstatymo mechanizmus po gedimų ir pažeidimų.	The database management solution must provide internal integrity assurance functions, have data restoration mechanisms after failures.	Sistemos architektūra/Technology Architecture	Yes and daily backups also prevent losing data in the database, should reverting to a previous date be required.
NFR-6.12	Sistemoje tvarkomų duomenų įrašų ir el. dokumentų skaičius neturi būti ribojamas, išskyrus tuos apribojimus, kurie atsiranda dėl virtualios infrastruktūros techninių parametrų ar apribojimų.	The number of system processed data records and e-documents should not be limited, except those restrictions that arise from the technical parameters or restrictions of the	Sistemos architektūra/Technology Architecture	The limits to processed documents are
NFR-6.13	Sistema su užsakovo eksploatuojamomis informacinėmis sistemomis integracijai turi turėti API grįstą REST arba SOAP Web servisų architektūrą.	System integration with other Purchaser systems must be based on the following or equivalent standarts: SOAP, REST.	Sistemos architektūra/Technology Architecture	Yes, confirmed.
NFR-6.14	Sistemos programinėje įrangoje turi būti galimybė importuoti ir eksportuoti duomenis į standartinius duomenų apsikeitimo formatus (pvz. XML, CSV, XLSX arba lygiavertės rinkmenos.)	Siystem software must be able to export and import data using data exchange files (e.g.. XML, CSV, XLSX or equivalent).	Sistemos architektūra/Technology Architecture	Yes, confirmed.
NFR-6.15	Sistemoje neturi būti įkoduotų (*angl. Hard Coded*) duomenų, kuriems koreguoti ir / ar keisti būtų reikalingos diegėjo paslaugos.	The System shall not have Hard Coded data, which correction and/or modification require additional vendor services.	Sistemos architektūra/Technology Architecture	Additional services are not required to implement obligations outlined in the contract.
NFR-6.16	Sistemoje turi būti galimybė visus negrafinius kaupiamus ir generuojamus duomenis eksportuoti (arba turėti galimybę kitoms sistemoms pasiimti) Ignitis grupėje naudojamiems: - duomenų sandėliui (angl. Data Warehouse); - Analitiniam įrankiui.	System must have possibility to export (or let other system to gather) data to: - data warehouse - data analysis tool	Sistemos architektūra/Technology Architecture	Yes, Nossa Data allows exports to Word, PDF, and Excel.
NFR-6.17	Sistemos papildomų funkcijų pridėjimas turi būti galimas įdiegiant tiekėjo arba 3-iųjų šalių sukurtus plėtinius	Adding additional system features should be possible by installing extensions created by the vendor or third parties	Sistemos architektūra/Technology Architecture	n/a
NFR-6.18	Sistemoje turi būti galimybė išlaikyti keičiamų požymių istoriją (pavyzdžiui, informacija apie atsakingo asmens pasikeitimą ir datą, vidinio judėjimo data).	There must be a capability in the System to maintain the history of changes in attributes (e.g. information and date on the change of the person in charge, internal movement date).	Sistemos architektūra/Technology Architecture	Yes, this is available via history change logs and activity tracking provided to the client.
NFR-6.19	Projektavimo metu turi būti pateiktas reikalingos diskinės talpos kiekis duomenų saugojimui pagal projektuojamą Sistemos apkrovą (projektuojamą suminį duomenų kiekį per mėn/ metus)	The System design must include the required disc capacity of data storage according to the projected System load (the total projected amount of data per month / year)	Projektinė dokumentacija (on-premice)	Yes, confirmed.

NFR-6.20	Architektūros aprašymo ir reikalavimų infrastruktūrai dokumentą parengęs Rangovas atsako už jo kokybę, priimtus projektinius sprendimus ir galimybę juos įgyvendinti, taip pat už jo atitikimą Techninei specifikacijai. Parengtą Architektūros aprašymo ir reikalavimų infrastruktūrai dokumentą Rangovas turi pateikti Perkančiajai organizacijai peržiūrai ir derinimui. Architektūros aprašymo ir reikalavimų infrastruktūrai dokumentas turi būti pakoreguotas, atsižvelgiant į peržiūros metu pateiktas Perkančiosios organizacijos pastabas. Rangovas Sistemos diegimo darbus gali pradėti vykdyti tik tuomet, kai Rangovas suderina Architektūros aprašymo ir reikalavimų infrastruktūrai dokumentą su Perkančiąja organizacija. Jei Rangovui vykdant darbus iškyla būtinybė pakoreguoti Architektūros aprašymo ir reikalavimų infrastruktūrai dokumentą, Rangovas turi atlikti jo koregavimą ir pateikti Perkančiajai organizacijai dokumentą su visais pataisymais.	The Contractor, prepared the Architectural Description and Infrastructure Requirements Document, is responsible for the quality of the document, the Design of solution and its compliance with the Technical Specification, the possibility to implement designed solution. The Contractor shall provide the prepared Architectural Description and Infrastructure Requirements Document to the Contracting Authority for review and alignment. Document should be adjusted according to Contracting Authority comments. The Contractor may start the installation of the System only after Architectural Description and Infrastructure Requirements Document agreement with the Contracting Authority. If the Contractor's work necessitates the adjustment of the Architectural Description and Infrastructure Requirements Document, the Contractor shall make an adjustment to the document and provide it to the Contracting Authority a document with all corrections.	Projektinė dokumentacija	n/a
NFR-6.21	Sistemos programinė įranga neturi būti ribojantis veiksnys didinant Sistemos našumą. Kitaip tariant, informacinės sistemos našumui padidinti užtenka pridėti reikalingos aparatinės įrangos, tuo pačiu nekeičiant Sistemos programinės įrangos išeities kodų.	The system software must not be a limiting factor in the performance of the system. It is sufficient to add the necessary hardware to increase the performance of the information system without changing the source code of the system software.	Sistemos architektūra/Technology Architecture	Yes, confirmed.
NFR-6.22	Sutarties pagrindu įsigyta OEM ir trečiųjų šalių programinė įranga: • Negali būti pasiekusi „gyvavimo ciklo pabaigos“ etapo per visą sutarties galiojimo laikotarpį. • Turi turėti aiškiai apibrėžtus vystymo ir palaikymo planus.	OEM and third-party software purchased under a contract: • Must not have reached the "end of life" stage during the entire contract period. • Must have clearly defined development and support plans.	Sistemos architektūra/Technology Architecture	Yes, confirmed.

Nr.	Reikalavimas	English	Reikalavimo tipas / Requirement category	NFR/Sutartis/Tech spec
NFR-7.1	Siūloma Sistema turi būti realizuota taip, kad pereinant prie aukštesnės Sistemos aplikacijų versijos, nereikėtų atlikti infrastruktūros atnaujinimo ar technologinės platformos atnaujinimo darbų (išskyrus tuos, kuriuos standartiškai rekomenduoja Sistema gamintojas, pereinant iš vienos versijos į kitą).	The offered System shall be implemented so that infrastructure or technological platform would not require upgrade in case of transition to the higher System application version (excluding those recommended by Sistema manufacture as standard during transition from one version to another).	Versijų atnaujinimas/Version renewal	The offered System shall be implemented so that infrastructure or technological platform would not require upgrade in case of transition to the higher System application version (excluding those recommended by Sistema manufacture as standard during transition from one version to another). The System shall include measures ensuring possibility to maintain modifications and configurations made in database level in case of replacement and/or version upgrade of the System and/or its components. The System shall be implemented so as to ensure possibility to carry out migration of all data without additional service and license purchasing from the implementer / System manufacturer in case of upgrade related to architecture components and/or database replacement.
NFR-7.2	Sistemoje turi būti priemonės, užtikrinančios, kad atliekant Sistemos ir (ar) atskirų jos komponentų pakeitimą ir (ar) atnaujinimą, turi būti galimybė išlaikyti duomenų bazės lygmenyje atliktus pakeitimus ir konfigūracijas.	The System shall include measures ensuring possibility to maintain modifications and configurations made in database level in case of replacement and/or version upgrade of the System and/or its components.	Versijų atnaujinimas/Version renewal	
NFR-7.3	Sistema turi būti realizuota taip, kad atliekant atnaujinimus, susijusius su architektūriniais komponentais ir / ar keičiant duomenų bazę, būtų galimybė atlikti visų duomenų migravimą be papildomų paslaugų ir licencijų įsigijimo iš diegėjo / Sistema gamintojo.	The System shall be implemented so as to ensure possibility to carry out migration of all data without additional service and license purchasing from the implementer / System manufacturer in case of upgrade related to architecture components and/or database replacement.	Versijų atnaujinimas/Version renewal	

NFR-7.4	Sistemoje atliekant pakeitimą ir / ar atnaujinimą, turi būti galimybė užtikrinti, kad: - Visi saugomi duomenys bus perkelti į naują duomenų bazės struktūrą; - Bus išlaikytas duomenų vientisumas ir integralumas; - Jokie saugomi duomenys nebus prarasti; - Nebus sutrikdytas Sistemoje realizuotas funkcionalumas.	In case of version replacement and/or upgrade in the System the following shall be ensured: - All stored data shall be relocated to the new database structure; - Data consistency and integrity shall be maintained; - No stored data shall be lost; - Functionality implemented in the System will not be affected.	Versijų atnaujinimas/Version renewal	In case of version replacement and/or upgrade in the System the following shall be ensured: - All stored data shall be relocated to the new database structure; - Data consistency and integrity shall be maintained; - No stored data shall be lost; - Functionality implemented in the System will not be affected.
NFR-7.5	Sistemos techninės ir / arba programinės įrangos modifikavimas, tobulinimas ir klaidų taisymas negali turėti įtakos anksčiau įvestų duomenų vientisumui.	Modification, improvement and debugging of System's hardware and/or software shall not affect integrity of previously entered data.	Versijų atnaujinimas/Version renewal	improvement and debugging of System's hardware and/or software
NFR-7.6	Sistema turi būti realizuota taip, kad atliekant atnaujinimus, susijusius su architektūriniais komponentais (aparatine įranga, serverių virtualizacijos, DB platformos), būtų galimybė tai atlikti be papildomų paslaugų ir licencijų įsigijimo iš diegėjo / Sistemos gamintojo.	The system must be implemented in such a way that during the upgrades related to architectural components (hardware, server virtualization, DB platforms), it must be possible to do so without purchasing additional services and licenses from the implementer / System manufacturer.	Versijų atnaujinimas/Version renewal	The system must be implemented in such a way that during the upgrades related to architectural components (hardware, server virtualization, DB platforms), it must be possible to do so without purchasing additional services and licenses from the implementer / System manufacturer.

NFR-7.7	Tiekėjas turi prižiūrėti ir teikti palaikymą visoms Sistemos programinėms dalims iki Sistemos priežiūros ir aptarnavimo bei garantinės priežiūros laikotarpio pabaigos. Tai turi būti taikoma, šiems komponentams, bet neapsiribojant pateiktu sąrašu: • Paslaugos ir palaikymas • Grafinė sąsaja • Duomenų bazė ar kita duomenų saugojimo platforma • Integracinė sąsaja • Sistemos administravimo priemonės • Programavimo įrankiai, diagnostiniai įrankiai	The Supplier shall maintain and provide support to all System software parts till maintenance and support period expiration. This shall apply for the following components, but not limited to: • Services and support • GUI • Database or other data storage platform • Integration interface • System administration tools • Programming tools, diagnostic tools	Priežiūros garantijos/Maintenance Warranties	The Supplier shall maintain and provide support to all System software parts till maintenance and support period expiration. This shall apply for the following components, but not limited to: • Services and support • GUI • Database or other data storage platform • Integration interface • System administration tools • Programming tools, diagnostic tools
NFR-7.8	Programinės įrangos garantinis aptarnavimas ir Sistemos priežiūros ir aptarnavimo paslaugos turi apimti ir palaikyti tiekėjo, OEM ir trečių šalių programinę įrangą, kuri buvo pateikta sutartyje.	The software technical support shall apply to Supplier-, OEM-, and third-party provided software that was included in the contract	Priežiūros garantijos/Maintenance Warranties	The software technical support shall apply to Supplier-, OEM-, and third-party provided software that was included in the contract
NFR-7.9	Sistema turi palaikyti įvykiais grįstus pranešimus (angl. event-based alarm) arba turėti pasyvias sistemos veikimo patikrinimo (angl. passive health check probe) funkcijas.	System shall support event-based alarm reporting or support passive health check probe(s)	Priežiūros garantijos/Maintenance Warranties	System shall support event-based alarm reporting or support passive health check probe(s)
NFR-7.10	Sistemos apdorojamų duomenų apimtys ir jų panaudojimas neturi būti ribojamas licencijomis.	The amount of information processed by the System must not be limited by licenses.	Licencijos/Licencing	The amount of information processed by the
NFR-7.11	Perkama programinė įranga turi būti licencijuojama.	The purchased software has to be licensed.	Licencijos/Licencing	The purchased software has to be licensed.