____

Date of the Agreement

AGREEMENT
(the "**Agreement**")

BETWEEN

EDGE Strategy AG
Neuhofstrasse 4, 6340 Baar, Switzerland
("**EDGE Strategy**")

AND

UAB "Ignitis grupės paslaugų centras"
Laisvės pr. 10, 04215 Vilnius, Lithuania
("**Client**")

(each Party hereinafter referred to individually as a "Party" or collectively as "Parties")

WHEREAS:

1. EDGE Strategy holds the exclusive right to the use of EDGE Certified Foundation's assessment methodology for gender and intersectional equity. Among the four pillars of this methodology is the gender and/or intersectional equity pay gap analysis, for which EDGE Strategy has developed a premium and customizable solution known as the EDGE Empower Pay Tool an offline proprietary software that enables organizations to assess the high-level risks associated with pay equity.

2. The Client wishes to use the EDGE Empower Pay Tool to assess the unexplained gender and/or intersectional equity as the case might be, pay gap.

[Remainder of the page left blank intentionally]

THE PARTIES AGREE TO THE FOLLOWING

1. SCOPE

1.1 EDGE Strategy will provide the Client with access to the EDGE Empower Pay Tool as outlined in Appendix A, for the scope specified therein.

The EDGE Empower Pay Tool enables the Client to assess the high-level risks associated with pay equity, focusing on gender, for the entities specified in Appendix A. If the EDGEplus add-on is included in the scope, as detailed in the List of Services and Pricing in Appendix A, the tool can also assess risks related to race/ethnicity and nationality.

1.2 EDGE Strategy will also provide the Client with up to four (4) hours of generic support in the use of the EDGE Empower Pay Tool for each of the entities specified in Appendix A.

1.3 The Client bears sole responsibility for the use, storage, integrity, and accuracy of this data, as well as the use of the EDGE Empower Pay Tool. Any sub-licensing or further licensing of the EDGE Empower Pay Tool is strictly prohibited. The Client is not entitled to create or possess a copy or backup of the EDGE Empower Pay Tool. The Client will ensure that the users adhere to the standard terms and conditions for the use of the EDGE Empower Pay Tool as outlined in Appendix B to this Agreement. Access to the EDGE Empower Pay Tool will not be granted without such agreement.

2. TERM AND TERMINATION

2.1 Subject to the termination provisions contained herein, this Agreement enters into force on the date of last signature and activation of the EDGE Empower Pay Tool Gender Binary Licence for an initial term of one (1) year (the "**Initial Term**"). The Initial Term may be extended for an agreed period of time only by a separate agreement between the Parties.

2.2 Agreement amendments of technical nature (for example, mistakes of the Parties, names, account numbers, contact details, other details, etc.) shall not be considered as amendments of the contract conditions. The Party shall inform the other Party in writing in advance about amendments of technical nature, a separate confirmation of the other Party shall not be provided. For the avoidance of doubt, the Parties shall agree that, after the Parties complete the conditions provided for in this paragraph, a separate agreement regarding contract amendment shall not be concluded, and the notice one Party provided to another Party shall be added to the Agreement and considered an integral part of the Agreement.

2.3 Other Agreement conditions (non-technical in nature) can be amended or supplemented only by mutual agreement of the Parties, when the amendment or supplementation is provided for in the Agreement and/or is permissible pursuant to the legal acts regulating public procurement. Agreement amendments and supplementations of such nature shall be concluded in writing and properly signed by both Parties.

2.4 Each Party may give written notice of immediate termination of this Agreement, if:

a) The other Party (including any user) fails to comply with a material term or condition of this Agreement,
b) The other Party breaches this Agreement and has not rectified the breach after thirty (30) days of written notification from the non-breaching Party,
c) In one Party's reasonable opinion the other Party has acted in such a way as to cause reputational or other harm or negative publicity to the other Party,
d) Either Party should become insolvent or start negotiations about composition with its creditors or a petition in bankruptcy should be filed by it or it should make an assignment for the benefit of its creditors or cancel its payments.

and if such circumstances have not been rectified within the term provided by the Party, which in all cases should be not less than 10 (ten) calendar days from the submission of written notice.

2.5 The Client shall have the right to terminate the Agreement by giving written notice to EDGE Strategy 60 (sixty) days before the moment of termination.

2.6 The Client shall be entitled to terminate the Agreement due to a substantial breach of the Agreement by EDGE Strategy, if EDGE Strategy, including any entity associated with EDGE Strategy, 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 Client or the Companies of Ignitis Group as an incentive or reward for any action or omission taken in relation to this Procurement or the Agreement, or for showing favour or disfavour or refraining from doing so (bribe) to any entity associated with this Agreement. In the event of termination of the Agreement by the Client on these grounds, EDGE Strategy shall compensate all costs incurred by the Client in relation to finishing of implementation of the Agreement as well as compensating all and any losses incurred as a result of termination of the Agreement.

2.7 Upon termination of this Agreement for whatever reason, the Client will destroy or return any Proprietary Information supplied by EDGE Strategy in connection to the EDGE Empower Pay Tool.

3. PRICE

3.1 The total fee payable to EDGE Strategy for the use of the EDGE Empower Pay Tool, as detailed in section 1 above, shall be as set out in Appendix A, excluding VAT and any other applicable taxes.

3.2 The fee will be invoiced, and payment received before the EDGE Empower Pay Tool is made available to the Client. EDGE Strategy shall provide an invoice to the Client for the use of the EDGE Empower Pay Tool not later than five (5) calendar days after signing this Agreement. In addition, EDGE Strategy undertakes to provide full access to EDGE Empower Pay Tool once the respective payment is received, but in all cases not later than one (1) business day.

3.3 All invoices issued by EDGE Strategy are payable within thirty (30) days of receipt of an invoice. Invoices issued shall remain payable and paid invoices shall be non-refundable.

3.4 Further work undertaken by EDGE Strategy at the request of the Client beyond what is set out in this Agreement will be subject to additional costs of CHF 2'500.00 per day for such additional services.

3.5 The Client shall reimburse EDGE Strategy for all reasonable expenses incurred in the provision of the services hereunder (including travel expenses at the Client requests). All expenses shall be pre-approved by the Client in writing or by e-mail. This provision shall apply only for additional services ordered by the Client, which are not included in the scope of this Agreement.

3.6 All payments under this Agreement shall be made in Swiss Francs (CHF). For payment in currencies other than CHF, a surcharge to the prevailing spot exchange rate will be applied to account for banking fees and exchange rate fluctuations. For payments in Euro (EUR) or in United States Dollar (USD) the surcharge amounts to 3% of the amount invoiced in CHF. Surcharges for payments in other currencies are available upon request.

3.7 When performing a procurement contract, invoices shall be provided only by electronic means. Electronic invoices, complying with the European standard on electronic invoicing, 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' (OJ 2017 L 266, 19) (hereinafter – European standard on electronic invoicing), shall be provided by the supplier's means of choice. Electronic invoices failing to comply with European standard on electronic invoicing can be provided only by using the tools of the information system "E. sąskaita".

4. SERVICE ACCESS

4.1 Throughout the term of the Agreement, EDGE Strategy will provide the Client with the necessary technical support, maintenance, upgrades, modifications or new releases of the EDGE Empower Pay Tool. Client's requests for technical support will be monitored by EDGE Strategy during standard CET business hours.

4.2 Throughout the term of the Agreement, while EDGE Strategy endeavours to ensure that the EDGE Empower Pay Tool is normally available 24 hours a day and 7 days per week, EDGE Strategy shall not be liable if for any reason the EDGE Empower Pay Tool is unavailable at any time or for any period.

4.3 Access to the EDGE Empower Pay Tool may be suspended temporarily due to maintenance or repair, or for circumstances beyond EDGE Strategy's control, such as unplanned outages or other external factors. In such cases, EDGE Strategy will endeavour to inform the Client in a timely manner.

4.4 EDGE Strategy makes no warranties or claims as to the performance of the EDGE Empower Pay Tool in the Client's computer environment.

5. INTELLECTUAL PROPERTY RIGHTS

5.1 The EDGE Empower Pay Tool including, without limitation, their database, table structures, and reports, their arrangement, organisation, and methods of interactions, the algorithms and other database artefacts, the online platform's structure, all textual and graphical materials, and all technical information and other content appearing on the online platform and their modifications and enhancements (the "**Proprietary Information**") are confidential and trade secret information that is proprietary to EDGE Strategy, together with all related copyrights and trademarks.

5.2 EDGE Strategy retains the exclusive and sole ownership of the EDGE Empower Pay Tool, as well as all Proprietary Information and related intellectual property rights. The Client agrees to hold all Proprietary Information in strictest confidence. The Client may not provide any of the Proprietary Information in any form to any person other than members of Client's management team and/or its supervisory bodies. The provision of Proprietary Information to any of the Client's employees (other than the users, members of Client's management team and/or its supervisory bodies), the general public or any third parties is permitted only with the prior written consent of EDGE Strategy and always provided that the Client strictly adheres to the provisions of clauses 5.3 and 5.4 hereafter at all times when providing Proprietary Information to any third parties.

5.3 The Client is permitted to print and download extracts from the EDGE Empower Pay Tool for their own internal use on the following basis:

a) No documents or related graphics on the EDGE Empower Pay Tool are modified in any way,
b) No graphics on the EDGE Empower Pay Tool are used separately from the corresponding text,
c) EDGE Strategy's copyright notice and the registered trademark symbol (®) associated with the respective registered trademarks must appear on all copies without exception.

5.4 No part of the EDGE Empower Pay Tool may be copied, reproduced, republished, modified, uploaded, posted, framed, transmitted, or distributed in any way other than in accordance with clause 5.3 above. No part of the EDGE Empower Pay Tool may be decompiled, reverse engineered, or disassembled, nor attempts to recreate the source code of the EDGE Empower Pay Tool may be permitted.

5.5 Any rights not expressly granted in this Agreement are reserved.

6. DATA PROTECTION AND CONFIDENTIALITY

6.1 This Agreement is entered into on the basis that each Party has complied with its obligations arising from the data protection and privacy laws in force and applicable to it, to the extent that those obligations are relevant to this Agreement.

6.2 To the extent that EDGE Strategy processes personal data controlled by the Client, EDGE Strategy confirms that it will act only on Client's instructions and that any processed data is used to provide the service to the Client and is handled in accordance with EDGE Empower's Data Privacy Policy (https://edgeempower.com/data-privacy-policy/).

6.3 The Client will run the offline EDGE Empower Pay Tool independently on its own systems. Any data input into the EDGE Empower Pay Tool will be stored exclusively on the Client's local computers and/or servers, remaining solely in the Client's possession and ownership. EDGE Strategy will not access, collect, retrieve, store, or process in any way the Client's data in any form in relation to the services under the Section 1 of this Agreement.

6.4 The Parties do hereby agree to keep this Agreement 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 Agreement as well as other information discovered/recorded/filmed, etc. in any other manner within the course of implementation of the Agreement. The Parties hereunder do hereby agree not to disclose any confidential information to any third parties without a prior written consent of the other Party, and also not to use any confidential information for personal or third parties 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. All information provided by the Client to EDGE Strategy as well as other information developed/discovered within the course of implementation of the Agreement shall be considered as confidential, except for publicly available information and the Procurement Documents; in all other cases the Client shall confirm in writing that certain provided information is not confidential.

7. EXTERNAL COMMUNICATIONS

7.1 EDGE Strategy undertakes not to use the Client's and Ignitis Group companies' trademark(s) and/or name in any promotional material, publications or elsewhere without a prior written consent of the Client.

7.2 Throughout the term of the Agreement, the Client may publicly describe themselves as a Client of EDGE Strategy.

8. DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITY

8.1 The Client accepts the EDGE Empower Pay Tool “AS-IS”, in their present condition and without any warranty, express or implied, and also acknowledges the Terms & Conditions for their use as attached in Appendix B.

8.2 The Client is solely responsible for determining the suitability of the EDGE Empower Pay Tool for their business. The EDGE Empower Pay Tool carry out analyses based on a set of specific inputs entered by the Client, and it does not predict future events nor the likelihood of any particular scenario occurring. The validity of the results depends on the validity of the Client’s input and EDGE Strategy does not make any representations or warranties of any kind, express, statutory, or implied, including (without limitation) regarding accuracy, timeliness, completeness, merchantability, fitness for any particular purpose, of any outcomes or outputs provided by the EDGE Empower Pay Tool.

8.3 In no event will EDGE Strategy be liable to the Client or to any third Party for any decision made or action taken in reliance upon the results obtained through the use of, or the information contained in or provided by the EDGE Empower Pay Tool. The Client assumes sole responsibility for results obtained from the use of the EDGE Empower Pay Tool, as well as its underlying data, and for any conclusions the Client may draw from such results. If the Client uses the results given as the basis for any decision making, the Client does so at its own risk.

8.4 In no event shall EDGE Strategy be liable for any damages, losses or expenses, including without limitation, direct, indirect, special, incidental, or consequential damages, losses or expenses based on breach of contract, including but not limited to, loss of profits, revenues, anticipated savings, business or investment opportunities, or internal or management costs, based on any theory of liability arising in connection with the use or interpretation of the information on The EDGE Empower Pay Tool or any information on a linked site, the inability to use such information, or any failure of performance, error, omission, interruption, defect, delay in operation or transmission, computer virus or telecom line or systems failure.

8.5 Nothing in this Agreement will exclude or limit the liability of either Party for:

a) Death or personal injury caused by its negligence,
b) Fraud or fraudulent misrepresentation,
c) Any other liability the exclusion of which is expressly prohibited by law.

8.6 The Parties shall be liable for non-performance or improper performance of their contractual obligations in accordance with the procedure established in the Agreement and legal acts. Indemnification and payment of penalties shall not exempt a Party from the proper performance of the provisions of the Agreement.

9. APPLICABLE LAW AND JURISDICTION

9.1 This Agreement shall be governed by, construed, and interpreted in accordance with the laws of the Republic of Lithuania, without reference to its conflict of law rules. Disputes arising between the Parties regarding the terms and conditions of the Agreement and/or its performance shall be resolved by negotiation. If the dispute cannot be resolved by negotiation within 30 (thirty) calendar days from the date of written notification by one Party to the other Party, all disputes shall be finally settled by arbitration in accordance with the Arbitration Rules of the Arbitration Institute of the Stockholm Chamber of Commerce (hereinafter referred to as the Arbitration), with the participation of one arbitrator. The seat of arbitration shall be Stockholm. The language to be used in the arbitral proceedings shall be English.

10. MISCELLANOUS

10.1 If any provision of this Agreement is held to be invalid or unenforceable in whole or in part, the validity of all other provisions shall not be affected, and such other provisions shall be carried out as if the invalid or unenforceable provisions were not contained herein.

10.2 This Agreement represents the entire undertaking between the Parties and supersedes all prior negotiations, representations, or contracts, either written or oral. This Agreement shall not be changed, replaced, amended, or otherwise altered without the written approval of the Parties.

10.3 This Agreement may not be assigned, in whole or in part, by either Party without the other Party’s prior written consent.

10.4 Nothing in this Agreement shall be construed to create a partnership, joint venture, or employer-employee relationship.

10.5 The Parties hereby agree that if any clause of the Agreement and/or its annexes contradicts the provisions of the legal acts regulating public procurement and/or the terms and conditions of the Public Procurement performed by the Client, the provisions of the legal acts regulating public procurement and/or the terms and conditions of the Public Procurement performed by the Client shall prevail and apply to the relations between the Parties.

10.6 EDGE Strategy shall familiarise with and, in its relations with the Client and the third parties engaged for the purpose of the implementation of the Agreement, 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 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. EDGE Strategy shall ensure that the requirements of this paragraph will be complied with by employees, members of supervisory bodies and other representatives of both

EDGE Strategy and the third persons engaged for the performance of the Agreement;

10.7 EDGE Strategy must immediately inform about any circumstances occurring within the course of the validity period of the Agreement, which could make the Agreement 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.

10.8 EDGE Strategy is familiar with the fact that AB “Ignitis grupė” has issued financial instruments, which are available 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. EDGE Strategy 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.

10.9 EDGE Strategy hereby acknowledges and confirms that both at the time of the conclusion of the Agreement and for the entire period of its validity EDGE Strategy (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 Agreement. EDGE Strategy shall immediately notify the Client 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 Client has the right to claim compensation for direct losses incurred by EDGE Strategy in violation of the obligations.

When the circumstances referred to in this paragraph of the Agreement become apparent, the Client has the right to suspend the performance of the Agreement for the period of validity of sanctions or unilaterally terminate the Agreement by notifying EDGE Strategy in writing within 1 (one) working day from the date of dispatch of the notice of suspension or unilateral termination of the Agreement 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 Agreement on the basis specified in this clause of the Agreement.

10.10 This Agreement may be either:

a) Executed electronically via DocuSign or any other similar means of electronic signatures where such electronically executed Agreement shall be deemed to be an original and binding on the Parties, or,

b) Executed in two counterparts, each of which is an original and which together have the same effect as if each Party had signed the same document. In this case, transmission of the executed signature page of a counterpart of this Agreement by email (in PDF, JPEG or other agreed format) shall take effect as delivery of an executed counterpart of this Agreement. For the avoidance of doubt, no counterpart shall be effective until each Party has executed and delivered at least one counterpart.

10.11 The Appendices listed below shall form an integral part of this Agreement.

10.12 All reports and notifications under this Agreement must be written in English.

THE FOLLOWING APPENDICES ARE INTEGRAL PART OF THIS CONTRACT:

APPENDIX A:	Scope and Pricing
APPENDIX B:	Terms and conditions for the use of EDGE Empower
APPENDIX C:	NFR template SaaS

[SIGNATURE PAGE FOLLOWS]

SO AGREED

APPENDIX A | Scope, List of Services and Pricing for UAB "Ignitis grupės paslaugų centras"

Prices are quoted in Swiss francs.

	Lithuania
Access to EDGE Empower® Pay Tool **Gender Binary**	8'500.00

APPENDIX B | TERMS AND CONDITIONS FOR THE USE OF EDGE EMPOWER

THIS APPENDIX CONTAINS A COPY OF THE TERMS AND CONDITIONS EMBEDDED IN EDGE EMPOWER AND/OR IN THE EDGE EMPOWER PAY TOOL INCLUDED THE EDGEPLUS ADD-ON IN THE LATTER AS THE CASE MAY BE, WHICH MUST BE ACCEPTED BY THE END USER BEFORE THEIR RESPECTIVE USE.

IMPORTANT LEGAL NOTICE - PLEASE READ CAREFULLY AND IN ITS ENTIRETY BEFORE USING EDGE EMPOWER.

BY PROCEEDING ACCESSING AND USING EDGE EMPOWER, YOU INDICATE YOUR PERSONAL ACCEPTANCE AND THE ACCEPTANCE ON BEHALF OF YOUR ORGANIZATION OF THE TERMS AND CONDITIONS AS SET OUT IN THIS COVENANT AND THAT YOU HAVE THE AUTHORITY TO ENTER INTO THIS COVENANT, AND ACCORDINGLY, REFERENCES TO "YOU" MEAN REFERENCES TO YOU PERSONALLY AND YOUR ORGANIZATION.

1. Scope of Application

These Terms and Conditions ("**T&C**") are issued by EDGE Strategy LTD, Neuhofstrasse 4, 6340 Baar, Switzerland ("**EDGE Strategy**") and apply to the Services (the "**Services**") provided according to the Agreement ("**Agreement**") between your organization and EDGE Strategy or its authorized licencing partners. The Services include, but are not limited to the access and the use of EDGE Empower with its components, as described below, as well as its entire content, via the Internet (Software-as-a-Service) under the domain name https://assessment.edge-strategy.com and/or to the provision and the use of the EDGE Empower Pay Tool, included the EDGEplus add-on as the case may be, and to any correspondence between EDGE Strategy and you ("**You**") in relation to the Services and/or any other prestation.

These T&C serve as an appendix to the Agreement between your Organization and EDGE Strategy or its authorized licencing partners, and their provisions have been accepted by your Organization upon the execution of the Agreement. To the extent that the provisions contained in these T&C are inconsistent with those contained in the Agreement between your organization and EDGE Strategy or its authorized licencing partners, the terms and provisions contained in the former shall prevail. Otherwise, such provisions shall be considered cumulative.

2. Services Provided by EDGE Strategy

2.1 Right of use

To the extent provided for in the Agreement, EDGE Strategy grants you access to EDGE Empower through the internet as a Software-as-a-Service solution, and all its components:

a) EDGE Insights, to measure DE&I with both quantitative and qualitative indicators,
b) EDGE Knowledge, providing DE&I practical guidance and support,
c) EDGE Connections, an access to a network of DE&I and human resources professionals for mutual learning and collaborative exchange,
d) Preparation for the EDGE Certification based on the outputs derived from EDGE Insights.

You are granted a limited, personal, non-exclusive, non-transferable, non-assignable licence, without rights to sublicense, to display and use EDGE Empower by means of a browser and an internet connection and solely for internal business purposes, and solely for the type of user expressly permitted by EDGE Strategy. You are not entitled to further rights associated with EDGE Empower, such as ownership, copyright, patent, trademark, or usage rights. You are solely responsible for the internet connection between your network/computer and the server hosting EDGE Empower, as well as for the necessary hardware and software (e.g., personal computer, network connection, browser).

Upon gaining access to EDGE Empower, you are also allowed to use EDGE Connection. This component enables you to post content ('User Content') that can be accessed by EDGE Strategy's staff member and other users of EDGE Empower.

You are solely responsible for any User Content you post and must ensure that you have all necessary permissions to publish such content. You guarantee to EDGE Strategy that you have the right to share your User Content according to the selected sharing options and to grant EDGE Strategy the license described below. You also guarantee that your User Content does not violate third-party rights, including intellectual property rights.

By posting User Content, you retain all ownership rights in your User Content, yet you provide EDGE Strategy a global, royalty-free, perpetual, transferable, and non-exclusive license to use, alter, adapt, translate, and disseminate by any means your User Content as necessary to operate EDGE Empower and deliver the Services. You also waive, and irrevocably commit to waive, any moral rights you may hold with respect to User Content in the context of the license mentioned above, in favour of EDGE Strategy, as well as its successors and assigns. We reserve the right to remove any User Content posted in violation of these T&C or considered inappropriate at our sole discretion.

In case you use the EDGE Empower Pay Tool, alone or in conjunction with EDGE Empower, you are granted a limited, personal, non-exclusive, non-transferable, non-assignable licence, without rights to sublicense, to use EDGE Empower Pay Tool solely for internal business purposes. You are not entitled to further rights associated with the EDGE Empower Pay Tool, such as ownership, copyright, patent, trademark, or usage rights. EDGE Strategy does not access, collect, retrieve, store, or process in any way any data entered into the EDGE Empower Pay Tool, and you are solely responsible for the use, storage, integrity and accuracy of such data.

2.2 Restrictions

You will not, directly or indirectly: reverse engineer, decompile, disassemble or otherwise attempt to discover the source code, object code or underlying structure, ideas, know-how or algorithms relevant to the Services provided, or any documentation or data related to the Services; modify or create derivative works based on the Services provided; or remove any proprietary notices or labels.

You are permitted to print and/or download extracts from the Services for your organization's internal use on the following basis:

a) No documents or related graphics on the Services may be modified in any way.
b) No graphics on the Services may be used separately from the corresponding text.
c) EDGE Strategy's copyright notice and the registered trademark symbol (®) associated with the respective registered trademarks must appear on all copies without exception.

2.3 Operation

EDGE Strategy endeavours to take appropriate measures to make it possible for you to use the Services as interruption-free as possible. EDGE Strategy cannot guarantee availability of the Services at all times and absence of any other disruptions and interruptions to its functioning.
You shall notify EDGE Strategy of any disruptions to the Services without delay and provide information regarding the details of the circumstances of the issue by sending an email to support@edge-strategy.com. EDGE Strategy shall remedy the disruption to the Services within an appropriate period of time.

2.4 User Login, User Conduct and Data Protection (EDGE Empower only)

The use of EDGE Empower requires that you become a registered user, as designated by your organization, by providing your email address. The email address you provide will be used for ensuring secure access to and use of EDGE Empower, as well as the recoverability of your user credentials for the duration of the Agreement. We may also use your email address (1) to notify you about new features, updates, and enhancements to EDGE Empower, as well as any other important news related to the use of EDGE Empower and, (2) to introduce your organisation to certification bodies, accredited and approved by the EDGE Certified Foundation, and who perform audits and certification processes in relation to the EDGE Standard.

Each login is for a single user only, *i.e.* for only one natural person. Logins and passwords are strictly personal and non-transferable. Strict confidentiality is mandatory with respect to authorisation codes or passwords. EDGE Strategy does not permit you to share your username and password with any other person or with multiple users on a network.

You are responsible for all activities that occur under your login, whether authorised by you or not, and successive use of equipment used with this login. You must take all reasonable measures to protect your login information and shall immediately notify EDGE Strategy on becoming aware of any unauthorised access to user logins, and passwords. You may not link EDGE Empower from any other website, without EDGE Strategy's express prior written permission.

Your use of EDGE Empower and its components, must, at all time, be lawful and comply with these T&C. Prohibited activities include, but are not limited to: (i) Breaching these T&C; (ii) Engaging in harmful, illegal or offensive behaviour; (iii) Harassing others; (iv) Sending spam; (v) Spreading malware; (vi) Promoting illegal activities; (vii) Illegally soliciting personal information; (viii) Disrupting the website or its network; (ix) Unauthorized collection of user names; or (x) Violating any applicable laws or regulations.

You acknowledge that EDGE Strategy may use third-party survey builder, data collection platforms and/or analytical. It is also possible that in certain interactions, cookies are delivered by the use of EDGE Empower. For more details, please refer to EDGE Empower Data Privacy Policy (https://edgeempower.com/data-privacy-policy/).

2.5 Support

In support of use of the Services, EDGE Strategy shall provide support. The support shall not include: general know-how transfer, trainings, configuration implementation or client-specific documentation or modification of the Services.

Support shall be carried out by email to support@edge-strategy.com. EDGE Strategy shall provide the support services during standard CET business hours.

2.6 Feedback

EDGE Strategy welcomes your suggestions, proposals, ideas, recommendations, or other feedback regarding improvements to our Services and related resources ("Feedback"). By providing Feedback, you grant EDGE Strategy and its affiliates a royalty-free, fully paid, sublicensable, transferable, non-exclusive, irrevocable, perpetual, worldwide right and license to make, use, sell, offer for sale, import, and otherwise exploit the Feedback (including by incorporating it into our Services) without restriction. For the avoidance of doubt, Feedback does not constitute your confidential information.

3. EDGE Strategy Data and Intellectual Property

The Services including, without limitation, their database (except for your organization's own data), table structures, and reports, their arrangement, organization, and methods of interactions, the algorithms and other database artefacts, the online platform's structure, all textual and graphical materials, and all technical information and other content appearing on the online platform and their modifications and enhancements (the "Proprietary Information") are confidential and trade secret information that is proprietary to EDGE Strategy, together with all related copyrights and trademarks.

EDGE Strategy retains the exclusive and sole ownership of the Services, as well as all Proprietary Information and related intellectual property rights. This includes, but is not limited to, ownership of registered trademarks for EDGE Insights, EDGE Knowledge and EDGE Connections, as well as the distinctive tagline of EDGE Empower. Furthermore, EDGE Strategy holds the exclusive license to use the registered trademark of EDGE Certification. You agree to hold all Proprietary Information in strictest confidence. You may not provide any of the Proprietary Information in any form to any person except to another user as defined by your organization. The provision of Proprietary Information to any of your organization's employees (other than users, members of your organization's management team and/or its or their supervisory bodies), the general public or any third parties is permitted only with the prior written consent of EDGE Strategy.

Any rights not expressly granted to you are reserved by EDGE Strategy.

4. Disclaimer of Warranties and Limitation of Liability

The Services are provided to you "AS-IS", in their present conditions and without any warranty, express or implied.

In no event will EDGE Strategy be liable to you or to any third party for any use of the Services or any decision made, or action taken in reliance upon the results obtained through the use of, or the information contained in or provided by the Services.

In no event shall EDGE Strategy be liable for any damages, losses or expenses, including without limitation, direct, indirect, special, incidental, or consequential damages, losses or expenses, including but not limited to, loss of profits, revenues, anticipated savings, business or investment opportunities, or internal or management costs, based on any theory of liability arising in connection with the use or interpretation of the information on EDGE Empower or any information on a linked site, the inability to use such information, or any failure of performance, error, omission, interruption, defect, delay in operation or transmission, computer virus or telecom line or system failure.

Nothing in these T&C will exclude or limit the liability of either party:

a) For death or personal injury caused by its negligence.
b) For fraud or fraudulent misrepresentation.
c) Any other liability which may not be excluded by law.

5. Final Provisions

5.1 Amendments to these T&C

These T&C may be amended at EDGE Strategy's sole discretion as new features, technology, or legal requirements arise. EDGE Strategy will notify you of any amendments to these T&C (**"Updated T&C"**) upon your log-in to EDGE Empower or trough the provision of an updated version of the EDGE Empower Pay Tool, included the EDGEplus add-on as the case may be.

5.2 Severability clause

Should individual provisions of these T&C be invalid or incomplete or should performance be impossible, this shall not negatively affect the validity of the remaining provisions of these T&C. Invalid provisions shall be replaced by an admissible, valid provision that is as close as possible to the content of the original in terms of its intent.

5.3 Date of contract conclusion

As an integral part of the Agreement, these T&C have been accepted by your Organization upon its execution. You are deemed to have accepted the T&C by clicking "Agree" at the bottom of the screen during your first access to the Services.

Any updates or amendments to these (T&C) will have immediate effect. Your continued use of the Services after any such update constitutes your acceptance of the modified T&C. Any previous versions of the T&C will be invalidated upon the implementation of these updates. It is your responsibility to review the T&C regularly to stay informed about any changes.

5.4 Breach and Termination

Any breach of any of the terms of these T&C will constitute a material breach of your organization's agreement with EDGE Strategy and your and your organization's permission to use the Services will automatically terminate.

Upon termination of these T&C for whatever reason, you will immediately destroy all Proprietary Information either supplied by EDGE Strategy in connection to your use of the Services or printed and/or downloaded, being reminded the restriction provisioned under section 3.2 of these T&C.

You are not permitted to keep copies in any form. Termination of these T&C shall not affect any rights, remedies, obligation or liabilities of EDGE Strategy that have accrued up to the date of termination, including the right to claim damages in respect of any breach of the Agreement which existed at or before the date of termination.

6. Applicable Law and Jurisdiction

These T&C shall be governed by, construed, and interpreted in accordance with the laws of Switzerland, without reference to its conflict of law rules. The courts of Zug, Switzerland will have exclusive jurisdiction in connection with all disputes arising out of or related to it.

Last updated: 11 December 2023

Nr.	Reikalavimas	Requirement	Reikalavimo tipas / Requirement category	Rangovo atsakymai/Vendor comment
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	Compliant
NFR-1.2	Paslaugų teikėjas turi turėti patvirtintą informacijos saugumo politiką (toliau – Politika) pagal Standarto reikalavimus.	The Service Provider must have an approved information security policy.	Reikalavimai paslaugų teikėjui / Requirements for Service Provider	Compliant
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	Compliant
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	Compliant
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	Compliant
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	Compliant
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	Compliant
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	Compliant
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	Compliant
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	Compliant
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	Compliant
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	Compliant

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	Compliant
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	Compliant
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	Compliant
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	Compliant
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	Compliant
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	Compliant
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	Compliant
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	Compliant
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	Compliant
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	Compliant
NFR-1.27	Tiekėjas turi reguliariai vykdyti įsibrovimo testavimus.	Service Provider must regulary do penetration tests.	Reikalavimai paslaugų teikėjui / Requirements for Service Provider	Compliant
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	Compliant
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	Compliant

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	Compliant
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	Compliant
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	Compliant
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	Compliant
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	Compliant
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	Compliant
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	Compliant
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	Compliant
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	Compliant
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	Compliant
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	Compliant
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	Compliant
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	Compliant
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	Compliant
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	Compliant
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	Compliant
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	Compliant

NFR-1.65	Sistema turi turėti bent 3 skirtingus žurnalizavimo lygius: - įspėjimai ir klaidos - visos klaidos, iškilusios 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: - warrnings & 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	Compliant
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	Compliant
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	Compliant
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	Compliant
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	Compliant
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	Compliant
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	Compliant
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	Compliant

Systems that process personal data are subject to ADA1, ADA2, and ADA3 requirements:

ADA1 – security requirements must be ensured in all systems where any personal data is processed (including storage), such as contact phone number, job title, first name, last name, etc.

ADA2 – security requirements must be ensured in systems where personal data of clients (such as identity, contracts, debts, ownership, payments, etc.) is processed, as well as employee data, insofar as it relates to the performance of work functions, tasks, or assignments.

ADA3 – security requirements must be ensured in systems used for processing employee data (for the purpose of employment relationship administration), and/or in systems where special categories of personal data are processed (such as health data, biometric data, or data concerning criminal convictions), and/or in systems where systematic and

Taikymas	Prieigų kontrolė	Access control and authentication	ADA1	ADA2	ADA3	Rangovo atsakymai / vendor comments
	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	Compliant

Nr.	Application	Reikalavimas	English	Reikalavimo tipas / Requirement category	Rangovo atsakymai/Vendor comment
NFR-4.1	To all	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	Compliant
NFR-4.2	To all	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	Compliant
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	Compliant
NFR-4.4	To all	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	Compliant
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	Compliant

Nr.	Reikalavimas	Requirement	Reikalavimo tipas / Requirement category	Rangovo atsakymai/Vendor comment
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	Compliant
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	Compliant
NFR-5.6	Sistema turi veikti pagal greitaveikos reikalavimus, kai su ja vienu metu dirbs x tiesiogiai prisijungusių vartotojų (atidarytų sesijų). y 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	Compliant
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	Compliant
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	Compliant
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	Compliant
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	Compliant
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	Compliant
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	Compliant
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	Compliant
NFR-5.16	Naudotojo sąveikos reakcijos laikas piko metu neturi viršyti 2 sekundžių, siekiant užtikrinti sklanžią vartotojo patirtį.	Response times for user interactions should remain under 2 seconds during peak usage, ensuring a seamless experience.	Sistemos darbas/Performance	Compliant
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	Compliant

Nr.	Reikalavimas	Requirement	Reikalavimo tipas / Requirement category	Rangovo atsakymai/Vendor comment
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	Compliant
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	Compliant
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	Compliant
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	Compliant
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	Compliant
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	Compliant
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 virtual infrastructure.	Sistemos architektūra/Technology Architecture	Compliant
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	Compliant

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	Compliant
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	Compliant
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	Compliant
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	Compliant
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	Compliant

Nr.	Reikalavimas	Requirement	Reikalavimo tipas / Requirement category	Rangovo atsakymai/Vendor comment
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	Compliant
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	Compliant
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	Compliant
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	Compliant

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	Compliant
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	Compliant
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	Compliant
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	Compliant
NFR-7.11	Perkama programinė įranga turi būti licencijuojama.	The purchased software has to be licensed.	Licencijos/Licencing	Compliant