Contract for the use of ClauseBuddy and Clause9

Commercial Section

To be read together with the Terms & Conditions, all prices excl. VAT

ClauseBase BV, A. Stesselstraat 9
B-3012 Wilsele - BE0723.768.270

Customer information
UAB "Ignitis grupės paslaugų centras"

Supplier information
ClauseBase BV

1. Term

Commencement Date: the date this Commercial Section is signed by the last party to sign it.

2. License to use the Platform and Usage Fees

The Contract price is 39.000,00 EUR excluding VAT.

Licenses are procured on the basis of need at such rates:

Administrator licenses or user (administrator) accounts (licenses/accounts covering the functionality specified in point 6.1.1 – 6.1.5 of the Technical Specification) – 240,00 EUR excluding VAT for license.

User licenses/user accounts (licenses/accounts covering the functionality specified in points 6.1.1 – 6.1.13 of the Technical Specification) – 80,00 EUR excluding VAT for license.

- Unlimited number of exported documents per month.

The Advanced Team Plan includes all of the following modules:

- **ClauseBuddy**:
  - Artificial Intelligence;
  - Inspiration;
  - Document analysis;
  - Quality Library;
  - Compare; and
  - Smart Templates.
- **Clause9**: all default functionalities available at the Commencement Date.

The Advanced Team Plan supports the following languages:

- English;
- Lithuanian;

- Latvian;
- Estonian;
- Polish;
- Finnish.

3. Standard Rates and payment

The following rates shall apply:

- Set-up Fee: 0 EUR.
- Initial training under the Setup Services: 15 hours at 0 EUR.

4. Guaranteed response and resolution times of support request

Incidents, meaning any deviation from the standard operation of the Software which causes an interruption to, or a reduction in quality of the Software, are classified by ClauseBase. Priority setting of the Incident is done on the basis of 2 axes:

(a) **Impact**: the amount of end-users (meaning customers using the Software) impacted by the issue

High	Affects more than 85% of average daily end-users
Medium	Affects between 15% and 85% of average daily end-users
Low	Affects less than 15% of average daily end-users

(b) **Severity**: the severity of an issue for the impacted end-users

High	Blocking for the core usage of the Software. No Work Around is available
Medium	Blocking for the core usage of the Software. A Work Around is available
Low	None blocking for the core usage of the Software

This gives the following matrix:

		Impact		
Severity		High	Medium	Low
	High	P1	P2	P3
	Medium	P2	P3	P4
	Low	P3	P4	P4

An Incident shall only exist when such can be demonstrated and reproduced using a version of the

supported release.

In relation to Incidents, ClauseBase shall adhere to the Response Times set out in the table below.

CATEGORY	RESPONSE TIME
P1 Incidents	4 Business Hours
P2 Incidents	8 Business Hours
P3 Incidents	15 Business Days
P4 Incidents	Next release

ClauseBase shall make reasonable attempts to resolve the Incident as soon as reasonably possible.

ClauseBase shall have no obligation to correct the Incident in respect of:

(a) Incidents resulting from any modifications of the Software made by any other person than ClauseBase or a third party authorised by ClauseBase;

(b) the incorrect use of the Software or the use of the Software in conflict with any instructions from ClauseBase;

(c) incidents not related to the Software.

In the event that any of the aforementioned situations would occur, ClauseBase may, after consultation with Customer, decide to correct the incident in relation to (a) and (b), or support and collaborate with Customer in the event of (c). In such case the service levels related to response time shall not apply and ClauseBase shall be entitled to invoice Customer for such correction and/or support/collaboration at its then current hourly rates.

5. Specific Conditions

This Contract was concluded during public procurement No [3034734] of the Customer, therefore any conditions set in this Contract which is not related to the procurement object, shall not apply.

The following order of precedence shall be applied in the event of conflict or inconsistency between provisions of the components of this Agreement, unless otherwise agreed:

- Proposed terms for the contract of goods
    - Technical specification
- This Commercial Section and Terms & Conditions

* * *

Electronically signed on the dates indicated in the signatures:

For the Customer:	**For ClauseBase:**
Signature:	Signature: .....

CLAUSE9 & CLAUSEBUDDY - TERMS & CONDITIONS

These Terms & Conditions apply to the use of "ClauseBuddy" and "Clause9" and all related services provided by ClauseBase BV. The entire Agreement consists of these Terms & Conditions and the Commercial Section (set forth on the invoice, or in a separate document).

1. DEFINITIONS

"Account" means the combination of a username, password, settings and personal files for a specific User.

"ClauseBase" means ClauseBase BV, Alfons Stesselstraat 9, 3012 Leuven, VAT BE0723.768.270, RPR Leuven, Belgium.

"Consultancy Services" shall mean any services rendered by ClauseBase that do not consist of Setup Services or Hosting Services — e.g. uploading the Customer's clauses, configuring the Accounts, training, clean-up of documents, legal workflow management, etc.

"Data Protection Legislation" means the GDPR and any national implementation that apply to the processing of personal data.

"Error" means a substantial, verifiable and reproducible non-conformity of the Platform with its Manual.

"Force Majeure" means any cause beyond Party's reasonable control, such as acts of God or authorities, war, fire, flood, explosion, civil commotion, electricity outages, telecom break-downs, strikes, failure of a third party, software bugs in third party software, industrial action, etc.

"Hosted Data" means any electronic data (e.g. clauses, templates, logos, PDF/DOCX files, questions, answers, accounts of Users, etc.) stored in the Platform, after being uploaded by a Customer or a User.

"Hosting Services" means the end-to-end provision of the technical environment in which the Platform resides and operates, consisting of hosting the Hosted Data and software, serving web pages and endpoints, passing on AI requests, maintaining/updating the Platform, etc.).

"Manual" means *help.clausebase.com* and *help.clausebuddy.com*

"Platform" means the proprietary web-based application that is either marketed as "Clause9" and "ClauseBuddy", respectively, or made available under another name by way of "white-labelling".

"Services" means the services provided by ClauseBase to the Customer, consisting of the Setup Services, Hosting Services and Consultancy Services.

"Setup Services" means those Services that relate to the initial setup of the Customer's Accounts. Unless otherwise indicated in the Commercial Section, the Setup Services shall be charged at the Standard Rates.

"Standard Rates" means the standard pricing for the Setup Services and Consultancy Services, as set forth in the Commercial Section.

"Term" means the term of this Agreement, from the Commencement Date.

"Usage Fees" means the fees to be paid by the Customer to ClauseBase for the use of the Platform.

"User" means a physical person who uses the Platform.

2. USE OF THE PLATFORM AND THE CONSULTANCY SERVICES

2.1. While ClauseBase may offer clauses and templates to the Customer, for inclusion in the Customer's documents, and the Consultancy Services may consist of services related to contract drafting, ClauseBase does not act as a law firm and ClauseBase does not offer the validity claims and warranties customarily offered by law firms to their clients.

2.2. To the extent Hosted Data is subject to ownership and intellectual property rights, it shall be and remain the Customer's exclusive property.

2.3. The Customer shall ensure that Hosted Data does not infringe upon any third party rights (particularly copyright), and shall have sole responsibility for its accuracy, quality and legality. Even though the Platform is advertised as a tool to accelerate the drafting of various legal documents, such tool shall not relieve the Customer and its Users of reviewing the correctness, quality and appropriateness of the Hosted Data, whether created by the Customer himself and/or through the Consultancy Services. The Customer is solely responsible to determine whether, how and where to use any Hosted Data. In light of contract automation's various subtleties, complex possible interactions between clauses/templates, as well as dependence on various "business rules" and domain-specific knowledge of the Customer, the Customer will duly test and periodically review the Hosted Data and contract automation facilities offered through the Platform, in particular when Hosted Data is created (partially or in full) through the Consultancy Services.

2.4. Each Account is bound to a single physical person and is to be treated strictly personal. Accordingly, it is strictly prohibited to share an Account between different physical persons.

2.5. The Customer shall use the Platform in accordance with the Manual (e.g., regarding operating instructions, technical warnings, intended usage, etc).

2.6. ClauseBase can remove or block any Hosted Data which third parties or authorities assert is illegal or infringes upon the rights of others. To the extent possible, ClauseBase shall inform the Customer in advance.

2.7. To allow ClauseBase to carry out its support tasks efficiently, the Customer shall organize a central point of contact within its organization, and staff this central point of contact with qualified personnel. The Customer shall report any Errors immediately on detection through the helpdesk, in a well-documented way, and shall render assistance, in all fairness, for the diagnosis, the reproduction and correction of the Error.

3. WARRANTIES

3.1. ClauseBase warrants that:

- it will deliver the Services in a professional manner;
- the Platform and Hosting Services shall substantially align with the Manual, it being understood that small deviations from the Manual will not constitute a breach of this warranty;
- it will adhere to reasonable industry standard efforts to maintain appropriate administrative, physical, and technical safeguards to protect the Hosted Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure and unauthorized access; and
- it shall use reasonable efforts to maximize the availability of the Platform, it being understood that this availability is subject to a variety of interdependent factors (such as telecommunication links), which are substantially out of the control of ClauseBase.

3.2. If the Platform or the deliverables of the Consultancy Services do not perform as warranted, ClauseBase shall undertake to correct the Errors. However, ClauseBase does not warrant that the Platform will be error free or will perform in an uninterrupted manner.

3.3. The Customer acknowledges that the access to and use of the Platform may be suspended from time to time due to unanticipated or unscheduled downtime. To the extent possible, ClauseBase shall schedule planned downtime outside Belgian working hours.

3.4. Unless explicitly agreed otherwise in writing by the Parties, any deadlines and timeframes for delivery of the Setup Services and Consultancy Services are indicative and shall not bind ClauseBase.

3.5. The Platform makes extensive use of Generative AI models, procured from third parties such as Microsoft. The Customer acknowledges that it is aware of the technology's limitations, e.g. as to how it was trained on the internet, and how it may behave unpredictable and "hallucinate". Accordingly, the Customer shall not treat these models as a substitute for legal knowledge.

3.6. In light of the software-as-a-service nature of the Platform, ClauseBase can activate a new or improved version of the Platform, add additional functionality, and modify its functioning, provided similar functionality is kept and reasonable efforts are undertaken to limit the impact for the Customer. ClauseBase can move its servers or networks to other locations or data centers within the EU.

4. FEES

4.1. Except as otherwise indicated in the Commercial Section, fees are quoted and payable in EUR, do not include any value added or similar taxes, and shall be invoiced at the Commencement Date (for non-recurring fees) or the start of each renewal (for recurring fees).

4.2. Invoices are payable within thirty days as from the invoice date.

4.3. In the event of any failure by the Customer to timely make the payments indicated above, then ClauseBase can suspend the provision of any Service until all outstanding invoices have been paid.

4.4. Complaints concerning an invoice must be submitted within one month after receipt. After this period, it will be deemed accepted.

4.5. The credits for use of the Generative AI-based functionalities granted to the Customer shall be limited to 3% of the Usage Fees

5. TERM AND TERMINATION

5.1. Unless otherwise indicated in the Commercial Section, this Agreement comes into force on the Commencement Date, with a period of twelve months.

5.2. Each Party can terminate this Agreement with immediate effect without intervention of a judge by written notice to the other Party, if the other Party commits a material breach of this Agreement and — if it is capable of remedy — fails to substantially remedy it within one month of receipt of a written notice specifying the breach and warning to terminate if the breach is not remedied within the grace period.

5.3. Each Party can terminate this Agreement without intervention of a judge with immediate effect on written notice if the other Party makes any arrangement for the benefit of its creditors; or if a receiver, administrator or similar officer is appointed over a part of the assets or undertaking of the other Party; or if the other Party goes into liquidation, save for the purposes of a genuine amalgamation or reconstruction.

5.4. After termination of this Agreement, each Party shall, upon request, return or destroy the other Party's Confidential Information. ClauseBase shall then, upon request made within thirty days after the termination, remove the Hosted Data, or provide the Customer with limited access to the Platform, for the sole purpose of enabling the Customer to copy the Hosted Data. After this period, ClauseBase shall have no obligation to maintain or provide any Hosted Data.

6. CONFIDENTIAL INFORMATION

6.1. "Confidential Information" means all confidential information of a Party ("Disclosing Party") disclosed to the other Party ("Receiving Party") in writing, designated as confidential or that reasonably should be understood to be confidential given its nature and circumstances. Confidential Information shall not include information:

- that is, or becomes, generally known to the public without breach of any obligation owed to the Disclosing Party;
- known to the Receiving Party prior to its disclosure by the Disclosing Party without breach of any obligation owed to the Disclosing Party;
- developed independently by the Receiving Party without breach of any obligation owed to the Disclosing Party;
- received from a third party without breach of any obligation owed to the Disclosing Party; and
- generated from the Hosted Data.

6.2. The Receiving Party shall not disclose or use Confidential Information of the Disclosing Party for any purpose outside the scope of this Agreement, except with the Disclosing Party's prior permission.

6.3. Each Party agrees to protect the confidentiality of the Confidential Information of the other Party in the same manner that it protects the confidentiality of its own confidential information of like kind (but in no event using less than reasonable care).

6.4. If the Receiving Party is compelled by law to disclose Confidential Information of the Disclosing Party, it shall provide the Disclosing Party with prior notice of such compelled disclosure (to the extent legally permitted) and reasonable assistance, at the Disclosing Party's cost, if the Disclosing Party wishes to contest the disclosure.

7. DATA PROTECTION

7.1. In relation to the processing of any personal data in the profile data of each Account (such as username, password, first name, last name, email address), ClauseBase qualifies as the "data controller" under Data Protection Legislation.

7.2. In relation to the processing of any personal data contained in the Hosted Data, the following shall apply:

- The primary purpose of the Platform is to store abstract templates and clauses, which should not contain any personal data. The Customer accepts to respect this general positioning of the Platform, and shall minimize the amount of personal data that is stored on the Platform.
- In relation to the processing of any personal data contained in the Hosted Data, the Customer shall be the "data controller" and ClauseBase shall be the "data processor". ClauseBase shall only process such personal data: (i) in accordance with the instructions received from the Customer, which may be specific instructions or instructions of a general nature as set forth in this Agreement, (ii) to the extent, and in such manner, as is necessary for the provision of the Services or (iii) as required by law or any regulatory body.
- Each Party shall comply with its respective obligations under the Data Protection Legislation and shall not undertake any action that would cause the other Party to breach any of the Data Protection Legislation obligations. In particular, the Customer shall ensure that: (i) all instructions given by it to ClauseBase in respect of the Hosted Data will comply with applicable Data Protection Legislation and (ii) it has all required consents, licenses and approvals to use, disclose and/or transfer the personal data included in the Hosted Data.

8. RISK ALLOCATION

8.1. The total aggregate contractual and extracontractual liability of ClauseBase under this Agreement shall be limited to the following amounts: (i) *if ClauseBase is liable due to a breach of its obligations under article 6 (Confidential information) or article 7 (Data protection) or due to its breach of 3rd party intellectual property rights:* twenty-five times the monthly Usage Fee set forth in the Commercial Section; or (ii) *in all other situations*: twelve times the monthly Usage Fee set forth in the Commercial Section. To the maximum extent allowed by applicable law, ClauseBase shall not be liable for indirect damage of any kind (such as loss of profits, loss of use, loss of customers, business interruption, third party claims, etc.) incurred by the Customer, Users or third parties connected to the Customer. The Customer shall indemnify ClauseBase for any claim submitted by such third party relating to the Customer's use of the Platform and shall refrain from submitting any contractual or extracontractual claim against the staff, agents or auxiliary persons of ClauseBase.

8.2. Nothing in this Agreement shall exclude or limit either Party's liability for fraud, wilful misconduct or gross negligence. The Customer explicitly accepts that the "Truffle Hunt" module is designed to search through templates and model clauses, must only contain copies of data also stored elsewhere, and must not be used as a document management tool. ClauseBase encourages the customer not to store any personal or confidential data in this module, and shall not be liable for usage of this module outside the usage scenario described in this clause 8.2.

9. MISCELLANEOUS

9.1. Neither Party shall be liable to the other for any delay in, or failure of, the performance of its obligations under this Agreement arising from Force Majeure. If Force Majeure continues for a period of three months, either Party may terminate this Agreement with immediate effect by giving written notice.

9.2. Should any article be found to be invalid or unenforceable, such article shall be deemed severed from this Agreement, and the other articles thereof shall remain in full force and effect.

9.3. In deviation of article 4 of the Commercial Section, this Agreement shall be governed by and construed in accordance with Belgian law, without prejudice to the application of provisions of Lithuanian mandatory law which cannot be derogated from. The Parties will endeavour to resolve any dispute in relation to this Agreement in good faith. If the dispute is not resolved within thirty days through such negotiations, any such dispute shall be finally settled under the Rules of Arbitration of the International Chamber of Commerce (ICC) by one or more arbitrators appointed in accordance with the said Rules. The seat of arbitration shall be Paris, France, and the language of arbitration shall be English. The arbitral award shall be final and binding upon the Parties. The costs of arbitration, including the fees of the arbitrators and the administrative expenses of the ICC, shall be borne equally by the Parties, unless the arbitral tribunal decides otherwise.

SIŪLOMOS PREKIŲ SUTARTIES SĄLYGOS	PROPOSED TERMS FOR THE CONTRACT FOR GOODS
1. Sutarties objektas yra Prekės, nurodytos Sutartyje.	**1.** The object of the Contract is the Goods specified in the Contract.
2. Pagal šią Sutartį Pirkimo objekto apimtys ir reikalavimai jam nurodyti Techninėje specifikacijoje.	**2.** In accordance with this Contract, the scope of and the requirements for the Object of Procurement are specified in the Technical Specification.
3. Siūlomų prekių sutarties sąlygoms prieštaraujant prekių sutarties nuostatoms, taikomos šios siūlomų prekių sutarties sąlygos.	**3.** In the event that the proposed terms of the contract for goods conflict with the provisions of the contract for goods, these terms of the proposed terms for for goods shall apply.
4. Taikoma kainodara **– fiksuotas įkainis.**	**4**. Applied pricing **– fixed rate.**
5. Bendra Prekių kaina sudaro 47.190,00 EUR (keturiasdešimt septynis tūkstančius šimtą devyniasdešimt eurų 00 ct), įskaitant PVM. Bendrą Prekių kainą sudaro: Prekių kaina 39.000,00 EUR (trisdešimt devynis tūkstančius eurų 00 ct) neįskaitant PVM; Pridėtinės vertės mokestis (PVM) 21 % - 8.190,00 EUR (aštuoni tūkstančiai šimtas devyniasdešimt eurų 00 ct). PVM į Lietuvos Respublikos biudžetą sumoka Klientas.	**5.** The Total Price of Goods is EUR 47.190,00 (forty seven thousand one hundred ninety EUR 00 ct), including VAT. The Total Price of the Goods comprises: The price of Goods EUR 39.000,00 (thirty nine thousand EUR 00 ct), excluding VAT; Value-added tax (VAT) 21 % – EUR 8.190,00 EUR (eight thousand one hundred ninety EUR 00 ct). VAT to the budget of the Republic of Lithuania shall be paid by the Buyer.
6. Sutartis įsigalioja: **nuo jos pasirašymo dienos** ir galioja 12 mėnesių.	**6.** The Contract shall enter into force **from the date of its signing**: and shall remain in force for 12 months.
7. Atsižvelgiant į Prekių specifiką nurodomos Pirkėjo teisės ir įsipareigojimai bei Tiekėjo teisės ir pareigos.	**7.** Taking into account the specifics of the Goods, the rights and obligations of the Buyer as well as the rights and obligations of the Supplier shall be indicated.
8. Bet kokie fiziniai ar juridiniai asmenys, kuriuos Tiekėjas pasitelkia tam, kad atitiktų Pirkimo dokumentuose nustatytus reikalavimus ar (ir) pasitelkia Sutarties vykdymui, neatsižvelgiant į tai, kokie teisiniai ryšiai sieja šiuos asmenis su Tiekėju, yra laikomi asmenimis, veikiančiais Tiekėjo vardu. Šių asmenų veiksmai, vykdant Sutartį, Tiekėjui sukelia tokias pačias pasekmes ir atsakomybę pagal Sutartį, kaip jo paties veiksmai.	**8.** Any natural or legal persons that the Supplier engages in order to meet the requirements set out in the Procurement Documents and/or engages for the performance of the Contract, regardless of the legal relations between these persons and the Supplier, shall be considered as persons acting on behalf of the Supplier. The actions of these persons during the performance of the Contract entail the same consequences and liability for the Supplier under the Contract as its own actions.
9. Atsiskaitymo terminas pagal pateiktą sąskaitą-faktūrą per 30 (trisdešimt) kalendorinių dienų nuo sąskaitos gavimo dienos.	**9.** Settlement period shall be according to the provided invoice within 30 (thirty) calendar days from the reception of the bill.
10. Vykdant pirkimo sutartis, 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 tiekėjo pasirinktomis priemonėmis. *Europos elektroninių sąskaitų faktūrų standarto neatitinkančios elektroninės sąskaitos faktūros gali būti teikiamos tik naudojantis informacinės sistemos* **SABIS“ priemonėmis.**	**10.** 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 means of the information system* ***“SABIS”.***

11. Sutarties sąlygų keitimu nėra laikomi techninio pobūdžio sutarties pakeitimai (pavyzdžiui, Šalių klaidos, pavadinimai, sąskaitų numeriai, kontaktiniai duomenys, kiti rekvizitai ir pan.). Apie techninio pobūdžio pakeitimus šalis iš anksto praneša raštu kitai šaliai, atskiras kitos šalies sutikimas neteikiamas. Siekiant išvengti bet kokių abejonių, šalys susitaria, kad šalims įvykdžius šiame punkte nurodytas sąlygas, atskiras susitarimas dėl sutarties pakeitimo nebus sudaromas, o šalies kitai šaliai pateiktas pranešimas dėl techninio pobūdžio pirkimo sutarties pakeitimų pridedamas prie sutarties ir laikomas neatskiriama sutarties dalimi.	**11.** Contract 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 Contract regarding contract amendment shall not be concluded, and the notice one party provided to another party shall be added to the contract and considered an integral part of the contract.
12. Kitos sutarties sąlygos (ne techninio pobūdžio) gali būti keičiamos ar papildomos tik Šalims susitarus, kai keitimas ar papildymas numatytas sutartyje ir/ar galimas vadovaujantis viešuosius pirkimus reglamentuojančiais teisės aktais. Tokio pobūdžio sutarties pakeitimai ir papildymai turi būti sudaromi raštu ir tinkamai pasirašyti abiejų sutarties šalių.	**12.** Other contract conditions (non-technical in nature) can be amended or supplemented only by mutual Contract of the parties, when the amendment or supplementation is provided for in the contract and/or is permissible pursuant to the legal acts regulating public procurement. Contract amendments and supplementations of such nature shall be concluded in writing and properly signed by both parties.
13. Pirkėjas turi teisę nutraukti Sutartį, raštu įspėjęs Tiekėją prieš 60 (šešiasdešimt) kalendorinių dienų iki nutraukimo momento.	**13.** The Buyer shall have the right to terminate the Contract by giving written notice to the Supplier 60 (sixty) days before the moment of termination.
14. Šalys susitaria laikyti šią Sutartį ir visą jos pagrindu viena kitai perduodamą ar kitokiu būdu sužinotą informaciją paslaptyje Sutarties galiojimo metu ir 1 (vienus) metus nuo Sutarties galiojimo pabaigos, neatsižvelgiant į tai, ar ta informacija pateikiama / sužinoma / gaunama žodžiu ar raštu ar kitu būdu. Konfidencialia informacija nelaikoma [Sutarties sudarymo faktas], informacija, kuri privalo būti viešinama pagal teisės aktus, taip pat informacija, kuri yra viešai prieinama tretiesiems asmenims ir (arba) dėl kitų priežasčių yra visiems bendrai žinoma, išskyrus atvejus, kai ji buvo atskleista pažeidžiant šioje Sutartyje nustatytus informaciją gaunančios šalies konfidencialumo įsipareigojimus. Šalis gali atskleisti konfidencialią informaciją be išankstino rašytinio kitos Šalies sutikimo: tiems savo darbuotojams ir (ar) teisėtai pasitelktiems tretiesiems asmenims, kuriems ši informacija yra reikalinga Sutarties įgyvendinimui. Tokiu atveju Šalis užtikrina, kad jos darbuotojai, Sutarties įgyvendinimui pasitelkti tretieji asmenys įsipareigotų laikytis šioje Sutartyje nustatytų konfidencialumo įsipareigojimų; Teisės, finansų ar kitos srities specialistui / patarėjui ar paskolos davėjui, kai tai reikalinga atitinkamų paslaugų teikimui pagal sudarytą sutartį. Tokiu atveju Šalis užtikrina, kad minėti asmenys įsipareigotų laikytis šioje Sutartyje nustatytų konfidencialumo įsipareigojimų; Kai tokia informacija privalo būti atskleista pagal teisės aktus, įskaitant informacijos teikimą teismui ar	**14.** The Parties agree to keep this Contract and all information transmitted to each other or otherwise learned on its basis confidential during the term of the Contract and for 1 (one) year after the termination of the Contract, regardless of whether such information is provided/learned/received orally or in writing or in any other manner. Confidential information shall not be considered [the fact of conclusion of the Contract], information that must be made public in accordance with legal acts, as well as information that is publicly available to third parties and/or is generally known to everyone for other reasons, except in cases where it was disclosed in violation of the confidentiality obligations of the receiving party set out in this Contract. A Party may disclose confidential information without the prior written consent of the other Party: to those of its employees and/or legally engaged third parties who need this information for the implementation of the Contract. In such a case, the Party shall ensure that its employees and third parties engaged for the implementation of the Contract undertake to comply with the confidentiality obligations set out in this Contract; To a legal, financial or other specialist/advisor or lender, when this is necessary for the provision of relevant services under the concluded contract. In such case, the Party ensures that the aforementioned persons undertake to comply with the confidentiality obligations set out in this Contract; When such information must be disclosed in accordance with legal acts, including providing

kitai ginčą nagrinėjančiai institucijai, siekiant apginti savo interesus.	information to a court or other institution considering a dispute, in order to protect its interests.
15. Šalys susitaria, kad jeigu kuri nors sutarties ir/ar jos priedų sąlyga prieštarauja viešuosius pirkimus reglamentuojančių teisės aktų nuostatoms ir/ar Pirkėjo atlikto viešojo pirkimo sąlygoms, pirmenybė teikiama ir šalių santykiams yra taikomos viešuosius pirkimus reglamentuojančių teisės aktų nuostatos ir/ar Pirkėjo atlikto viešojo pirkimo sąlygos.	**15.** The Parties hereby agree that if any clause of the Contract 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 Buyer, the provisions of the legal acts regulating public procurement and/or the terms and conditions of the Public Procurement performed by the Buyer shall prevail and apply to the relations between the Parties.
16. Tiekėjas turi susipažinti ir santykiuose su Pirkėju ir Sutarties vykdymui pasitelkiamomis trečiosiomis šalimis laikytis AB „Ignitis grupė“ valdybos sprendimais patvirtintų Antikorupcinės politikos (toliau - Politika) ir Tiekėjų etikos kodekso (toliau - Kodeksas) nuostatų, įtvirtinančių gerosios verslo praktikos, etikos ir elgesio normas. Susipažinti su Politika bei Kodeksu ir/ar jų pakeitimais galima adresu http://www.ignitisgrupe.lt.	**16.** Supplier shall familiarise with and, in its relations with the Buyer and the Third Parties engaged for the purpose of the implementation 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 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.
17. Tiekėjas privalo 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.	**17.** Supplier must 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;
18. Pirkėjas turi teisę nutraukti Sutartį dėl esminio Sutarties pažeidimo iš Tiekėjo pusės, jei Tiekėjas, įskaitant bet kurį su Tiekėju susijusį asmenį, duoda arba 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.	**18.** 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 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 Buyer 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 compensating all and any losses incurred as a result of termination of the Contract;
19. Tiekėjui yra žinoma, kad AB „Ignitis grupė“ yra išplatinusi finansines priemones, kurios yra įtrauktos į 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.	**19.** The Supplier 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

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.	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.
20. tiek Sutarties sudarymo metu, tiek visą jos galiojimo laikotarpį Tiekėjui (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. 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. Šiame punkte nustatytų reikalavimų pažeidimas ir/ ar nesilaikymas sukelia Sutartyje nurodytas pasekmes.	**20.** 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 Contact. 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.
20.1. Paaiškėjus šiame punkte numatytoms 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	**20.1.** When the circumstances referred to in this paragraph 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

baudų, atlyginti žalą ar išmokėti kokias nors kompensacijas, susijusias su Sutarties nutraukimu ar jos sustabdymu, išskyrus Sutartyje nurodytus atvejus.	compensation related to the termination or suspension of the Contract on the basis specified in this clause of the Contract.
21. Tiekėjas įsipareigoja nenaudoti Pirkėjo ir Ignitis grupės įmonių ženklo (-ų) ir (ar) pavadinimo jokioje reklamoje, leidiniuose ar kitur be išankstinio raštiško Pirkėjo sutikimo.	**21.** the Supplier undertakes 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

TECHNICAL SPECIFICATION

1. CONCEPTS AND ABBREVIATIONS

1.1. **Buyer –** UAB "Ignitis grupės paslaugų centras".

1.2. **Supplier –** an economic entity who is a natural person, private or public legal entity, another organization or division thereof or a group of such persons, with whom the Buyer concludes the Contract.

1.3. **Contract –** the agreement concluded between the Supplier and the Buyer regarding the Procurement object.

1.4. **Technical Specification –** this technical specification.

1.5. **Services –** encompass the ability to use Supplier's Software and other services such as: initial setup and configuration of the Software / user's accounts, initial and other training related with proper usage of the Software, storing data and software, maintaining / updating the Software, troubleshooting, consultancies related with usage of the Software and Services.

1.6. **Software –** a web-based application or add-in / plugin to existing document drafting software (e.g. MS Word) or other computer program provided by the Supplier for legal drafting, reviewing, comparison, analysis, translation, building standardized clause and precedent documents libraries / databases, documents automatization (automated templates, contract proofreading, styling etc.), generative AI assistance.

1.7. **License –** a full Software license for the use on Software, including all available features – themes, authentication, Q&A, documentation and broadcast integration.

1.8. **GDPR –** Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

1.9. **Business Day –** shall mean any day except Saturday, Sunday and any day which is legal / public holiday in the country of the Buyer and / or Supplier.

1.10. **Critical Issue –** a significant problem or failure within the Software that severely impacts its functionality, performance, security or availability leading to complete inability to use Software or its main features according to the scope outlined in the Contract and / or Technical Specification, e.g. inability to log in to the user's accounts, access loss to the Software, data breaches and non-compliance with GDPR, downtime of the Software, doesn't work main functions of the Software, doesn't work control feature of managing user access and permissions to prevent unauthorized actions etc.

1.11. **Major issue –** the Software is operational, but the functionality is very degraded, (the system has a low efficiency, slow response times or frequent system lags, part of the solution does not work or has a significant error).

1.12. **Minor issue –** small issues that do not impact the normal operation of the Software or prevent from normal usage of the Software, but some of the noncritical features do not work completely or properly, not frequent small system lags etc.

1.13. **Temporary Resolution –** a working solution which reduces the impact level on users and allows for impacted functionalities to be fully or partially executed to the extent that provides acceptable results to the user.

1.14. **Final Resolution –** solution of the problem which completely resolves the reported issue.

1.15. **Critical Vulnerabilities –** shall mean vulnerabilities that are assigned 9.0-10.0 points according to the international CVSS classification scale.

1.16. **Important vulnerabilities –** shall mean vulnerabilities that are assigned 7,0-8,9 points according to the international CVSS classification scale.

1.17. **Medium-level vulnerabilities –** shall mean vulnerabilities that are assigned 4,0-6,9 points according to the international CVSS classification scale.

1.18. **Low-level vulnerabilities –** shall mean vulnerabilities that are assigned 0,1-3,9 points according to the international CVSS classification scale.

2. PROCUREMENT OBJECT

2.1. A comprehensive Software solution for legal drafting, reviewing, comparison, analysis, translation, building standardized clause and precedent documents libraries / databases, documents automatization (automated templates, contract proofreading, styling etc.), generative AI assistance.

3. SCOPE OF THE OBJECT OF PROCUREMENT

3.1. The quantities of the Software are presented in Table No. 1:

Table No. 1

Seq. No.	Software	Preliminary quantity
1.	Number of user's accounts or licenses	30 units / month

Services related to the usage of the Software shall be included in the procurement object and shall not be priced separately from the user's accounts or licenses of the Software.

The preliminary number of user's accounts or licenses may increase or decrease from the specified quantity depending on Buyer's needs. (

The Software / Services will be purchased according to the Buyer's needs up to a maximum value of the procurement, i.e. the Buyer shall not be obliged to buy Software / Services for the maximum value of the procurement.

4. PLACE OF DELIVERY OF CONTRACTUAL OBLIGATIONS

4.1. Services and / or other related services shall be provided remotely.

5. DESCRIPTION OF THE CURRENT SITUATION AND THE GOALS OF THE PROCUREMENT

5.1. The Buyer currently relies on standard document drafting software like MS Word for its legal document drafting needs. While MS Word is a versatile tool, it lacks specialized features required for efficient legal drafting, reviewing, analysis, translation, versioning. The process of creating and managing legal documents is time consuming and prone to human error. Additionally, the Buyer does not have a centralized repository for standardized clauses, precedent documents and their management system, leading to inconsistencies and inefficiencies. By implementing comprehensive digital solutions for legal document drafting, the Buyer seeks to:

a) enhance legal drafting and reviewing process ensuring accuracy and compliance with legal standards;
b) enhance document comparison and analysis to identify discrepancies and ensure consistency;
c) handle multilingual legal documents efficiently;
d) build and maintain a centralized database of standardized clauses and precedent documents to streamline the drafting process and ensure uniformity;
e) automate repetitive tasks such as template creation, contract proofreading, and document styling to save time and reduce errors;
f) utilize generative AI to assist in drafting, proofreading, and providing suggestions, enhancing the overall quality and efficiency of legal documents;
g) keep up with new technologies and implement new legal-tech trends into daily legal work process, improve legal staff competencies in digitalization field.

6. REQUIREMENTS FOR PROCUREMENT OBJECT

6.1. **The Software shall meet the following technical conditions and requirements:**

General Functional Requirements

6.1.1. The Software solution must have integrations with Microsoft Word, (preferable desktop version), and all features, functionalities must be available directly within the Microsoft Word environment.

6.1.2. The Software solution must have Artificial Intelligence (AI) integration with Microsoft Word to enhance legal drafting, and have at least following features: automated clause suggestions, first draft suggestions, contextual editing, compare, recognition, provision of streamline of drafting process directly within the Microsoft Word environment.

6.1.3. The Software solution must have functionalities supporting efficient and accurate legal document reviews, including error detection, compliance checks, and document consistency.

6.1.4. The Software solution must have functionalities supporting documents / clause / definition precedents or drafting history within Microsoft Word to quickly identify and retrieve relevant information, clauses or documents, definitions ensuring consistency and efficiency in the legal drafting or review process.

6.1.5. The Software solution must have functionalities supporting comparison of clauses, definitions and documents against precedents, drafting history, or company standard rules and requirements (including a previous version to the current) to ensure consistency, compliance, and alignment with organizational standards.

6.1.6. The Software solution must provide the ability to create a custom library of clauses, definition and documents (custom database) which would be accessible directly within the Microsoft Word environment. There shall be no limitations / restrictions of clause and / or documents and / or other data amounts. There shall be ability to adjust, delete, complement, modify in other than aforementioned ways existing clauses, definitions, documents.

6.1.7. The Software solution shall provide functionality to create, modify, and delete database / library management rules that grant or restrict permissions to access, modify, create, delete data / databases / libraries, also possibility to adjust platform's settings to align with the specific workflows and processes of the Buyer.
6.1.8. The Software solution must allow to add headlines, extra information about the clauses, definitions or documents stored in the library to be recognizable.
6.1.9. The Software solution must have search / filter functionalities to search and filter clauses, definitions or documents within the library.
6.1.10. The Software solution must provide the ability to create specific documents styles, use them as standard which would be automatically followed in case of insertion of new clause, definition from the library or other source.
6.1.11. The Software solution must have ability to detect undefined terms within a document.
6.1.12. The Software solution must allow to create standard templates and automate those templates by filling requested data, questionnaire, conditions, pre/sub-conditions.
6.1.13. The Software solution must have integrated translation features allowing to draft bilingual documents, clauses, definitions. Translations must contain at least Lithuanian, Latvian, Estonian, Polish, Finnish, English languages.
6.1.14. The Software solution must have version history of the clauses, definitions or templates and provide an easy way to see which clauses, definitions or templates were impacted by a modification to a specific clause or definition.
6.1.15. The Software solution must allow to build templates from clauses in the clause library and have ability to automatically update those templates to reflect the latest versions of those clauses.

6.2. **Cyber security requirements.**
6.2.1. Supplier must inform the Buyer about any related parties involved in the Services, if they are already used or will be used. Safety requirements also apply to all related parties (subcontractors) engaged by the Supplier.
6.2.2. Supplier must ensure that only legal software is used providing the Software and / or Services. All system application and infrastructure platforms / libraries must be up to date with the latest security patches. Additionally, it must be ensured that the versions of application and infrastructure platforms / libraries are supported by the manufacturer.
6.2.3. Supplier must make a patch for elimination, or vulnerability mitigation plan of Critical Vulnerability per day after vulnerability was identified.
6.2.4. Supplier must make a patch for elimination, or vulnerability mitigation plan of High Criticality Vulnerability per one week after vulnerability was identified.
6.2.5. Supplier must make a patch for elimination of other Vulnerabilities with a regular system or system components update.
6.2.6. Software and its components software must be updated periodically, versions of the Software and its components shall be reviewed and/or updated at least once a year.
6.2.7. Software must be able to set the Daylight Saving Time and automatically change the applicable time without affecting the operation of the Software.
6.2.8. Software time for all Software level architectural models must be synchronized with the Network Time Protocol.
6.2.9. Unused physical and logical ports (if any) in the system must be disabled.
6.2.10. Supplier must be certified to ISO/IEC 27001:2022 (Information security management systems) or equivalent.
6.2.11. Supplier must have information security policies complied with most common industry standards.
6.2.12. Supplier must regularly carry out business continuity management tests.
6.2.13. Supplier must have an individual, group or product security incident response team that handles product security, vulnerabilities and reported weaknesses.
6.2.14. Supplier must ensure that data storage containing the Buyer's information will not be transferred to third parties.
6.2.15. Supplier's servers (including cloud servers) must be located in data centers within EU countries and data centers must meet at least Tier 3 requirements.
6.2.16. Network segmentation must be done in Supplier's data centers.
6.2.17. Protection against DDoS attacks must be used in Supplier's data centers.
6.2.18. Regular backups of virtual servers, databases including their configuration must be performed.
6.2.19. The data of the Buyer must be isolated from other Software users (third parties). In connection with this requirement, virtual machine and associated custom subdomain shall be dedicated specifically to the Buyer and hosted on a physical machine within EU countries.
6.2.20. Any data from the Software or with the Software shall not be transferred to any third party without the permission / authorization of the Buyer.
6.2.21. Any data of the Buyer must be fully and reliably deleted by the Buyer's request.

6.2.22. All data exchanged between the browser / Software and the server must be encrypted, strongly compressed, and protected against Cross-Site Request Forgery (CSRF) attacks.
6.2.23. In any Software usage scenario if any business data or personal data need to be inserted (to the template etc.) and (or) sent to the server it shall be done by using secure connection and shall be deleted from the server environment after usage of particular feature of the Software e.g. after filled template is generated.
6.2.24. Software 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 Software operation (such as personal information of users).
6.2.25. At client side, all working data shall be exclusively kept within the temporary Software environment.
6.2.26. Supplier must have solutions for log analysis and intrusion, threat & vulnerability detection.
6.2.27. Automated checking of customer applications for application vulnerabilities, particularly before going live shall be implemented.
6.2.28. Supplier must regularly do penetration tests at least once in a year.
6.2.29. Antivirus software must be centrally managed.
6.2.30. The Supplier must ensure the confidentiality obligations of staff and the confidentiality of the data in the Software so that only authenticated users may login to the Software and have access only to the data or functionality intended for them in accordance with their roles and responsibilities.
6.2.31. The Supplier's employees, who have access to the Buyer's information, must sign confidentiality agreements.
6.2.32. The Supplier must apply the principle "Need-to-Know", meaning that the employees of the Supplier should have only the access rights that are necessary to perform their direct functions.
6.2.33. The Software shall prevent saving and recording sensitive and / or confidential information on system users, such as user password, personal code in plain text.
6.2.34. Encrypted communication (TLS/SSL or alternative) between Cloud Service provider and Cloud Service user must be used.
6.2.35. Encrypted communication (TLS/SSL or alternative) between Cloud Service locations must be used.
6.2.36. Encrypted communication (TLS/SSL or alternative) must be used with third party providers where these are required for the provider's own offering.
6.2.37. In case of Buyer's and Supplier's systems integration, data transmitted between integrated systems must be encrypted and encryption should use not less than TLS v1.3 or an IPSec tunnel.
6.2.38. Remote administration must be done via a secure communication channel (e. g. SSH, TLS/SSL, IPSec, VPN).
6.2.39. Digital certificates issued by trusted certification authorities must be used for data encryption.
6.2.40. For encryption of connection with external systems SSL/TLS key length must be 2048 bits or longer.
6.2.41. Software and hardware used for encryption must be able to fail securely.
6.2.42. The encryption algorithm must not have known vulnerabilities during Software deployment.
6.2.43. The perimeter firewalls of the Software network must have IDS/IPS.
6.2.44. The Software shall ensure protection against unauthorized access to the internal computer network within system and its modules.
6.2.45. The Software shall not allow system users, including administrators, to delete or edit action logs.
6.2.46. The following events must be recorded in the Software in an appropriate format:
- Enabling, disabling, or reloading the Software 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).
- Software network flow events (NetFlow, IPFIX, sFlow)
- Security equipment generated security logs.
- Other events specified by the Customer.

6.2.47. Logs must be stored for at least 90 days.
6.2.48. 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.
6.2.49. Log entries must have identifiers which allow to track unique transactions across all the systems (end to end).
6.2.50. Software log records must be stored on separate, specialized, and appropriately designed hardware or software.
6.2.51. Software 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.

6.2.52. Software vulnerabilities are measured using the international CVSS grading scale https://web.nvd.nist.gov/view/vuln/search.
6.2.53. Supplier shall inform the Buyer 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.
6.2.54. Supplier shall provide the Buyer 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 Buyer. The information to the Buyer must be provided no later than 1 month after the incident identification date.
6.2.55. Supplier must regularly notify cloud users about security measures, changes to the IT security management system, security incidents, the results of IS reviews and penetration tests.
6.2.56. Buyer or its authorized service providers shall have the right by the Buyer's expense to audit the Supplier's compliance with these security requirements. Supplier undertakes to facilitate such an audit during the Contract period or in the event of a major incident as follows:
   a) in case of major incident (e.g. a breach, a near-breach of cyber security requirements, serious downtime, loss of data, etc.) – within 5 Business Days from the date of receipt of the prior notification from the Buyer;
   b) In other cases (e.g. yearly audit etc.) – within 30 calendar days from the date of receipt of the prior notification from the Buyer.
6.2.57. Easy review of certain audit records shall be enabled for system administrator. During Software installation, the Supplier shall have to determine and agree with the Buyer which information must be provided.

WEB portal

6.2.58. A new session identifier must be created when a user logs on.
6.2.59. Access to the Software should be able to be limited by IP addresses provided by the Customer.
6.2.60. All data must be stored in session variables instead of client-side cookies.
6.2.61. All input has been validated for expected range, length, format and data type.
6.2.62. All input validation is conducted on a trusted system (i.e. server-side, not client-side).
6.2.63. Client-side caching is disabled on pages containing sensitive information (e.g. using “Cache-Control: no-store” and “Pragma: no-cache” headers).
6.2.64. It is prohibited to store login name, password, keys/tokens, etc. in the source code.
6.2.65. Logout mechanisms are available to users from all screens that are protected by authorization to terminate the associated session or connection.
6.2.66. Obligatory functionality for HTTP session protection:
   - Protect the entire visitor's/user's session with a help of TLS (The version of TLS must be v1.3 or newer);
   - Do not include session ID into URL address and/or do not send it in the Referrer header;
   - Ensure long, complex, generated from random numbers, not easily guessed session ID;
   - Saving of session ID is prohibited;
   - Session ID has to be encrypted by a key of length at least 128 bits;
   - Session ID has to be changed in case of transfer to SSL;
   - The software has to reject ID, which is already used by another user;
   - Session object has to be deleted when user signs out or when the session is terminated.
6.2.67. Passwords on the user’s screen are obscured so that they cannot be viewed by ‘shoulder surfing’.
6.2.68. Persistent authentication sessions or cookies are disallowed, except short-lived cookies if SSO is enabled.
6.2.69. Security-relevant data (e.g. passwords, connection strings) must be stored server-side.
6.2.70. Server-side source code is protected from being downloaded by unauthorized users.
6.2.71. Session identifiers and cookies are never sent to the web server as HTTP GET parameters.
6.2.72. The Software must be protected against automatic brute force attacks. Tests must be recorded.
6.2.73. The Software 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.
6.2.74. Use of cache functionality is prohibited for authenticated pages.

Users authentication, authorization and administration

6.2.75. All accounts of the Software must be uniquely identified and authenticated.

6.2.76. Authentication of Software users must be implemented using Ignitis Group's MS Azure Active Directory (Entra ID).
6.2.77. Software administrator must have possibility to block activities of one or more users by providing notification in user's interface that no activity in the Software can be performed during certain period.
6.2.78. Software authorization mechanism shall be implemented on the basis of Role-based Model and managed centrally for all levels of Software architecture model. User creation, authorization, authentication and rights management shall be centrally managed for all levels of the Software Architecture Model.
6.2.79. Software 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 Software shall not autofill the rest password characters.
6.2.80. Software user must confirm his/her identity by password or using other authentication mean according to Software requirements. Only authenticated users shall see the information provided in the Software and will be able to perform actions.
6.2.81. Software user shall be able to view only such information and use only such functions that are assigned to access rights (e.g.., if Software user wants to view certain information, the Software shall notify that the user has no rights to view certain data or otherwise restrict information display, etc.).
6.2.82. Software's administrator must have possibility to force stop selected logged-in user, i.e. the Software shall have the capability to terminate selected user's work session in the Software.
6.2.83. The Software 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)
6.2.84. The Software must have the capability to manage user access rights by assigning different roles or permission groups, following the principle "need-to-know".
6.2.85. The Software 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.
6.2.86. The Software shall allow Single Sign-On, if user has authenticated him/herself through Ignitis Group's MS Azure Active Directory (Entra ID).
6.2.87. The Software shall allow stopping of role validity and automatic cancelation of associated functions and access for role user.
6.2.88. The Software 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.
6.2.89. The Software shall have automatic Lock or Lock Screen and/or user work session termination function when inactive period exceeds preset duration (15 minutes).
6.2.90. When the user is suspended in the Client's Microsoft Azure Active Directory service, the user has to be suspended in the Software as well.

Security of personal data and GDPR compliance.

6.2.91. The Supplier must ensure that Software and / or Services are provided in compliance with the principles and requirements of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
6.2.92. In providing Software and / or Services, the Supplier shall implement appropriate organizational and technical measures to protect the personal data processed / stored on the Software against accidental or unauthorized unlawful destruction, loss, alteration, disclosure or any other unlawful processing, and shall only use the access granted to the Supplier only for the purposes of providing the Software and / or Services.
6.2.93. The Supplier shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: the pseudonymization and encryption of personal data; the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing system Software and Services, the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident, a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.
6.2.94. The Supplier will be required to execute with the Buyer personal data processing agreement in accordance with the terms of the Article 28 (3) of GDPR. The Supplier will act as a data processor and must fulfil the obligations imposed on the processor by the GDPR.
6.2.95. Any data processed on the Software may not be transferred or / and accessed to any third party without the permission / authorization of the Buyer.
6.2.96. The Supplier must inform in advance the Buyer about any third party involved in provision of Software and / or Services, if they are or will be used.
6.2.97. The Supplier undertakes to inform the Buyer of any confirmed information security breaches immediately but not later than in 48 hours after having become aware of such a breach. The Supplier must have a plan for responding to security incidents, to ensure effective response to incidents, related to the security

of personal data management. All security incidents, including personal data breaches, must be recorded together with all relevant information about the incident and subsequently the mitigation measures taken to address the impact of the incident actions. The Supplier must notify the Buyer without undue delay, but no later than in 24 hours, after becoming aware of a personal data breach. The Supplier must ensure that in the event of a physical or technical incident, it must be possible to restore the processing of personal data.

6.2.98. The physical location of data (at rest and for processing) must be in the Europe Union, UK or countries, meeting the criteria of any transfer of personal data set out in GDPR. The Software should include functionality to delete fully and reliably or depersonalize personal data from the Software at the end of the retention period or at the Buyer's request.

6.2.99. The Software shall have the possibility to delete / depersonalize personal data of an individual person if there is no legal reason to retain them and to exercise the data subject's rights (to rectify, to delete, to access and others).

6.3. **Non-functional Requirements:**

6.3.1. 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 at least 5 days.

6.3.2. The system should be capable of auto-scaling and load balancing to maintain performance standards, even under heavy traffic conditions.

6.3.3. System shall support UTF8 and characters of Lithuanian alphabet. Graphical interface must support Multilanguage including Lithuanian and English.

6.3.4. System integration with other Buyer's systems (if needed) must be based on the following or equivalent standards: SOAP, REST.

6.3.5. The software technical support shall apply to Supplier, OEM and third-party provided software that was included in the contract during the entire contract period.

6.4. **The Services shall meet the following technical conditions and requirements:**

6.4.1. Supplier must deliver the Services in a professional manner and in accordance with most common industry standards.

6.4.2. Supplier must use all reasonable efforts to meet uptime of 99.95% for the Software in a given calendar year and 99.8% in a given calendar month and ensure all Software availability calculations would be recorded.

6.4.3. Supplier shall perform scheduled maintenance as necessary to ensure the Software remains fully functional, compatible with the hosting provider, secure, and performs in accordance with the expected level of service. Supplier shall use its best effort to conduct scheduled maintenance in a manner that causes minimum disruption to the usage of the Software. If maintenance takes place during the Business Day and / or working hours of the Buyer, the Buyer must be informed about any scheduled maintenance of the Software at least 3 (three) Business Days in advance.

6.4.4. Supplier must provide to the Buyer all manuals related with usage of the Software and / or Services in order to enable the Buyer to use all features of the Software.

6.4.5. Initial and other training and consultancies related with usage of the Software and / or Services shall be provided remotely by using Microsoft Teams or another safe communication platform.

6.4.6. Initial and other training and consultancies related with usage of the Software and / or Services and all necessary manuals shall be provided in Lithuanian or English language.

6.4.7. Supplier must have help desk team and dedicated platform / support channel (hereinafter **– Support platform**) to send support request, reports regarding malfunction, errors other discrepancies of the Software and / or Services and receive support.

6.4.8. Registration of issues of the Software and / or Services must be accounted and managed in the Support platform or other equivalent tools offered by the Supplier, which would not require additional funds or efforts from the Buyer to install and / or use the Support platform or another equivalent tool offered by the Supplier.

6.4.9. The Support platform or other equivalent tool offered by Supplier must store data about registered issues of the Software and / or Service, the progress and result of their resolution, and this data must be available to the Buyer whole Contract period.

6.4.10. Guaranteed response and resolution times of support request must be at least as follows:

Incidents, meaning any deviation from the standard operation of the Software which causes an interruption to, or a reduction in quality of the Software. Priority setting of the Incident shall be as follows:

High **–** when incident affects more than 85% of average daily end-users and blocking core usage of the Software and no work around is available.

Medium – when incident affects between 15% and 85% of average daily end-users and blocking core usage of the Software and a work around is available.

Low – when incident affects less than 15% of average daily end-users and none blocking core usage of the Software.

Response Times shall be at least as follows:

CATEGORY	RESPONSE TIME
High	4 Business Hours
Medium	8 Business Hours
Low	15 Business Days

In any case Resolution Times shall be as soon as possible.

7. PROCEDURE AND TERMS OF EXECUTION OF CONTRACTUAL OBLIGATIONS

7.1. Software shall be prepared for use within 15 calendar days after Contract comes into force. In this term shall be included all necessary Services to make the Software ready to use, included, but not limited to: initial setup, configuration, updates of the Software, creation, setup, configuration of user's accounts.

7.2. Initial and / or other necessary training related with proper usage of the Software shall be provided within 30 days after Software preparation for use.

7.3. Software and Services shall be provided in accordance with Lithuanian Law on Public Procurement.

8. PAYMENT CONDITIONS

8.1. The Buyer pays for the Supplier for the ordered Software and / or Services within 30 (thirty) calendar days from the date of receipt of the invoice.

8.2. The Supplier shall submit an invoice for the Software no later than within 10 Business Days after provision of the Software.

8.3. In the course of the Contract, invoices are issued only electronically. Electronic invoices complying with the European standard for electronic invoicing, the reference of which was published on the 16th of October 2017. October 16 Commission Implementing Decision (EU) 2017/1870 on the publication of the reference of the European Electronic Invoicing Standard and the list of syntax in accordance with Directive 2014/55 /EU of the European Parliament and of the Council (OJ 2017 L 266, p. 19) (hereinafter referred to as the European Electronic Invoicing Standard) are provided by the means chosen by the Supplier. Electronic invoices that do not comply with the European standard for electronic invoicing may only be submitted using the SABIS.