GENERAL TERMS AND CONDITIONS FOR PARTNERS OF ZAVAROVALNICA TRIGLAV, d.d.

I. General Terms and Conditions for all partners of Zavarovalnica Triglav, d.d.

1. Introductory provisions

1. The General Terms and Conditions of Zavarovalnica Triglav, d. d., (hereinafter: the General Terms and Conditions) define the terms and conditions of the partnership cooperation of Zavarovalnica Triglav, d. d., (hereinafter: the contracting authority), within the framework of business relations with providers and partners arising in the process of choosing a partner in the procurement of goods and services, either on the basis of a contract or agreement, unless otherwise agreed in writing. The General Terms and Conditions contain:
2. general provisions for the purchase of goods and services applicable to all partners of the contracting authority;
3. specific general conditions for partners providing IT services to the contracting authority; and
4. supplement to the general terms for IT service providers who perform an activity for the contracting authority that is critical or important to the contracting authority's business.
5. The General Terms and Conditions have the character of and are an integral part of a contract; they supplement it and bind the contracting parties in the same way that the contract does. By concluding a contract with the contracting authority, the partner declares that they are familiar with and fully accept the content of the General Terms and Conditions. If the provisions of the General Terms and Conditions and the contract differ, the provisions of the contract shall apply.
6. The General Terms and Conditions shall always apply, unless otherwise agreed in writing with the contracting authority.
7. The Contracting authority reserves the right to determine the derogations that may prevail over these General Terms and Conditions of Purchase, but only if expressly stated in the contract.
8. The General Terms and Conditions are available to partners on the website of Zavarovalnica Triglav, d. d., at the following link: <https://www.triglav.eu>.
9. These General Terms and Conditions shall be applicable regardless of whether the partner has other terms of purchase or supply.

2. Definitions of terms

1. For the purpose of these General Terms, the following definitions shall apply:

* "Contracting authority" means the company of the Triglav Group, which will participate in the individual procurement procedure.
* "Provider" means a natural or legal person who participates in the procurement procedure by submitting bids.
* "Partner" refers to a natural or legal person who was chosen in the procurement procedure and to whom the order is addressed, and can refer to a "supplier", "seller", "provider of goods or services", or "contractor" depending on the procurement phase or procurement object.
* "First Contracting Party" means the company of the Triglav Group, which will enter into a contractual relationship with the second Contracting Party.
* "Second Contracting Party" means a natural or legal person who will enter into a contractual relationship with the company of the Triglav Group.
* "Procurement procedure" refers to purchasing activities such as market research, analysis of received bids, and selection of the most suitable bid.
* "Procurement Commission" is a group of employees appointed by the contracting authority from the procuring business function and the strategic procurement function who are responsible for the conduct of the procurement procedure in accordance with the authorisations.
* "Procurement Portal" refers to the Triglav Group's information support for the implementation of procurement procedures, bid selection processes, and negotiation processes.
* "Reverse online auction" refers to a tool within the procurement portal that the purchasing commission can use to optimise bidder prices.
* "Contracting Party" is a common term for a partner and a contracting authority that enter into a mutual agreement.
* "Order" means a written order (purchase order, e-mail, contract) to a specific partner for the purchase of goods, services, or fixed assets.
* "Material" shall mean a thing or a material asset, such as goods, components, etc., specified in the order or contract submitted by the Contracting authority.
* "Service" shall mean a type of work, such as the manufacture or repair of an asset, physical or mental work, etc., specified in the order or contract submitted by the Contracting authority, and a related service, technology, data, or documentation.
* "IT service" refers to (i) the supply and rental of hardware and software, (ii) hardware and software maintenance, and/or (iii) custom software development, (iv) cloud services, and (v) data forwarding or access.
* "Contract or contractual relationship" refers to a written agreement in the form of a record on a single document between the contracting authority and the partner (s) regarding mutual rights and obligations.
* "Force majeure" refers to circumstances that occur independently of the will of the contracting authority or partner and that could not be anticipated, avoided, or averted (natural disasters, ice, extraordinary atmospheric phenomena, acts of third parties, war, etc.).
* "Triglav Group Companies" are listed at <https://www.triglav.eu/sl/o-nas/skupina-triglav>.

1. Words and expressions in the singular shall include the plural and vice versa. Words and expressions that indicate a whole shall also apply to any part of the whole.

3. General

3.1. Demand and supply

1. The prices stated in the offers are expressed in euros (excluding VAT), unless otherwise stated in the offer documentation.
2. The validity of the tender shall be at least 60 days, unless otherwise agreed in the tender conditions.
3. The costs of preparing and sending the tender documentation (tenders, pro forma invoices, samples, etc.) shall be borne by the provider themselves, unless the payment of the latter is specifically assumed by the Contracting authority in writing.
4. During the procurement procedure, the Contracting authority may change the conditions of demand, of which it shall inform the bidder in writing and request a new offer, adapted to the changed conditions.
5. Unless otherwise specified in the specification according to which the partner is selected, the price in the offer must include all preparatory works, auxiliary works, unforeseen works, costs of small and consumable materials, production costs, packaging costs, shipping costs, customs or entire transport to the client's premises (franco office or customer's warehouse).
6. The contracting authority is not obliged to accept any of the received tenders on the basis of its demand.
7. The contracting authority shall not be obliged to explain to the bidders the reasons for which the procurement procedure has not been completed or for which the bidder’s offer has not been selected or placed in the next round of negotiations.
8. The contracting authority shall in no case reimburse the bidder for the costs incurred in preparing the offer or supplying the samples.
9. In most cases, the Procurement Portal is used to manage the process of inquiry, supply, negotiation, and selection. In this case, the entire communication between the contracting authority and the provider must take place through the Procurement Portal. All communication through other channels can only have an explanatory character and is not part of the procurement procedure documentation.
10. If the price optimisation is done in the purchasing portal using the reverse online auction, the bidder must submit his minimum bid price in the context of the reverse online auction. The reverse online auction is designed to optimise the prices of comparable bids made by suppliers in a short period of time, with first place in the reverse online auction in no way implying acceptance of the bid. It also does not imply that bids that do not finish first in the reverse online auction have not already been accepted.
11. If the contracting authority's representatives coordinate with the bidder on the content of the offer, price, and other conditions, or are already precisely coordinating on the characteristics of the goods or service, the conditions and deadlines for execution or delivery, the preparation of samples, and other activities of harmonisation of the terms of the purchase order or contract, this does not imply acceptance of the offer and the actual order of the goods or service. It makes no difference whether this communication takes place with a single member of the purchasing commission, several members of the purchasing commission, or other employees of the contracting authority.
12. If the Contracting authority invites the bidder to supplement the bid within the bid's validity period or to improve the terms of the bid, this does not imply that the existing bid is rejected.
13. The Contracting authority accepts no obligations towards the selected bidder and is not required to conclude a contract or issue purchase orders with them as a result of the formal selection of the bidder and the notice of selection.
14. The Contracting authority assumes its obligations by issuing a purchase order or a signed contract to the selected bidder.
15. The Contracting authority is not required to return in physical form the submitted written documentation (e.g., submitted bids, correspondence, etc.) to the selected or unselected bidder. The Contracting authority will treat all documentation received from providers as a business secret, regardless of its form.

3.2. Order

1. Only a written order, sent to the provider via e-mail from the online domains of individual Triglav Group companies (for example: triglav.si) or regular mail, is valid, unless otherwise agreed with the partner. This also applies to potential supplements and changes to orders.
2. If the purchase terms (delivery deadlines, price, specifications, etc.) change during the procurement process, the provider must notify and obtain written consent from the contracting authority.
3. It is not possible to unilaterally change the purchase conditions after the procurement procedure has already been carried out.

3.3. Contract

1. Only a contract concluded in writing shall be valid. The same applies to all annexes to the contract.
2. The contract may refer to a written confirmed offer by the contracting authority and/or valid tender documentation within the framework of the procurement procedure, sent by the information support of the contracting authority.
3. The contract shall specify the administrator of the contract on the side of the partner and the Contracting authority (e-mail address, telephone number).
4. All mandatory clauses are defined in these general terms and conditions, so as a rule, it will be specified which will refer to the general terms and conditions regarding the content of mandatory contractual clauses that will be used in an individual umbrella contract/annex in a potential umbrella contract/annex. The anti-corruption clause, which must be recorded in the relevant annex, is an exception to this rule.

3.4. Supply of goods, services, and fixed assets

1. The partner must deliver the goods, services, or fixed assets in accordance with the received order or the concluded contract.
2. The partner will supply quality goods (new, original, unused), services, or fixed assets in a timely manner and in accordance with the legislation and standards of the profession. They must have all the required permits and/or certificates.
3. The supply of goods, services, or fixed assets is accepted when they are inspected and taken over in writing by the representative of the contracting authority.
4. Each delivery of goods, services, and/or fixed assets must be confirmed by the contracting authority's representative by signing the delivery note, specification of work performed, or other appropriate document. Goods, services, and/or fixed assets shall be deemed to have arrived on time if delivered within the agreed deadline to the agreed place provided for in the tender documentation or contract. For services, the service is considered to have been performed timely if the Contracting authority takes it over (signs the handover note) within the deadline provided for in the tender documentation or contract.
5. When the Contracting authority agrees in writing to accept the delivery in parts (successive delivery), the contract or order shall be interpreted as a single contract or order.
6. If the partner does not supply a part of the supply in case of successive delivery, the Contracting authority may withdraw from the contract and pay only the delivered part of the material or service unless the Contracting authority and the partner agree otherwise.
7. If the ordered goods are delivered to the client in larger quantities than ordered, the client is not obliged to accept and pay the excess of the delivered quantity. The surplus of goods shall remain available for collection by the partner for one month after delivery, with all associated risks and costs borne by the partner themselves. After one month, the Contracting authority can dispose of the excess delivered goods, while the costs of the disposal and destruction shall be borne by the partner.
8. The partner is obliged to immediately notify the Contracting authority in writing of any new circumstance that could cause a delay in the agreed delivery period.
9. The Contracting authority does not assume responsibility for the handling of packaging waste. The partner is obliged to take back free of charge all packaging waste related to the delivered goods (e.g., transport and sales packaging), unless otherwise agreed with the Contracting authority. The Contracting authority will return to the partner all empty returnable packaging, if so, agreed in writing in the order or contract.
10. The contracting authority is not required to accept or pay for goods, services, or fixed assets of unsatisfactory quality, and this also applies to possible undelivered partial deliveries. The partner is obliged to comply with the regulations governing the management of packaging waste.
11. In the event of unusual circumstances, such as a declared epidemic affecting the supply of goods, services, or fixed assets, the partner must notify the contracting authority in writing.

3.5. Payments and payment terms

1. The invoice for the delivered goods, services, and/or fixed assets must be sent by regular mail or via the e-invoice system, along with the signed delivery note or other documents specified in the contract. If the delivery note is sent by ordinary mail, it is sent to the address of the contracting authority. The order or contract specifies the method and address for sending the invoice.
2. Payment shall be made in accordance with the contract or purchase order terms and upon receipt of the following documentation: invoice, confirmed delivery note, delivered goods/fixed assets, a confirmed handover record, or other document, as defined in the contract in the case of services provided.
3. The payment deadline is 30 days from the date of receipt of the invoice by the client, unless otherwise stated on the order or in the contract.
4. The payment deadline shall begin to run on the next working day after the date of receipt of a correctly issued invoice.
5. The Contracting authority is not obliged to pay the invoice if the goods, services and/or fixed assets have not been ordered in writing or contractually agreed and demonstrably confirmed by the representatives of the Contracting authority. Exceptions to this provision are the services for which the payment is defined in laws, decrees, or regulations.

**3.6.** **Complaints**

1. If the goods and/or the fixed asset are not delivered in accordance with (quality, technical characteristics ...) with a confirmed bid or specification or with a contract, the contracting authority may:

* at the expense and risk of the partner, refuse or return the inadequate goods or fixed assets to the partner,
* after a special agreement with the partner, accepts inferior goods or fixed assets when the purchase price is reduced or agrees to eliminate the defect in goods or fixed assets.

1. If the service is not performed in accordance with (quality, other characteristics) with a confirmed bid or specification, or with a contract, the contracting authority:

* require the partner to immediately eliminate the error and perform the services in accordance with the offer, specification, or contract,
* at the expense and risk of the partner, perform the service (repair or correction of the error) with another partner.

1. The consequences of disruptions in the work process of the contracting authority due to late delivery of goods or fixed assets, poor quality of goods or fixed assets, or inadequate services by the partner are fully taken over by the partner. Liability for damage shall be calculated on a case-by-case basis, unless otherwise stipulated in the contract or order.
2. Quantitative complaints and visible errors in goods or fixed assets shall be communicated in writing by the contracting authority to the partner immediately upon receipt of the goods. Hidden defects shall be notified by the Contracting authority to the partner in writing as soon as identified, but no later than within six (6) months after acceptance. The defect notification must contain a detailed description of the defect and a call to the partner to rectify the defect.
3. The partner is obliged to provide the Contracting authority with a written substantive reply to the complaint or notification of the defect within 24 hours following the receipt of the complaint or notification of the defect.
4. The partner is obliged to achieve the contractually agreed quality and eliminate the defects within a subsequent period set by the Contracting authority. If the partner fails to achieve this or is unable to achieve the contractually agreed quality even within the subsequent period, they shall be obliged to provide replacement goods, fixed assets and/or services at their own expense.
5. If the delivery conditions are not met, the Contracting authority may charge the partner the costs incurred as a result of the damage and obtain a replacement delivery from another partner (buy-in).
6. In case of delay in the delivery or the performance of the service, the partner must immediately notify the Contracting authority in writing when any changes occur. If the Contracting authority is not informed in advance and has not confirmed the changes in writing, they are not obliged to accept or pay for such goods and/or services.

3.7. Reporting on risks to successful performance of a supply or service

1. The partner undertakes to disclose to the Contracting Authority all new or changed circumstances and facts that could affect their ability to legally, successfully, and timely perform the contract. This includes, but is not limited to, informing the Contracting authority of the following events and facts:

* The perceived significant (operational) risks related to the performance of the contract;
* any activities of the partner or the intention of the partner to restructure the status or ownership;
* the initiation of insolvency proceedings against the partner or the liquidation of the partner;
* any judicial, administrative, or other formal proceedings initiated against the partner and any civil actions, findings of auditors, decisions of supervisory authorities and the like, which directly or indirectly relate to the subject of this contract and/or could materially affect the partner's ability to fulfil their contractual obligations;
* the conclusion of other agreements that require a significant part of the personnel, professional, time or other availability of the partner and could adversely affect the performance of services under the contract.

1. The Contracting authority reserves the right to issue general guidelines and individual instructions to the partner regarding the performance of the contract.

**3.8**. **Sustainable operations and preliminary assessment of supplier suitability**

The bidder or partner is required to complete, at the request of the contracting authority, a questionnaire sent once a year regarding the sustainability of operations (hereinafter: the TRP form) and the contracting authority's questionnaire regarding the preliminary assessment of the supplier's suitability (hereinafter: the Pud form), and to meet the conditions from the forms throughout the business relationship.

If the provider or partner does not meet at least the first six points of the TRP questionnaire, which is an annex to these General Terms and Conditions (fulfilling obligations to workers, ensuring a healthy and safe working environment, preventing discrimination and all forms of harassment and compliance with legislation including environmental requirements), and if it does not meet the conditions from the TRP form, which is an annex to these General Terms and Conditions, the contracting authority has the right to withdraw from the procurement procedure by a unilateral statement and without notice if the contract has already been concluded. The provider or partner is then obliged to reimburse the contracting authority for any costs and damages incurred.

The obligation of the provider or partner is:

* complete the TRP form and the PUD form before registering on the Portal;
* fill in the TRP form and the PUD form once a year, upon the invitation of the contracting authority;
* throughout the contractual relationship, report any changes that would affect the non-compliance with the conditions set out in both forms.

4. Contractual clauses

4.1. Anti-corruption clause

1. By confirming these conditions, the Contracting Parties declare that at any stage of the contract's conclusion or performance, neither of them has offered, given, or promised any undue benefit to any employee or member of the other party’s management or supervisory bodies, or any representative or intermediary of a public sector body or organisation for:

* for the acquisition of a transaction, or
* the conclusion of a business contract under more favourable terms, or
* failure to exercise due control over the performance of the contract; or
* other conduct or omission that has caused or could cause damage to the other party or an authority or public sector organization or enable an unauthorized benefit to any employee and member of the management or supervisory body of the other party or representative or intermediary of an authority or a public sector organization.

1. In the event of a breach or attempted breach of this clause, the contract already concluded shall be null and void. In the event that the contract has not yet come into force, it shall be deemed that it has not been concluded.
2. The Contracting Parties undertake to establish, in proportion to the size of their organization, their own exposure to the risk of corrupt practices, the nature of their business and the anti-corruption legislation binding to each Contracting Party, to take appropriate measures to prevent corrupt practices, ensure their detection and appropriate treatment, and the reporting of detected violations to the competent official authorities.
3. In the event of suspicion of corrupt practices or breach of obligations under the previous Paragraph by one of the Contracting Parties (hereinafter referred to as: "the infringing contracting party"), the other contracting party (hereinafter referred to as: "the contracting party loyal to the contract") is entitled to take appropriate measures to manage its own risk exposure to commercial damage and damage to its own reputation, including but not limited to:

* limitation or revocation of contractual powers to act in the name and on behalf of the party loyal to the contract,
* conducting an audit of the implementation of the provisions of the agreement with the infringing Party,
* a requirement for the infringing Party to provide additional insurance in the event of commercial damage or damage to the reputation of the Party loyal to the contract.

1. In the event that proceedings are instituted against the infringing Party in front of official authorities for acts of corruption relating to the content of business cooperation under this contract, the Party loyal to the contract may suspend the performance of its obligations under the contract until a final decision is taken in this procedure, without any liability for damage resulting from the infringing Party.

4.2. Conflict of interest management

1. The contracting parties declare that there are no given circumstances in connection with the conclusion of this contract that represent or could represent a conflict of interest. Each Contracting Party shall immediately notify the other Contracting Party of any existing or potential conflict of interest detected, as well as the perceived appearance of a conflict of interest during the performance of this contract.
2. The Contracting Parties agree to take all necessary steps to manage the risks that may arise from a conflict of interest, including, but not limited to:

* the exclusion of persons subject to a conflict of interest from any further proceedings relating to the performance of the subject-matter of the contract or other measures which reasonably prevent such persons from interfering with the performance of the contract;
* carrying out control procedures over acts already performed by persons with a conflict of interest;
* hiring another person who will regularly check and approve all actions performed by the person with whom a conflict of interest is expressed in relation to the performance of the contract.

1. Each contracting party is responsible for the implementation of measures in relation to persons acting on its behalf and/or on its account. The measures taken shall be notified to the other party. Where the contracting party cannot implement the necessary measures without the participation of the other contracting party, the contracting parties shall separately agree on the implementation of the measures.
2. Each contracting party's conflict of interest represents any private interest of the managers or employees involved in the conclusion or implementation of this contract, or the private interest of the employees' immediate family members, which could adversely affect the careful, economical, fair, and efficient implementation of this contract. The contracting parties undertake to protect as confidential all data and information obtained in connection with the announcement of conflicts of interest within the framework of the applicable legislation, and to process any personal data in accordance with the applicable regulations governing the protection of personal data.

4.3. Protection of business secrets

The contracting parties undertake to protect the content of this contract and all documentation (business, financial, technical) related to the provision of services under this contract as a business secret and will not forward, disclose, or otherwise make it available to third parties without the prior written consent of the other party. The contracting parties also undertake to protect all business secrets, personal data, and other confidential information of the other party, that they become acquainted with due to or in connection with the implementation of this contract, regardless of the medium in which the information is contained or the manner in which the confidential information was obtained.

Each contracting party agrees to provide confidential information only to those who require it for the performance of this contract in the name and on behalf of each contracting party, to the extent strictly necessary for this purpose. Each contracting party shall be liable as its own breach for breaches of the protection of business secrets and confidential information committed by persons acting on its behalf and for its account. If the disclosure of information is requested by a competent court, supervisory authority, or a third party to whom an individual contracting party is required by law to disclose this information at its request, the parties are relieved of these responsibilities.

Business secrets or confidential information do not represent the following information:

* information already in the possession of the contracting party before it received it from the other contracting party;
* information that has been or becomes public for reasons other than breach this contract;
* information derived from or related to this contract that, according to applicable legislation, is considered to be public information of at least one of the contracting parties and which that contracting party is required to publicly disclose.

The obligation to protect confidential information referred to in this Article shall remain in force even after the termination of this contract.

The contractor agrees to notify in writing all employees, contractors, and external colleagues who will become acquainted with the data as a result of the contract's implementation of the obligation to protect data.

4.4. ZDIJZ clause

1. The partner is aware that the contracting authority is obliged to disclose information of a public nature in accordance with the Public Information Access Act (hereinafter: ZDIJZ).
2. Notwithstanding the provisions of the contract regarding the protection of business secrets, the contracting authority is entitled to publicly disclose the information specified by the ZDIJZ as information of public character of the contracting authority, either by their public publication on the contracting authority's website or by disclosing it to the eligible applicants.

4.5. Protection of human rights

1. The contracting parties agree to respect, for the duration of the contractual relationship, the human rights and fundamental freedoms to which they and their subcontractors are subject at the time of the conclusion of this contract, with a minimum scope of human rights and fundamental freedoms to be respected in accordance with the objectives and principles of the United Nations, as enshrined in the Universal Declaration of Human Rights and the Convention on the Rights of the Child, adopted and proclaimed by the General Assembly of the United Nations, and in the Declaration of the International Labour Organization on Fundamental Principles and Rights at Work. The contracting parties also undertake to implement the requirements of environmental legislation in all the countries in which they operate.
2. If it is established by a final decision of a court or other body that a partner has violated the obligations referred to in the previous paragraph, the contracting authority may unilaterally withdraw from the concluded contract due to a serious breach of contractual obligations, without liability for damage caused to the contracting authority. The partner is obliged to reimburse the client for all damage and costs incurred as a result of the partner's breach of obligations.

4.6. Force Majeure

1. The partner is not liable for partial or complete failure to perform contractual obligations if the failure is the result of force majeure. If the fulfilment of the partner's contractual obligations is partially or completely disrupted or prevented due to force majeure, the partner is obliged to inform the contracting authority immediately, but no later than within three (3) working days. If the partner fails to do so, the contracting authority may withdraw from the contract on grounds of a serious breach.
2. The partner is obliged to immediately inform the contracting authority about the termination of circumstances that represent force majeure.
3. The burden of proof of the existence of force majeure shall be borne by the partner.

4.7. Protection of personal data

The contracting parties undertake to act in accordance with the applicable Personal Data Protection Act of the Republic of Slovenia and the General Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter: the General Data Protection Regulation).

If the contracting parties, in the performance of their obligations under the contract, exchange personal data of individuals, process them for the other party’s account, or dispose of them in a relationship of joint management of personal data sets, the contracting parties agree to adopt a special agreement on the processing or joint management of personal data, in which they will regulate in detail the mutual relationship and obligations in relation to personal data, before the commencement of the processing of personal data.

In accordance with the applicable regulations of the Republic of Slovenia, the other party shall be liable for damages to the first party for any unauthorised disclosure of personal data or confidential information obtained on the basis of a contractual relationship or for the fulfilment of an agreed-upon business purpose.

4.8. Fraud prevention

The contracting parties actively implement a zero-tolerance policy against fraud. The other party shall refrain from any conduct that may constitute fraud in the performance of this contract.

The other party shall actively cooperate with the first party in the prevention, detection, and investigation of fraud. The other party shall ensure that its employees and subcontractors are aware of the zero-tolerance fraud policy and other guarantees of the other contracting party referenced in this article.

All suspicions of fraud that the other contracting party discovers in the performance of this contract must be reported to the first contracting party, as a rule, through the line for reporting suspicions of fraud, available on the website of the first contracting party (www.triglav.eu), but if this is not possible, suspicions of fraud must be reported via e-mail to sporp@triglav.si or by mail to Zavarovalnica Triglav, d. d., delivered to: SPORP – do not open!, Miklošičeva 19, 1000 Ljubljana.

If the first contracting party suspects fraud in relation to this contract, it may, at its sole discretion, limit the scope of the second contracting party's powers, suspend the performance of this contract in whole or in part, and prohibit the performance of transactions under this contract, depending on the nature of the suspected fraud.

4.9. Restrictive measures

1. Notwithstanding any other provision of the contract, the parties shall not be obliged to fulfil their obligations to the contracting authority arising from the contract and related contracts and agreements if performance would constitute a breach of any trade or economic restrictive measures or sanctions, prohibitions, or restrictions adopted by international organizations, authorities of individual countries, in particular, but not exclusively, the authorities of the Republic of Slovenia, the European Union, the United Kingdom, or the United States of America.
2. A contracting party who fails to fulfil their obligations under the contract due to compliance with the restrictive sanctions and restrictions referred to in the preceding paragraph shall not be liable for damage caused to the other party or third parties due to the failure to fulfil their contractual obligations.
3. Each contracting party shall immediately notify the other party if any restrictive sanctions, prohibitions, or operating restrictions referred to in the first paragraph of this Article have been imposed on them, their parent or subsidiary companies, their business partners or its ultimate owners.
4. Either party may withdraw from the contract without liability for any potential damage caused to the other party and without notice if sanctions or similar restrictions are taken against the other party that prevent further performance of the contract.

5. Third Party Rights and Intellectual Property Rights

1. The partner is responsible for ensuring that the services it is obligated to provide, and their outcomes do not infringe upon the rights of third parties or intellectual property rights. If the contractual service violates the rights of a third party, the partner will defend the contracting authority against all claims based on competing rights to the contractual service, unless the partner is responsible for the violation.

**6.** **Validity of the offer within the companies in the Triglav Group**

1. The partner agrees to offer the goods and services to other subsidiaries of the Triglav Group under the same terms and conditions, if they express an interest.

7. Contract termination

1. The termination and notice period are outlined in the contract between the partner and the client; otherwise, the rules outlined in this point apply.
2. The contractual relationship must be terminated in writing and sent to the other party via registered mail. The notice period commences on the fifteenth (15th) business day following the date on which the written cancellation is sent by registered mail to the known address of the other contracting party.
3. The contracting parties undertake to implement all the provisions of the concluded contract within the notice period.
4. A contractual party loyal to the contract may terminate the contract without notice if the other contractual party fails to fulfil any of its essential obligations under the contract and fails to remedy this breach within thirty (30) days of receiving a written request to remedy this violation from the other contractual party.
5. Pursuant to the provisions of the preceding paragraph, the contracting party may withdraw from the contract even if the other contracting party becomes insolvent or ceases operations, and in the case of IT services, also in the circumstances described in point 4 of Chapter II of the Special General Terms and Conditions for Partners or IT Service Providers.

8. Final provisions

1. The stated General Terms and Conditions of Purchase apply regardless of whether the bidder sends their general terms and conditions of business when submitting the bid.
2. The partner and the contracting party shall resolve any possible disputes amicably and by peaceful means. Unless otherwise stipulated by the contract, the court in Ljubljana shall have jurisdiction to resolve the dispute. Slovenian law shall apply.
3. The contracting authority has the right to change or supplement these General Terms and Conditions at any time. Any changes to the Terms and Conditions will be published on the website of Zavarovalnica Triglav, d. d. The contracting authority will notify the partner by e-mail or regular mail before the expected application of the amended General Terms and Conditions. As soon as the partner is made aware of the modifications, they become enforceable. Nonetheless, the partner shall be deemed to be aware of the changes upon their publication on the website of Zavarovalnica Triglav, d.d. and upon receipt of the change notification. If the partner does not agree with the changes, they must notify the contracting authority in writing within eight days of receiving the notice. In the event of disagreement, the contracting authority has the right to withdraw from the contract, unless the parties agree otherwise.
4. The contracting authority is informed and agrees that the data will be processed in the information system of the contracting authority in accordance with the Rules on the retention of business documentation.

II. Special general conditions for partners or IT service providers

II.I. General provisions for partners or IT service providers

1. General provisions

1. Particular general terms and conditions for partners or IT service providers in addition to the above general terms and conditions apply in cases where the subject of the IT service contract is: (i) the supply and rental of hardware and/or software, (ii) the maintenance of hardware and/or software and/or (iii) the development of custom software and in respect of which additional terms and conditions are set out below, (iv) cloud services or (v) the transmission or access to data.
2. The partner must inform the contracting authority whether it relies substantially on cloud infrastructure for the provision of its services (for example, if part of a subcontracting chain is a cloud service provider). If the partner relies significantly on cloud infrastructure for the provision of its services, the contracting authority treats it in the same way as cloud service providers.
3. The partner is obligated to provide the services referred to in the first paragraph of this Article with the characteristics described in the contract, including the reference documents, and not subject to errors that nullify or reduce the value or suitability for normal use or use specified in the contract. The provision of contractual services shall be based on the current technological state of the art, with due regard for the degree of diligence customary in the industry, and with the diligence of a competent professional. Applicable legal regulations must be complied with insofar as they determine the requirements relating to the provision of services. The software must be provided in accordance with the relevant quality and security standards.
4. The partner is required to meet the relevant information security standards and to keep up with technological advancements in this field. In providing its services, the partner is obliged to take into account all information and security policies of the contracting authority through the communication channels agreed upon in the contract.
5. The contracting authority will also involve partners in its security awareness programmes in the field of information and communication technologies and training in the field of digital operational resilience, where appropriate. The partner undertakes to participate in such awareness-raising and training programmes. The terms and conditions of the said cooperation shall be determined by a special agreement between the contracting authority and the partner.
6. The partner agrees to cooperate with the contracting authority's supervisory authority, if necessary, or to provide the contracting authority with the necessary assistance in responding to potential supervisory authority requests relating to the services provided by the partner to the contracting authority.
7. If the parties agree that the partner will provide the source code for the software, it must be supplied along with all documentation and development tools, including updates, upgrades, or other new versions of the software supplied as part of the maintenance services. In addition, the contracting authority may request the deposit of the source code under reasonable conditions if there is a justified reason for doing so (e.g., the software is important for the contracting authority's essential business processes).
8. The partner is obliged to meet the relevant technical standards and related innovations in the field of equipment, services, or solutions supplied to the contracting authority. In the event of a technical backlog of individual building blocks, the partner undertakes to fully provide a free upgrade to the current industry standard.
9. The partner's deliveries and services, whether on data carriers or electronically transmitted, must be thoroughly reviewed and tested using checks and analysis of procedures to ensure that they have the required characteristics, are of appropriate quality, and are free of malware (e.g., trojans, viruses, spyware) and security vulnerabilities. If malware or security vulnerabilities are discovered, the contracting authority must be immediately notified, and a solution that does not contain malware or security vulnerabilities must be agreed upon or created in collaboration with the contracting authority.
10. If the partner has any doubts about the information, policies, instructions, or documents provided by the contracting authority, he must notify the contracting authority in writing as soon as possible. If changes or improvements to services are required during the provision of services, the partner must notify the contracting authority in writing as soon as possible and obtain the contracting authority's approval before making any changes.
11. The partner only hires personnel who are technically and personally qualified to perform the services and tasks specified in the order.
12. All resources provided by the contracting authority, such as documents, data, information, data carriers, access to systems, hardware, or other facilities, are used solely for the execution of the order or contract. Access rights, particularly to information and other systems provided by the contracting authority, as well as the ability to use infrastructure, computers, or licences, shall expire upon completion or termination of the contract. The partner is obliged to return to the contracting authority all the items and data received from the contracting authority in connection with the contract. Electronic documents, information or means of access shall be destroyed, deleted, or transcribed in such a way that they can no longer be recovered. These provisions do not affect the rights and obligations of the contracting parties arising from the contract until the date of termination of the contract. Regardless of the foregoing, the contracting parties agree that the provisions of the contract governing: intellectual property rights; consequences of contract termination or termination of the contract; obligation to protect confidentiality and business secrets; guarantees and liability; liability for damage and data protection will apply even after the date of contract termination or fulfilment.
13. The contracting authority reserves the right, in exceptional circumstances or if the partner is late in performing his contractual obligations, to release to a third party the performance of obligations that the partner did not perform within the contractual deadline. This can be done despite the provisions of the contract, which in any way (directly or indirectly) prohibit or restrict the performance of these obligations by the partner to unauthorised persons. The contracting authority must notify the partner in writing of the transfer of implementation at least 24 hours before the third party begins to perform these obligations.
14. Upon termination of the contract, in the event of insolvency, resolution, or termination of the partner's business, the partner shall, without delay or at the latest within 5 working days from the written request of the contracting authority, the cancellation, the date of termination of the contract, if the contract's validity is not extended, or from the decision of the court initiating insolvency proceedings against the partner, or other means of termination:

* provide the contracting authority or a third party designated by the contracting authority with free access to, renewal of, and restoration of all data (personal and non-personal) in an easily accessible form, or for a fee if the costs are defined by contract;
* return all data of the contracting authority, including all copies of the contracting authority's software, software code, documentation, and any other software that is subject to the performance of services in accordance with the contract;
* return to the contracting authority free of charge all materials created by the supplier in accordance with the contract, if they are owned by the contracting authority;
* stop using the contracting authority's data and provide a complete and uninterrupted version in electronic format in formats and media agreed upon with the contracting authority, allowing the contracting authority's data to be portable;
* unless required by law, destroy all copies of the contracting authority's data and/or software provided or licenced free of charge, and provide proof and written confirmation to the contracting authority that the data are securely destroyed by him, and all subcontractors specified in the contract;
* return all possible payments for services that have not been delivered to the contracting authority in accordance with the contract.

1. All permits, leases, and permits issued by the contracting authority to the partner will expire at the end of the contract's validity period, during which the contracting authority is not required to explicitly notify the partner in writing.

2. Information security

1. The partner is required to meet the relevant information security standards and to keep up with technological advancements in this field.
2. The partner shall have appropriate technical and organisational measures in place to prevent disruptions to the availability, integrity, authenticity, and confidentiality of its information, technological systems, components, and processes, as well as all information and data of the contracting authority, and shall implement appropriate industry standards, procedures, and methods to prevent, identify, evaluate, and eliminate all vulnerabilities, malicious code, and other disruptions.
3. The partner must test and assess the safety of the services it provides prior to delivery to the contracting authority and, if the contractual obligation is continued, on a regular basis during the period of performance of the contractual services for the contracting authority. The partner shall document the results in accordance with industry standard practice and provide them to the contracting authority upon request. The contracting authority is entitled but not obliged, at any time, to comprehensively test and review the contractual services regarding vulnerabilities, malicious code, and other defects. The contracting authority has the right to carry out those tests and the necessary testing with the help of third parties bound by confidentiality. The partner shall provide reasonable assistance to the contracting authority.
4. For the performance of tasks under the contract and these general terms and conditions, the partner will use internationally established equipment of recognised contractors and services of established and verified suppliers (quality of services, security of services, technological competence, financial soundness, etc.).
5. For the performance of key tasks under the contract or tasks that can significantly affect the performance of tasks under the contract or the protection of personal data, the partner may use subcontractors only with the explicit written consent of the contracting authority, unless otherwise specified in the contract or general conditions of use of services.
6. The partner is obliged to provide and maintain data model documentation, where applicable, for all data processed by the partner for the contracting authority.
7. All maintenance work must be carried out at the place where the equipment is located. If this is not possible, the data carriers from the equipment must be removed and stored safely. If the data cannot be removed or otherwise protected, the maintenance process must be supervised.
8. The partner is required to notify the contracting authority of the locations, namely the regions and countries where the contractual functions are performed and the service is provided in relation to the contracting authority, as well as the location of the retention (including data centres in the management of the partner's subcontractors). The partner is required to notify the contracting authority of any planned change of the aforementioned locations and may not change it without the prior written consent of the contracting authority regarding the change of location, unless the contract provides for a different manner of acquaintance with the aforementioned locations and the right of the contracting authority to submit objections to the proposed changes.
9. The partner is obliged to oblige its subcontractors and suppliers to fulfil the obligations from Chapter II of these General Terms and Conditions.
10. Changes to information solutions or documentation during the term of the contract between the parties may result from:

* the reasons for improving or introducing new solutions that are the subject of the contract;
* elimination of errors in the information solutions that are the subject of the contract;
* organisational changes that affect the solutions that are the subject of the contract or legal changes that affect the solutions that are the subject of the contract.

1. All requests for changes are kept exclusively in the change management system specified by the contracting authority and the partner in the contract. A traceable link must be provided between the change request and the individual change in the information solution or documentation.
2. The development, testing, and production environments of the information solutions that are the subject of the contract are always completely separate.
3. Any changes to the information solutions or documentation that are the subject of the contract are first tested exclusively in the development environment and exclusively with imaginary data or publicly available digital content. Every change must be properly documented by marking a new version, identifying the causes of the change and material additions in a descriptive manner, and determining the retention location of the new and previous versions.
4. All versions of the IT solution and documentation are always stored securely.
5. Real data must never leave the production environment and must never be transferred to another environment or transmitted to other people unless there is an explicit legal basis for doing so or without the express consent of all contractual partners and the final party to whom the data pertains, and only after a prior assessment of whether such conduct complies with all applicable regulations.
6. Before each installation of a new version of the IT solution:

* provide for the manner and possible problems of installation and operation in the system,
* successfully test the new version in the test environment, which is properly documented, in accordance with the changes, supplement or otherwise correct the project documentation or the documentation of the information solution.

1. New versions of the information solutions subject to the contract between the contracting parties may not be installed until all of the tasks referred to in the preceding paragraph have been successfully and correctly completed. The modified IT solution, which is the subject of the contract, is installed after the contractual partners agree on it and the contracting authority confirms in writing the appropriateness of the change.
2. Both parties are obliged to provide the necessary cooperative activities so that the employees or users can be properly and effectively acquainted with new information solutions or changes to them.
3. The partner may change the information solutions and/or agreed service levels exclusively in agreement with the contracting authority. Notwithstanding the above, the partner may improve and update the services in cases of:

* the implementation of necessary corrections, the omission of which would constitute a disruption to the operation of the services;
* eliminating system security vulnerabilities
* and/or to ensure compliance with regulations or decisions of supervisory authorities.

1. The contracting authority may propose changes to the services agreed upon in the contract. The obligation of the partner is to respond to the proposal of the contracting authority within 14 days at the latest and to define the conditions under which the proposal would be feasible, including any financial consequences for the contracting authority.
2. When providing services, the partner considers standards and good practises in the field of information security (e.g. ISO 27001), in connection with the development of online technologies, takes into account OWASP-standards, as well as other standards or guidelines for the proper functioning of information and communication technologies and modern technologies (e.g. regarding algorithms, the Internet, information security, trust services, artificial intelligence, etc.) issued by the European Information Security Agency (ENISA) or national or European supervisory authorities, and other provisions of these special conditions.

3. Personnel safety

1. The partner ensures that only its reliable employees are involved in the processing of personal data, which:

* have been duly checked in the recruitment procedures and the fulfilment of the conditions has continued to be checked on an ongoing basis;
* contractually or by special declaration are obliged to protect sensitive data;
* are professionally qualified for their work and their knowledge and skills are constantly maintained.

1. The partner will only give employees access to personal data or confidential information that is strictly necessary for their work in connection with the tasks outlined in the contract with the contracting authority. It will also ensure that all sensitive tasks are properly regulated and implemented separately (segregation of duties), that critical tasks require the participation of at least two authorised and qualified employees (four-eyes principle), and that no employee can independently jeopardise the security and integrity of personal data or confidential information.
2. If not expressly agreed otherwise in a special contract, the partner may also provide confidential information, but not necessarily personal data, to its professional advisors, agents, and advisors, on the condition that they sign a confidentiality statement under the same conditions as this contract.
3. If the service requires the partner's employees to have access to the systems where the contracting authority's data is processed, the partner is required to provide the contracting authority with a list of authorised persons working on the performance of works under the contract, as well as their role, and the contracting authority must be kept informed of any changes in authorised persons. The contracting authority has the right to check the compliance of the list of employees in these works with the actual situation.
4. At the request of the contracting authority, the partner is obliged to replace the authorised person referred to in the fourth paragraph of this point if the latter proves that he acted or tried to act in contravention of the provisions of these conditions.
5. The provisions of the preceding paragraphs shall apply mutatis mutandis to the partner's external associates or employees of subcontractors, provided that the partner uses them for the provision of services and the cooperation with them is approved in advance by the contracting authority.

4. Termination of the contract with partners or IT service providers

1. The contracting authority may terminate the contract with the partner or the IT service provider in the event of the following circumstances:

* a material breach by the partner of applicable laws, regulations, or contractual terms;
* circumstances discovered during the partner's risk monitoring that are deemed capable of altering the performance of the functions performed under the contractual arrangement, including significant changes affecting the contract or the partner's position;
* the partner's demonstrated weaknesses in terms of overall risk management in the field of information and communication technologies, particularly in terms of ensuring the availability, authenticity, integrity, and confidentiality of data, whether personal or otherwise sensitive data or non-personal data;
* where the competent authority is no longer able to effectively supervise the contracting authority due to the terms of the contractual arrangement or the circumstances surrounding it.

5. Cooperation with competent authorities

1. The partner undertakes to cooperate with the competent authorities, including the persons designated by them.

II.II Specific provisions according to the type of IT service

1. Supply and rental of hardware and software

1.1. Scope of Services and Subject Matter of the Contract

1. The provisions of this Chapter shall apply to hardware or software provided to a subscriber for a definite period of time or on a permanent basis.
2. Hardware is always delivered with pre-installed operating systems and system software (hereinafter: hardware). The associated system and operating software are also available to the contracting authority on a commercially available data medium. The hardware must be set up, installed, integrated, and configured by the partner and handed over to the contracting authority in a ready-to-use state, with ownership transferred to the contracting authority. If the contracting parties have agreed to provide the hardware for a limited time, the partner is responsible for performing the maintenance and repairs required to keep the hardware in contractual condition throughout the lease period. The provisions of point 2. 2 of the special part of these terms and conditions titled "Maintenance of hardware and software" also apply in this case.
3. The contracting authority shall be provided with software for use within the contractually defined scope. If agreed upon, the partner is obliged to install the software and hand it over to the contracting authority in a condition ready for operation. If the contracting parties have agreed that the software will be provided for a limited time, the partner will perform maintenance and repair services to ensure that the software is available for the duration of the service lease. The provisions of point 2. 2 of the special part of these terms and conditions: "Maintenance of hardware and software" also apply in connection with the stated provision.
4. As a rule, the partner provides the software in object code on a commercially available data medium in such a way that it can be implemented. If the client loses or accidentally deletes the software, the partner will replace it or substitute it free of charge.
5. The hardware and software must be supplied with generally understandable documentation, particularly on how to install, use, operate, or maintain them, in Slovenian or at least in English, and this is a mandatory contractual requirement.
6. The partner shall provide the contracting authority with instructions for the use of the hardware or software.
7. The purchase price or rental price for hardware and software covers all services provided by the partner referred to in this point of the General Terms and Conditions, including the granting of the rights of use defined in point 1. 2. of these Terms.

1.2. Rights of use

1. In the event that the contracting parties agree to purchase hardware or software, the partner providing the subject of the contract grants the contracting authority a non-exclusive, irrevocable, and permanent right to use the subject of the contract without spatial and substantive restrictions, including types of use not yet known at the time of contract conclusion. The contracting parties agree on the appropriate compensation if the rights of use are exercised for types of use that are not yet known at the time of the conclusion of the contract. The reproduction of the software submitted for contractual use, storage, including any necessary installation in IT systems, and the loading, execution, and processing of data are all examples of use. The right of use shall include, in particular, the right of the contracting authority or third parties to adapt and develop programmes that interact with the software on its behalf, including with a view to enabling interoperability with other systems and programmes.
2. If the contracting parties agree that the hardware or software will be leased, the partner providing the subject of the contract grants the contracting authority a non-exclusive right to use the subject of the contract for the duration of the contract and without spatial or substantive limitation, unless expressly agreed otherwise. The contracting authority may make backup copies in accordance with the provisions of the Copyright and Related Rights Act, which govern the substantive limitations of computer programme authorship.
3. In the event of the elimination of defects or the performance of maintenance services within the lease, the partner shall provide the contracting authority with corrections, updates, upgrades, or new versions of the software contained in the subject of the contract or updated documentation (hereinafter: updates), and all agreements agreed by the contracting parties for the provided software, including the granted rights of use, shall also apply to the updates.
4. All results of the work, in particular data or documents, in any form arising within or in connection with the use of the subject of the contract, are the property of the contracting authority. The contracting authority is entitled to all current or future rights for their use and exploitation. The partner is not entitled to use these results beyond the scope agreed by the contract between the contracting parties.
5. If special access tools, devices, or special permissions are required to use the contract's subject matter, the partner must provide them in sufficient quantities.
6. The contracting authority has the right to adapt the subject of the contract in the event of software modification, extension, or other processing, if it is necessary for the use of the computer programme in accordance with its purpose and provided that he has given the partner prior notice of the possibility of correcting the errors. The contracting authority shall have no right to use or exploit those adaptations. The contracting authority will also have the right to decompile the software in accordance with the provisions of the Copyright and Related Rights Act that govern decompilation conditions. The partner shall provide the contracting authority with all data and information required to enable interoperability with other hardware and software upon written request.
7. The contracting authority has the right to create and use copies of the software made available to him for backup and archiving purposes. If the contracting authority obtained the software through an online download, he may copy it to the data carrier unless otherwise agreed by other terms or contract.
8. The licence terms of third-party providers that are applicable in connection with the subject of the contract must be sent to the contracting authority in full along with the offer for software, or before the contract is signed; otherwise, these general terms and conditions apply in full.
9. The Triglav Group companies are entitled to the above rights if a fixed asset was also purchased for them or if they were users of services and it was not agreed otherwise.
   1. . Manufacturer's warranty
10. If the subject of the contract is covered by a manufacturer's warranty, the partner will eliminate all defects in the delivered goods free of charge during the warranty period, as well as properly perform improper or poorly performed services and eliminate errors in their results.
    1. . Testing and experimental operation
11. Before handing over the contract subject, the partner must first test it to ensure that it meets the contractual requirements as well as the product description and specifications. The partner shall assist the contracting authority in carrying out testing and trial operations upon request. Only after confirmation of successful completion of testing and trial operation shall the price and capacity risk pass to the contracting authority.
12. Testing and trial operation must be recorded in writing after completion, together with all errors that occurred in the performance of the contractual service. The contracting authority must confirm the successful testing in writing. If the requirements are not met, the contracting authority reserves the right to refuse confirmation. The partner must immediately eliminate the resulting errors, re-submit the contractual service for testing, and test the operation within the agreed dates and deadlines. When the testing and trial operation results are successful, it is assumed that the contractual service is ready for acceptance by the partner and acceptance testing with the contracting authority can begin. The partner shall provide appropriate assistance in carrying out the tests referred to in this point.

2. Maintenance of hardware and software

* 1. . Scope of services and subject matter of the contract

1. The provisions of this chapter shall apply to the provision of hardware and software maintenance services.
2. The partner undertakes to maintain and service the hardware. The partner keeps the hardware in good working order for the contracting authority and performs maintenance and related repairs.
3. If the partner takes over the maintenance of the contracting authority's existing system, all detected errors must be recorded in the takeover record. Faults are corrected by the partner as part of maintenance services, unless the scope of normal maintenance services is significantly exceeded and noted in the acceptance report. As part of maintenance, the partner must ensure that the hardware is permanently and properly functioning. This includes replacing hardware components that are defective, do not meet current standards, or are unsafe. The contracting authority will acquire ownership of the new hardware components upon their delivery. The partner removes the replaced hardware components and permanently deletes the data contained in them.
4. The partner undertakes to maintain the software, including the documentation. It keeps the software in a working condition suitable for the needs of the contracting authority as part of its maintenance services. The partner provides continuous software development and provides the contracting authority with upgrades and new versions on a regular basis, but at least once a year.
5. The partner plans maintenance work in such a way that the contracting authority's use of hardware and software is not impaired. If maintenance work cannot be avoided during the system's regular operating hours, the partner must notify the contracting authority and agree on the implementation with the contracting authority in a timely manner, or at least two weeks in advance. Updates that may affect the functioning of the software at the contracting authority must be installed in a maintenance time window agreed upon in advance by the contracting parties. The partner must take into account the existing system requirements when performing the services, as well as any updates.
6. When troubleshooting, the partner must take into account the agreed service levels.
7. All partner services defined in this chapter, as well as the provision of rights of use referred to in point 2.2 of this chapter, are included in the price of maintenance services.
   1. . Rights of use
8. The partner grants the contracting authority the rights to use the maintenance services in accordance with the contract governing the supply of hardware or software.
9. If the partner is in charge of limited maintenance of hardware or software on which the contracting authority has exclusive rights and the contracting authority has notified the partner, the partner must provide the contracting authority with the rights to updates in accordance with point 3.3 of these Terms.
10. In all other cases of limited hardware or software maintenance, the partner shall ensure the right to update in accordance with Section 1.2 of these Terms.
    1. . Errors and troubleshooting
11. If problems are not resolved to the required extent or within the agreed or reasonable time frame, the service contains errors. Non-essential defects can be corrected by the partner during the next scheduled maintenance.
12. If the contract is terminated early for any reason and the contracting authority is unable to timely transfer maintenance services to a third party or perform them by themselves, the contracting authority may request that the partner perform maintenance services even after the contract expires, when this is necessary to ensure the smooth operation of the contracting authority.

3. Custom software development by the contracting authority

* 1. . Scope of services and subject matter of the contract

1. The provisions of this point apply to the contracting authority's provision of concept design services for software, custom software development, or software customization.
2. The partner shall provide customised services to the contracting authority in the fields of conceptual design, software development, and customization, including the creation of software and processes, specifications as part of a rough, detailed, or test concept, and the creation and implementation of software design or applications (hereinafter: custom software).
3. If the partner is going to maintain custom software for the contracting authority, they must also follow the conditions in point 1.2 of these conditions ("Maintenance of hardware and software").
4. The partner will fully supply the contracting authority with the custom software, documentation, and all necessary documents for use in a ready or suitable-for-use state. As a rule, this also includes source code, development history documentation, quality assurance, processes and results, and the quality management systems and development tools used.
5. Custom software must be supplied with generally understandable documentation in Slovenian or at least English, which is considered an essential contractual obligation. The partner also provides documents and information related to the development of the software, which enables the contracting authority's professional staff to install, operate, maintain, and further develop the custom software.
6. The partner must install, integrate, and configure the custom software and hand it over to the contracting authority in a condition that is ready for operation and transfer ownership to the contracting authority.
7. Within the framework of testing and trial operations carried out in accordance with point 3.4. of these conditions, the partner shall assist the contracting authority in becoming acquainted with the custom software functions and, to the extent necessary, provide the contracting authority with instructions.
8. All partner services defined in this chapter, as well as the granting of the rights of use defined in point 3.3, are covered by the Custom Software Development Fee.
   1. . Responsibility and obligations of the partner
9. If the service includes software that does not originate with the partner or is not provided by the contracting authority, the partner acquires the software and makes it available to the contracting authority, unless otherwise agreed.
10. The partner keeps the contracting authority up to date on the status of service implementation.
11. The partner and its employees must be specially qualified to provide contractual services and have relevant experience. The contracting authority has the right to demand proof of this. If the partner fails to submit it, the contracting authority may request that the staff be replaced with more suitable personnel.
    1. . Rights of use
12. The ownership of all potential results of the partner and intermediate results created in the context of the development of the custom software, including source code, test and development reports, templates, ideas, drafts, plans, templates, samples, models, drawings, data records, service descriptions, documentation, programmes, software, including the devices created for it, customization services for existing software, and other service results (hereinafter: services or results of work) shall pass to the contracting authority at the time of their creation, except to the extent expressly specified otherwise in the contract.
13. Furthermore, unless otherwise agreed, the contracting authority acquires an exclusive, irrevocable, transferable, and sub-licensable right in time, space, and content to use these work results as soon as they are created, but no later than the moment they are handed over. This right of use encompasses all types of use, including storage, uploading, implementation, data processing, adaptation (including by third parties), including the permanent combination of the latter with the services of a partner, the right to reproduce and disseminate the work's results, the right to display and communicate them to the public, the right to their further marketing, and the right to make changes, processing, translation, additions, and further development, including without specifying the author.
14. If the ownership of the rights of the partner at the time of the contract's conclusion is required for the production or use of the contractual services, the contracting authority shall be irrevocably granted non-exclusive, free of charge, transferable, and sublicensable rights of use, which are unlimited in time and space, for the use of the contractual services by the contracting authority or authorised third parties. Prior to the commencement of works, the partner must communicate which of his property rights are important for the performance of the contractual service.
15. If the partner includes subcontractors, it must ensure by means of appropriate contractual agreements that the subcontractors also provide the above-mentioned results and rights of use to the contracting authority. The use of the contractual services by the partner or third parties requires the prior written consent of the contracting authority.
16. The Triglav Group companies are entitled to the above rights if a fixed asset was also purchased for them or if they were users of services and it was not agreed otherwise.
17. The revocation or termination of the contract shall have no effect on the sublicenses granted or the right of use.
    1. . Testing and test operation
18. Before submitting the subject of the contract, the partner must first test the subject of the contract himself in order to determine whether it meets the contractual requirements, product description, and specifications. The partner shall assist the contracting authority in carrying out testing and trial operations upon request. Only after confirmation of the successful completion of testing and trial operations shall the price and risk pass to the contracting authority.
19. Testing and trial operation must be recorded in writing after completion, together with all errors that occurred in the performance. The record must be signed by both parties. The contracting authority must confirm in writing the success of the testing and trial operation carried out. If the contracting authority's requirements are not met, the contracting authority may reject the performed testing. The partner must immediately eliminate the resulting errors and resubmit the contractual service for the performance test within the agreed dates and deadlines. When the testing and trial operation results are successful, it is considered that the contractual service is completed for the partner's acceptance, and acceptance testing with the contracting authority can begin, with the partner providing testing assistance to the required extent.
    1. . Specific requirements for the takeover of the service
20. The contracting authority must perform acceptance testing only after successful testing.
21. Errors in the contractual services detected during acceptance testing are:

* errors that mean that the contracting authority cannot use the subject matter of the contract or an economically significant part thereof;
* errors that result in significant restrictions on the use of important contract subject-matter functions that cannot be circumvented in a reasonable time;
* other errors.

1. If errors referred to in the first two indents of the previous paragraph are discovered, the contracting authority has the right to refuse to take over the subject of the contract and terminate the takeover. If the errors mentioned in the previous paragraph's last indent are discovered, the contracting authority may refuse to accept the service if the contractual service contains insignificant errors, or the work is hampered to an insignificant extent. In this case, the partner must correct the errors immediately and resubmit their services for acceptance testing. The partner shall bear all costs incurred by the contracting authority due to retesting and trial operation. The contracting authority's rights remain unaffected if the agreed-upon deadlines for performance are missed.
2. The contracting parties agree on the types of errors, priority, response time, and time to correct the error.
3. If the contracting authority accepts the service despite the identified errors, the errors are recorded in the takeover report, and the partner is required to eliminate them immediately.

4. Cloud services

1. Cloud services are those provided by cloud computing, which is a model for providing continuous and convenient on-demand network access to a common set of flexible computing resources (e.g., networks, servers, memories, applications, and services) that are available quickly and with little effort or interaction with the service provider.
2. In addition to the above provisions, as a provider of cloud services, the partner agrees to:

* to the extent that the provider of cloud services has an appropriate contractual relationship with the principal or equipment manufacturer whose licences are offered in its offer, which enables/allows it to enter into any contracts with the client in the required scope, type, and quality;
* that all data, information, evidence, statements, and documents provided by the cloud service provider in relation to itself and/or its subcontractors are true and accurate;
* to dispose of all necessary intellectual property rights, including materials made available by the partner (and/or any of its subcontractors) to the contracting authority, which are necessary for the performance of the obligations of the cloud service provider under the contract;
* adopt and implement, in accordance with the diligence of a good professional and established international professional standards, all reasonable measures to prevent the introduction, creation, or dissemination of any interventions (including viruses, worms and/or trojans, spyware, or other malware) into the systems, data, software or confidential data of the contracting authority (in electronic form) owned or controlled by the contracting authority and/or other customers using them.

1. The partner must ensure the provision of cloud services in such a way that the provision of services is measurable, documented, sufficiently granular, and verifiable. By contract or under general conditions, the contracting parties define the metrics used, which objectives are measured, and which decisions can be made according to the individual required objectives.
2. The partner (unless otherwise specified in the contract or general terms and conditions of the partner) reports to the contracting authority on a monthly basis by submitting reports at least on:
   1. the level of services used under the contract;
   2. the level of service where all the required objectives have been met;
   3. service levels where not all the required objectives have been met.
3. The partner is required to monitor the contract's required objectives and levels of service and to notify the contracting authority in a business-as-usual manner of any failure to meet measurable indicators/goals and the measures that the partner has implemented to meet the goals. In the contract, the partner and the contracting authority define the consequences of non-compliance with the objectives.
4. The partner may change the agreed levels of services, unless otherwise stipulated by the contract, exclusively in agreement with the contracting authority.
5. In the contract, the partner and the contracting authority define the manner (where feasible depending on the cloud service model) in which the contracting authority may propose changes to the services agreed upon in the contract, as well as the partner's obligation to respond to the contracting authority's proposal within a certain deadline and the conditions under which the proposal would be feasible, including any financial consequences for the contracting authority.
6. The partner must inform the contracting authority about the availability of data centres and the data preservation strategy, which includes resources, the relevant period, backup, data recovery, and data integrity verification. The availability information shall reflect the availability and downtime for a period of one year according to industry standards. The contracting authority has the right to test the required level of service availability at any time.
7. The partner is required to notify the contracting authority of the location of the data (where they are processed), as well as the countries to which the data are transferred, and to notify the contracting authority of any changes in a timely manner. The contracting authority has the right to terminate the contract in the event that it does not agree with the change of location of the data.
8. The cloud service provider is obliged to inform the contracting authority in the event that the cloud service provider ceases to exist or there is a threat that it ceases to exist (e.g., insolvency proceedings).
9. Unless otherwise specified in the contract, all contracting authority data processed in the cloud by the partner, as well as all data arising from the processing of client data (e.g., log files, backup copies, etc.), are the exclusive property of the contracting authority. The contracting authority shall always have the right to access this data in the cloud, and the partner shall provide permanent access to this data, unless otherwise specified in the contract.

4. Transmission or access to data

1. The transmission of data constitutes any transfer of data from the partner's databases to the contracting authority's databases.
2. Access to data refers to the contracting authority's ability to access the partner's databases and free disposal of this data or information, including subsequent manual entry into the contracting authority's databases.
3. The partner is obliged to ensure the quality of the data provided to the contracting authority. The data must meet all the criteria that define the quality of the data (accuracy, completeness, adequacy ...).
4. The partner is obliged to ensure that all its employees, as well as its contractual or external associates involved in the preparation or processing of this data, are familiar with the requirements for the provision of quality data for the contracting authority.
5. The duty to ensure data quality means that the aforementioned persons may not intentionally perform actions or omit due diligence that could have a negative impact on the quality of the data.

III. Annex to the special general conditions for partners or IT service providers

1. General

1. Additional provisions are binding for IT service providers for whom the contracting authority, in accordance with regulations and guidelines in the field of insurance or other binding regulations, assesses that, depending on the nature, extent of risks and effects of the contract on the contracting authority, they are crucial or important for the continuous operation of the contracting authority or essential for the operation of the contracting authority, since without them, the contracting authority would not be able to provide its services to its clients continuously, regularly, and on an ongoing basis.
2. If the contracting authority determines that the partner's services to the contracting authority would constitute a key or significant outsourcing of services due to the identified higher risks to the contracting authority's business, ensuring compliance with regulations, and potential impact on the contracting authority's reputation, the contracting authority will notify the partner in writing in advance.
3. The partner is aware that the contracting authority is required to notify the supervisory authority in the Republic of Slovenia: **Insurance Supervision Agency, Trg republike 3, 1000 Ljubljana, Slovenia about the partners and services referred to in point 1 of this Annex, as well as the content of the contracts and any changes thereto, prior to concluding, amending,** or terminating the contract with the partner. International cooperation of the Agency includes activities within the framework of insurance and occupational pension supervisory associations such as EIOPA ( European Insurance and Occupation Pensions Authority) and IAIS ( International Association of Insurance Supervisors). The Insurance Supervision Agency is also in charge of overseeing the implementation of outsourcing in insurance companies and with their partners, as stated in point 1 of this annex.

2. Technological safety

1. The partner referred to in the first paragraph of point 1 of this Annex shall ensure data security and storage in accordance with its internal acts and security policies, which shall include all necessary organisational, technical, and logical-technical procedures and measures to ensure information security and data protection (data and information confidentiality, authenticity, integrity, and availability). Internal acts or security policies shall govern at least the following obligations:

* that all premises where the information system or its parts or backups are located, as well as personal data on physical or electronic data carriers, are physically or electronically protected;
* the physical and electronic security of hardware, systems, and application software, including input-output units, and the security of personal data on physical or electronic media in accordance with the principles of information security;
* operational security (electronic security and network security, application security, audit trails and the like);
* identity and access management (authorizations, identities, key management, encryption, authentication, audit trails);
* resource management (inventory of information resources, powers and obligations regarding management, its location, security classification and ownership, and ensuring the separation of resources or at least data of different subscribers);
* established information security training and safety awareness programmes for all employees;
* carrying out testing of the elements of the information system in terms of safety and proper functioning;
* providing a business continuity plan and testing the plan;
* procedures and roles and responsibilities in the management of security/cyber and operational incidents;
* monitoring security and established adequate and effective capabilities to detect, report and respond to unusual activities and threats, such as physical or logical intrusions, breaches of confidentiality, integrity and availability of information assets, malicious code and publicly known vulnerabilities of software and hardware;
* the management and use of third-party licences or services used for and/or in connection with the provision of the services;
* an effective framework for information security testing is in place to confirm the reliability and effectiveness of information security measures and to ensure that this framework takes into account the threats and vulnerabilities identified through the monitoring of threats and the assessment of ICT security risks;
* an effective way of deleting or anonymising personal data of the information system insofar as it processes the data of the contracting authority on the basis of a decision of the contracting authority, competent state authority, local self-government authority or directly on the basis of applicable regulations;
* ensuring the secure transfer of data and preventing unauthorized access to personal data when transferring or modifying data during transfer, including transfer via public telecommunication means and networks;
* ensuring the use of encryption protocols or mechanisms that use a generally accepted cryptographic algorithm with key lengths and the manner of use in accordance with current best practices for all communications between ICT components and other data processing used to perform the service;
* prevent unauthorised access to personal data on physical media by ensuring that:
  + 1. data carriers with personal data are not left on open areas of office equipment or other places where they are accessible to unauthorised persons,
    2. personal data to be printed must be safely removed from printers after printing, wastepaper and other data carriers with personal data must be destroyed in such a way that it is impossible to read all or part of the destroyed data; the auxiliary material must also be handled in the same way;
    3. indestructible data carriers containing personal data must not be disposed of in trash cans, but must be safely destroyed;
* ensuring an effective system for managing safety risks.

3. Comprehensive descriptions of service levels and setting performance targets

1. Within the framework of the contractual provisions, the partner agrees to provide a comprehensive description of the service levels, including updates and corrections, that set precise quantitative and qualitative performance targets within the agreed service levels, so that the contracting authority can effectively monitor the information and communication technology services and take appropriate corrective measures without undue delay when the agreed service levels are not met.

4. Built-in and default personal data protection

1. The partner must perform the contractual services, in particular in relation to the development of the software, in such a way that, to the greatest extent possible and in accordance with best practices and standards, it strives to comply with the principles of privacy by design and privacy by default, which derive from the General Data Protection Regulation (GDPR). The partner will provide the contracting authority with documentation on the implementation of these requirements and the GDPR principles. When developing (in the context of the design and architecture of IT solutions), designing, selecting and using applications, services, and products based on the processing of personal data or which process personal data in the performance of their function, these measures may include minimizing the processing of personal data, pseudonymising personal data as soon as possible, transparency in tasks and processing of personal data, securing data throughout the data processing cycle, enabling data subjects to monitor data processing and enabling the subscriber or controller of personal data to establish and improve security measures. The integration of the concept of embedded privacy should not affect the effectiveness of the operation of the system.

5. Reporting of information security events

1. The partner is obliged to monitor and record each information security event (incident), i.e., any event that has or could have the following consequences in relation to the contracting authority:

* unavailability of the system or its part or services,
* disclosure of confidential data or loss or undesirable change of data,
* damage to or loss of equipment and assets, or
* any other act that violates the contracting authority's security procedures or policies.

1. The partner shall ensure that authorised and professionally trained employees respond to each information security event and take all necessary precautions to prevent the event's consequences and future occurrences.
2. When a partner discovers an incident that may have an impact on the contracting authority, the partner is required to notify the contracting authority without undue delay and, in accordance with the contracting authority's agreement, report on the status of the incident resolution. The partner is required to notify the contracting authority of incidents that constitute a violation of personal data protection in accordance with data protection regulations as soon as the violation occurs, or at the latest within the deadline determined by the contract on personal data processing.
3. In the event of an ICT incident, the partner is obliged to provide assistance to the contracting authority at no additional cost or at a predetermined price.

6. Compliance information

1. The partner is required to provide understandable and transparent information on any existing and valid certificates and attestations that have been certified or certified by the provider in relation to the services it offers and have been issued by independent third parties on:

* compliance of information security, business continuity and quality management systems with international standards;
* compliance with the GDPR, such as the adopted and approved Code of Conduct in accordance with the provisions of the GDPR or in relation to any binding business rules, insofar as it is obliged to comply with them;
* the adequacy and effectiveness of the internal control system;
* certificates or attestations for the specific requirements of cloud computing customers;
* trust services in accordance with the Regulation on the Implementation of the Regulation (EU) on electronic identification and trust services for electronic transactions in the internal market, where such a service is provided to the contracting authority;
* certification of hardware, software, and services in accordance with the Act on the Protection of Documentary and Archival Material and Archives or other certifications in accordance with European regulations
* or other similar services, where compliance with special conditions is required or recommended in connection with the service, perform certification or obtain the permission of independent third parties.

7. Business Continuity

1. The partner agrees to implement and carry out reasonable measures in its environment to ensure business continuity, allowing the contracting authority to continue providing services even in emergency situations.
2. If so expressly agreed with the contracting authority, the partner is required to provide a valid business continuity plan, the purpose of which is to ensure the smooth operation of the contracting authority's services, to establish procedures to prevent the interruption of business continuity activities, response times, to ensure the smooth operation of individual services, to describe the procedures in the event of a service failure, and to ensure compliance with the contract. The partner is obliged to align the business continuity plan with the contracting authority's requirements or the contracting authority's business continuity plan.
3. The partner shall take all necessary measures to preserve the data, including sufficient resources and availability of the data in accordance with the contracting authority's requirements, backup, data recovery and verification of data integrity.
4. The partner is obliged to regularly carry out testing of business continuity plans or the required level of service availability (at least once a year or whenever there is a major change in processes, equipment, or risk exposure; mandatory operational testing rules; simulation of the failure of the entire primary location; simulation of the restoration of operation at the primary location).
5. Upon the occurrence of an extraordinary event, the partner is obliged to ensure the performance of its services at the latest at the time specified in the contract with the contracting authority. In the event of an emergency, the partner will provide a replacement working environment in accordance with its own business continuity plans within the deadline specified in the contract with the contracting authority.

**8.** **Exit strategy**

1. The partner must carry out its responsibilities in such a way that the contracting authority can transfer the data back to its own implementation or to another contractor. For an appropriate and feasible transition to another partner or into its own implementation for this purpose, the capability of data export, the operational plan of data transfer, and other related measures are required. The contracting parties shall define the exit strategy in the event of termination of the agreement by contract and during the contractual cooperation. In the event that the contract is terminated, the partner agrees to assist and support the contracting authority in the transfer of data, systems, or applications that have been outsourced to another service provider or directly to the contracting authority until the contracting authority successfully transitions to a new solution.

9. Right of access and audit

9.1 General

1. The contracting authority has unrestricted access, inspection, and audit rights by the contracting authority or a designated third party and the competent authority for the purpose of continuous monitoring of the partner's performance, as well as the right to obtain copies of relevant documentation on the spot if they are critical to the partner's business, while other contractual arrangements or implementing policies do not impede or limit the effective exercise of these rights.
2. Internal audit contractors of the contracting authority, its external auditors or supervisory institutions of the contracting authority or other persons authorised by the contracting authority may carry out a due diligence or audit and review of the controls over the performance of the contract and any related contracts, access to data and invoices or copies thereof, in order for the contracting authority to verify the performance of the partner and the obligations agreed by the contract (hereinafter: supervision), and in particular to:

* verify the correctness of charging for services under the contract;
* verify the compliance of the partner and each subcontractor with the applicable law;
* identify or investigate actual or suspected breaches of regulations and irregularities or accounting errors, or any breach or threat of security, without specifically informing the partner of the purpose of the additional verification referred to in this indent;
* obtain the information and explanations necessary to fulfil the obligations of the contracting authority vis-à-vis the supervisory authorities in the Republic of Slovenia and/or in the European Union;
* obtain information for the purpose of conducting an internal audit with the contracting authority and the preparation, investigation, or confirmation of annual and other interim reports with the contracting authority;
* enable the national supervisory authorities responsible for the supervision of the contracting authority to carry out the inspection in accordance with the rules binding on the contracting authority;
* verify the accuracy and completeness of any management information supplied or required in accordance with the conclusion and performance of the contract;
* review reports and/or other records relating to the partner's performance in providing the services and verify that they reflect the partner's internal reports and records.

1. The partner shall provide permission to carry out the supervision referred to in this point of the terms and in the mutual agreement for its subcontractors.
2. The partner undertakes to cooperate with the contracting authority's supervisory authorities and other competent institutions or appointed third parties in all proceedings brought against the contracting authority, and to assist the contracting authority in making statements, submitting documentation, and other material and procedural actions in such proceedings, if necessary.
3. Supervision is carried out exclusively with regard to the performance of the contract or the provision of services within the framework of projects under the contract and in order to protect the interests of the contracting authority, the interests of the final customers, and the public interest.
4. Due diligence is carried out exclusively for the purpose of analysing and assessing various types of risks in connection with the purchase of the partner's service (material, legal, information and security, risks for the protection of personal data, etc.) and serves for further contractual regulation of the relationship between the contracting parties. The contracting authority has the right to immediately check or re-perform due diligence at the time of each conclusion of an additional contract or change of contract with a partner, or if the contracting authority becomes aware of significant deficiencies and/or significant changes in the services provided or the position of the partner.
5. The scope, manner, frequency of supervision and other mutual rights and obligations related to supervision, if they deviate from the provisions of this point of the terms and conditions, shall be regulated by the contracting parties by a contract, unless the general conditions of the partner or its partners would satisfactorily enable the contracting authority, its authorised persons, or the supervisory authorities of the contracting authority to effectively exercise the rights of the contracting authority to access and exercise the supervision referred to in this point of the terms and conditions. The partner is required to notify the contracting authority of the existence of the general conditions referred to in the preceding sentence no later than before the contract's conclusion and to allow him the necessary time to check the general conditions in the part referred to in the preceding sentence of this item.
6. The contracting authority may use, where appropriate and following prior verifications in accordance with the guidelines of the supervisory authorities that bind the contracting authority, (i) certificates issued by third parties and audit reports of third parties or internal audit reports provided by the partner; (ii) joint audits (carried out jointly with other parties of the same partner) or joint audits carried out by a third party appointed by the contracting parties.

9.2. Powers of the authorised person of the contracting authority

1. The authorised person of the contracting authority may, unless otherwise agreed in accordance with the thirteenth paragraph of this point of the terms and conditions, contact the partner or his subcontractor:

* inspect the premises, facilities, machinery, devices, means of work, installations, objects, goods, and documentary material relating to the performance of this contract;
* access all information (in any form);
* interview co-workers of the partner and, at the same time, review documents with which they can determine the identity of persons;
* take free samples of goods or materials and equipment of minor value that are not strictly necessary for their operation and examine the samples taken;
* photograph or digitally record people, places, facilities, installations, and other objects, as well as reproduce the documents, audiovisual recordings, and other documents referred to in the first indent;
* seize objects, documents, and samples to protect evidence;
* perform other actions consistent with the purpose of control.

1. The partner undertakes to inform the contracting authority about the scope, required procedures and frequency of inspections and audits.
2. The partner must ensure that competent persons are available at the time of the supervision, which must be announced in advance by the contracting authority, to provide explanations regarding the subject of the inspection or audit at the request of the authorised person performing the supervision. The partner must enable the authorised person performing the supervision to perform the tasks described in the first paragraph of this Article without interruption. Subject to the protection of business secrets and confidentiality, the partner shall, at the request of authorised persons exercising supervision, ensure reasonable cooperation and assistance with respect to any audit or inspection.
3. When performing supervision tasks, the authorised person may withdraw the documentation required to deal with the actual situation in the case for a maximum of 15 days if he believes there is a reasonable suspicion of violation of the applicable regulations, standards, and rules of the profession or this contract, and if this does not significantly interfere with the partner's or other supervised person's activities. Upon withdrawal of the documentation, the authorised person shall issue a written confirmation. The authorised person may not withhold documents or data that constitute a particularly sensitive business secret or such data, the transmission of which would constitute a violation of the applicable regulations.
4. The authorised person has the right to enter the premises and facilities, land, and parcels, as well as the equipment and devices mentioned in the previous paragraph, during normal working hours, unless the contract or applicable regulations state otherwise. The authorised person may not enter premises and facilities that the partner has expressly declared inaccessible in advance, because they have no essential connection with the execution of this contract and are specially protected due to provisions of applicable regulations or the partner's vital business needs. In doing so, it must adhere to the requirements of applicable regulations, international technical standards, and recommendations, and, to the greatest extent possible, the partner's internal acts and procedures.
5. If the authorised person of the contracting authority believes that they are not permitted to exercise control or obstruct it in violation of this contract, they must notify the responsible persons of both contracting parties. If, even on the basis of such a request, the partner does not allow control, he is obliged to explain the circumstances in writing to the contracting authority, which can act in accordance with the contract (serious breach of contract) and the applicable regulations. Information on any such escalation in supervision may be part of the report of the authorised person of the contracting authority.
6. The authorised person of the contracting authority may forward reports to the responsible persons of both contracting parties, including information on the scope and manner of supervision, identified shortcomings, and imposed measures.
7. If the authorised person of the contracting authority discovers a violation of the applicable regulations, standards, and rules of the profession or this contract while performing supervision tasks, he has the right and obligation to warn the partner of the irregularity or, in the case of major irregularities, to order measures to eliminate irregularities and deficiencies within the deadline determined by him in agreement with the partner. If the deadline cannot be determined unanimously, the authorised person of the contracting authority shall set a deadline that cannot be shorter than 30 days.
8. In determining the deadline for the elimination of irregularities, the authorised person of the contracting authority must consider the gravity of the violation, its consequences on the rights of individuals (end customers, employees, and others), and possible public interest, as well as the circumstances that depend on how long the partner or his subcontractor, under whose supervision the authorised person performs supervision, can eliminate irrationalities with due diligence.
9. If the partner fails to ensure the elimination of the identified irregularities and deficiencies within the deadline set by the authorised person of the contracting authority, the authorised person may, if necessary, stop the performance of certain contract tasks until the irregularities are eliminated or for as long as necessary. A longer suspension of tasks due to the fault of the contractual partner is considered a serious breach of contract.
10. If the authorised person of the contracting authority discovers, while performing supervision tasks, that the partner or his contractual partner, subcontractor, or supplier has violated the applicable regulations, interfering with the rights or legal benefits of other legal or natural persons, he is required to first inform the partner, and then these persons, and, upon their request, inform them of their findings, the measures imposed and other data necessary for the exercise of the rights of the affected persons.
11. Unless otherwise agreed, the contracting authority is obligated to pay the price of the partner's participation in the supervision referred to in the preceding Articles after completion of man/hours, unless:

* the incident occurred for reasons on the part of the partner;
* the audit shows that the service partner has unduly charged an amount equal to or greater than ten percent (10%) of the management costs to be paid for any contract year under the contract, then the partner shall reimburse the contracting authority for the reasonable costs related to the audit without prejudice to other rights of the contracting authority under the contract;
* the audit shows that the partner has unduly charged an amount equal to or greater than twenty-five percent (25%) of the management costs to be paid during any contract year, then the contracting authority has the right to terminate the contract.

1. The deviations referred to in point 9.2 may be regulated by the partner and the contracting authority by means of a contract, whereby the powers in substance include at least the rights of the contracting authority, competent authorities, or persons designated by them under point 9.1 of this Chapter of the Terms. The contract shall also specify the manner in which those powers are to be exercised.
2. Annexes:
   1. Annex 1: Business sustainability

**TRP (Business sustainability) form**

**SUPPLIER QUESTIONNAIRE**

**(Business sustainability)**

If the supplier does not meet all of the conditions in this form at the time of transaction or throughout the duration of the business relationship, Zavarovalnica Triglav, d. d., has the right to withdraw from the contract due to significant violations, and the supplier is obligated to cover all costs and/or damage incurred as a result of the violation of the given obligations.

1. The Company regularly and in a timely manner fulfils all obligations from employment contracts that comply with the applicable legislation within the legally and contractually determined deadline.

YES NO

1. The Company regularly and timely fulfils the obligations under contracts with employees who work for them through other forms of employment.

YES NO

1. The Company ensures a healthy and safe working environment for their employees and workers who work for them through other forms of employment (at least in compliance with the applicable legislation).

YES NO

1. The Company pursues a business policy that protects permanently employed persons and other workers from verbal, physical and sexual harassment.

YES NO

1. The Company respects the Constitution of the Republic of Slovenia, relevant sectoral legislation, and international legal acts in the field of human rights (does not use child, compulsory or forced labour, undeclared work, respects the prohibition of discrimination, etc.)

YES NO

1. The Company meets the requirements of environmental legislation in all countries of business operation.

YES NO

1. Do you have a code of ethics?

YES NO

1. Do you have a human rights policy in place?

YES NO

1. Do you have a diversity policy?

YES NO

1. Do you have a sustainability policy in place?

YES planning to in the following years NO

1. Are you reporting according to any sustainability standard?

Yes Yes, one Yes, two or more

1. By what standard do you report (indicate by which)?

GRI                  SASB                  TCFD               CDP                Other: \_\_\_\_\_\_

1. Are you calculating the company's carbon footprint?

YES NO

1. Provide carbon footprint data Scope 1 and 2 according to the location method (in tonnes of CO2 equivalent) in the current year:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Do you have goals to reduce your carbon footprint?

YES NO

1. Do you evaluate your suppliers according to ESG criteria?

YES NO

1. Do you invest in socially responsible projects?

YES NO

If the supplier fails to meet the conditions in the first six questions of this questionnaire for the duration of the business relationship, the contracting authority has the right to withdraw from the contract due to significant violations, and the supplier is obligated to cover all costs and/or damage incurred as a result of the breach of the given obligations.

With my signature, as the supplier, I expressly declare that the given answers are true.

Place and date:

Questionnaire completed by the authorised person of the supplier:

Answers were provided by the authorised person of the supplier:

*Name and surname that* guarantees their integrity and truthfulness:

*Name and surname:*

* 1. Annex 2: Preliminary assessment of the suitability of the supplier

PUD form

**SUPPLIER QUESTIONNAIRE**

**(Preliminary assessment of supplier suitability)**

**The questionnaire is completed by the supplier himself, accurately and in full.**

1. **General information**

1. Company/name and registered office of the supplier and name and surname of the legal representative and other persons authorised to represent:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. **Risk assessment**

1. Are your managers, members of the supervisory authority, procurators, company owners, or other management employees, to the best of your knowledge, closely related (related, friendly) to any of the members of the Management Board, members of the Supervisory Board or its committees, the procurator of Zavarovalnica Triglav, d. d., (hereinafter: ZT, d. d.), or persons who participate in the ZT's procurement processes? If so, please indicate the circumstances of such relations.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Do your company or its managers, procurators, members of supervisory bodies, or other management employees have ownership or management links with ZT, d. d.? If yes, please describe the nature and circumstances of such relations.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Are you facing proceedings before a labour, criminal, or other court for serious violations of the law, proceedings before the Commission for the Prevention of Corruption, or similar proceedings that could result in ZT d.d. losing its reputation as a result of doing business with you?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Do you finance political parties or other forms of political engagement, or have you financed them in the last five years?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. To the best of your knowledge, are any of your company's members of management, supervisory bodies, or ultimate owners considered politically exposed persons as defined in Article 61 of the current Anti-Money Laundering and Terrorist Financing Act? If yes, please state the names and surnames of these persons and the reason why they are considered to be politically exposed persons?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. To the best of your knowledge, are any of your management members, members of supervisory bodies, ultimate owners, or executives a close family member or close associate of a politically exposed person?

If yes, please provide the names and surnames of these persons and a description of the association with the politically exposed person?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

With my signature, as the supplier, I expressly declare that the entered data is true.

Place and date:

Questionnaire completed by the authorised person of the supplier:

The data was provided by the authorised person of the supplier:

*Name and surname that* guarantees their integrity and truthfulness:

*Name and surname:*