Procurement documentation for a tender of submitting a small value order procedure in accordance with Article 47 of the Public Procurement Act (Official Gazette of the Republic of Slovenia, No 91/15, with changes: hereinafter referred to as »ZJN-3«)

SUBJECT OF THE PUBLIC CONTRACT:

»SOFTWARE SERVICES/SOLUTIONS IN THE FIELD OF AML AND RESTRICTIVE MEASURES«

Reference no: JN 0581/2025

Contracting Authority:

SID – Slovenska izvozna in razvojna banka, d.d., Ljubljana,

Ulica Josipine Turnograjske 6, 1000 Ljubljana

Oktober 2025

Classification code: 30-81/2025-3

SID Banka

Podpisnik: STANKA ŠARC MAJDIČ
Izdajatelj: SIGEN-CA G2
Številka certifikata: 00E595996A0000000572843 5B
Potek veljavnosti: 14. 01. 2027
Čas podpisa: 24. 10. 2025 11:03

mag. Stanka Šarc Majdič
Member of the Management Board

SID Banka

Podpisnik: BORUT JAMNIK
Izdajatelj: SIGEN-CA G2
Številka certifikata: 0084E8C36C0000000572A2CAB
Potek veljavnosti: 03. 05. 2028
Čas podpisa: 24. 10. 2025 12:16

Borut Jamnik
Chairman of the Management Board

TABLE OF CONTENTS

1 Invitation, subject and information on the public contract 4
2 Submission of tenders, deadline for the submission of tenders and the opening of tenders....4
3 Access to and clarifications of the procurement documentation and contract award decision 6
4 Form, language and costs of drafting of a tender 6
5 Period of validity of a tender 8
6 Trade secrets and protection of confidential data 8
7 Joint tenders....8
8 Tender with subcontractors 9
9 Supplements, corrections, amendments or clarifications of tenders 10
10 Contract 11
11 Criterion 11
12 Tender price 14
13 Guarantees 14
14 Qualitative selection criteria and supporting documents 14
14.1 Grounds for exclusion 15
14.1.1 Absence of criminal record 15
14.1.2 Settlement of mandatory tax and other non-tax financial liabilities 16
14.1.3 Non-inclusion in the list of economic operators with negative references and compliance with the conditions regarding remuneration for work 16
14.1.4 Other grounds for exclusion 16
14.2 Terms and conditions of participation 17
14.2.1 Capacity to pursue a professional activity 17
14.2.2 Economic and financial standing 18
14.2.3 Professional capacity 18
14.2.4 Suitability of a Tenderer with regard to an assessment of reputation and compliance risk....18
14.2.5 Suitability of the Tenderer with regard to an evaluation of the status of information security 19
14.2.6 Suitability of the Tenderer with regard to an evaluation of the status using cloud services (SaaS) 19
14.2.7 Suitability of the Tenderer regarding data protection....20
15 Legal protection 20
16 Content of the tender documentation 22
17 Annexes 22
17.1 Basic information on the tender and Tenderer 23
17.2 Subcontractor's request for direct payment 25
17.3 Specifications....27
17.3.1 General information 27
17.3.2 Audit trail and data storage....33
17.3.3 Functional specifications....34
17.3.4 Technical specifications 36
17.3.5 Implementation (timetable and action plan) 39
17.3.6 Support and maintenance 40
17.3.7 Additional services 41
17.3.8 Implementation of specific services related to DORA, EBA Guidelines on Outsourcing and EBA Guidelines related to ICT and Security 41
17.4 Tender pro-forma invoice....43
17.5 References 48
17.6 Questionnaire to assess reputation and compliance risk 49

17.7 Questionnaire on methodology for evaluating the state of information security at the provider 55
17.8 Questionnaire regarding cloud data processing controls 61
17.9 Questionnaire for Personal Data Protection 66
17.10 Sample contract 74
17.11 Sample of the Exit Plan 94

INSTRUCTIONS FOR TENDERERS

1 Invitation, subject and information on the public contract

Pursuant to Article 47 of the ZJN-3, SID – Slovenska izvozna in razvojna banka, d.d., Ljubljana, Ulica Josipine Turnograjske 6, 1000 Ljubljana ("Contracting Authority" or "SID Bank"), invites interested Tenderers to submit written tender in accordance with this documentation.

The subject of the public procurement is implementation/integration of software services/solutions in the field of AML and restrictive measures of the services to support the compliance function in accordance with the technical and functional specification of the applications, and the maintenance of the applications for a period of three (3) years from the signing of the record of handover for the implementation/ integration of the software solution in the field of AML and restrictive measures.

The Contracting Authority will consider as admissible regarding the price a tender that does not exceed the Contracting Authority's guaranteed resources, which will be evaluated on the basis of the sum of:

- the price for implementation/integration of the software solution including training (cell 1F in "17.4 Tender pro-forma invoice" form)
- the price for the first year for user licences or software licences for approx. 70 named user licences or 10 concurrent licences, for up to 10,000 insights/inquiries (cell 2C in "17.4 Tender pro-forma invoice" form),
- the highest price for the second year for user licences or software licences for approx. 70 named user licences or 10 concurrent licenses, regardless of the number of insights/inquiries (cells between 2D and 4D in "17.4 Tender pro-forma invoice" form),
- the highest price for the third year for user licences or software licences for approx. 70 named user licences or 10 concurrent licenses, regardless of the number of insights/inquiries (cells between 2E and 4E in "17.4 Tender pro-forma invoice" form),
- total price for the duration of the Contract for additional services during regular hours (cell 5F in "17.4 Tender pro-forma invoice" form) and
- total price for the duration of the Contract for service implementation under DORA, EBA outsourcing guidelines, and EBA ICT and security guidelines (cell 6F in "17.4 Tender pro-forma invoice" form).

The subject of the public procurement is specified in detail under Specifications (Annex 17.3) in this documentation. The tendered services must meet the requirements set out in this documentation in full.

The subject of the public procurement is indivisible and shall not be divided into lots. Variant tenders are not permitted.

2 Submission of tenders, deadline for the submission of tenders and the opening of tenders

Based on the tenders received through this procedure, the Contracting Authority will invite tenderers fulfilling the minimum requirements (admissible tender as in point "1 Invitation, subject and information on the public contract", requirements in point "14 Qualitative selection criteria and supporting documents" and requirements in point "17.3 Specifications") to participate in negotiations. The date and details of these negotiations will be communicated via the e-JN information system.

Negotiations will primarily be conducted in writing using the e-JN information system. The minimum requirements and award criteria of the public procurement procedure shall not be subject to negotiation. In the context of the negotiations, the Contracting Authority will discuss mainly the price and all other terms and conditions specified in the documentation of submitted tenders with each tenderer's authorised representative. If required, oral negotiations may also occur. In such cases, representatives

must provide written authorisation signed by the Tenderer's responsible person unless that individual is presented as the legal representative.

Negotiations will be conducted in approximately two rounds. Minutes of all negotiations will be maintained and signed by authorised representatives from both the Contracting Authority and the Tenderer. These signed minutes will become an integral part of the tender. The signature of the minutes by the legal representative or authorised representative of the tenderer will be considered a new tender from the tenderer, which shall be identical, except in so far as it is negotiated, to the original tender submitted. Article 44 of the ZJN-3 may be applied to these negotiations.

In the first round, the Contracting Authority may negotiate in particular, but not exclusively, on the following matters: the contractual provisions of the public procurement, the substantive and technical presentation of the proposed solution, the implementation timeline, tender price,... until final documentation is aligned. In the event that the aforementioned negotiation areas also affect other fields or other sections of the documentation related to the award of the public contract, the Contracting Authority may also incorporate these areas into the negotiations. Therefore the Contracting Authority advises tenderers to ensure the presence of individuals with the necessary expertise and authorization for negotiations in the mentioned areas during the negotiations.

Subsequently, in the second (final) round, the Contracting Authority will invite both tenderers to submit their final offers based on the finalized documentation.

After receiving the final tender, the Contracting Authority will make a decision regarding the award of the public contract, which will be will be published on the Public Procurement Portal of the Republic of Slovenia.

Tenderers shall submit their tenders to the e-JN information system at https://ejn.gov.si/eJN, in accordance with Section 3 of the Instructions for using the e-JN system for use of the functionalities of electronic submission of tenders in the e-JN system: TENDERERS (the "Instructions for the Use of e-JN"), which form an integral part of this procurement documentation and are published online at https://ejn.gov.si/eJN.

Prior to submitting a tender, tenderers shall register at https://ejn.gov.si/eJN, in accordance with the Instructions for the Use of e-JN. Tenderers that are already registered on the e-JN information system should log into the application at the same address.

The user of a tenderer authorised to submit tenders in the e-JN information system shall submit the tender by clicking on the "Submit" button. Upon submission of a tender, the e-JN information system logs the user's identity and the time of submission of the tender. By submitting a tender, the user demonstrates and declares their intention to submit a binding tender on behalf of the tenderer (Article 18 of the Code of Obligations).[1] Upon submission of a tender, that tender is binding for the time stated in the tender, unless the tenderer's user withdraws or amends the tender before the deadline for submission.

A tender is deemed to have been submitted on time if the Contracting Authority receives it via the e-JN system (https://ejn.gov.si/eJN) by no later than **10:00 AM on 10 November 2025** (deadline for the submission of tenders). A tender is deemed to have been submitted if it is designated as "ODDANO" (SUBMITTED) in the e-JN information system.

Tenderers may withdraw or revise their tender up until the deadline for the submission of tenders. If the tenderer withdraws its tender from the e-JN information system, the tender shall be regarded as having not been submitted and the Contracting Authority shall not be able to see it in the e-JN system. If the tenderer revises its tender in the e-JN information system, the last submitted tender shall be available to the Contracting Authority in the system. Once the deadline for submission passes, tenders may no longer be withdrawn, revised or supplemented.

[1] Code of Obligations (Uradni list RS, Nos 97/07 [official consolidated text], 64/16 [Constitutional Court ruling] and 20/18 [OROZ631]).

Tenders submitted electronically via the e-JN information system shall be binding on the tenderer vis-à-vis the Contracting Authority. Consequently, electronically submitted and signed documents shall be binding on the tenderer vis-à-vis the Contracting Authority for the entire duration of the public contract award procedure and until the signing of the contract.

Tenders may not be submitted after the deadline for the submission of tenders has passed.

The opening of tenders shall take place automatically within the e-JN information system at noon on 10 November 2025 at https://ejn.gov.si/eJN.

3 Access to and clarifications of the procurement documentation and contract award decision

The procurement documentation is available free of charge on the public procurement portal (www.enarocanje.si). Tenderers should note that the ESPD is available only in electronic form and should be imported in XML format and completed in English at https://ejn.gov.si/espd/.

Tenderers may request additional clarifications regarding the documentation in English via the public procurement portal no later than by noon on 31 October 2025. Questions or additional clarifications may be submitted within the specific public procurement procedure under the tab 'Questions, Answers and Clarifications'. The Contracting Authority shall reply to enquiries, without mentioning the source, via the public procurement portal by no later than 5:00 PM on 4 November 2025. The Contracting Authority assumes no obligation to reply to enquiries not made in the manner and by the deadline specified above.

The Contracting Authority reserves the right to partly amend or supplement this documentation and, if necessary, extend the deadline for the submission of tenders. Amendments or supplements to the documentation and clarifications in the form of replies to enquiries shall form an integral part of the documentation.

The Contracting Authority shall award the public contract to the tenderer that submits the most economically advantageous admissible tender in accordance with the provisions of the documentation.

The Contracting Authority reserves the right to make use of all decision options set out in Article 90 of the ZJN-3 without any liability for damages.

The Contracting Authority shall publish the contract award decision on the public procurement portal. The decision shall be deemed to have been delivered on the day of its publication on the public procurement portal.

4 Form, language and costs of drafting of a tender

The content of a tender shall encompass the forms completed in accordance with the instructions for each form, and any required annexes to the individual forms:

1. a completed and signed »17.1 Basic information on the tender and Tenderer« form;
2. a completed and signed »17.2 Subcontractor's request for direct payment« form (if the Tenderer will be performing the contract with Subcontractors and the Subcontractors request direct payment);
3. a completed and signed ESPD for all economic operators in the tender;
4. a completed and signed "17.3 Specifications" form;
5. a completed and signed "17.4 Tender pro-forma invoice" form;
6. a completed »17.5 References« form;
7. a completed and signed »17.6 Questionnaire to assess reputation and compliance risk« form;
8. a copy of valid ISO/IEC 27001 certificate or completed and signed "17.7 Questionnaire on methodology for evaluating information security" form;

9. a copy of valid ISO/IEC 27017 or ISO/IEC 27018 certificate or completed and signed "17.8 Questionnaire regarding cloud data processing controls" form;
10. a completed and signed "17.9 Questionnaire for Personal Data Protection" form;
11. supporting documents (and completed forms) relating to compliance with the requirements laid down in Section "14.2 Requirements for participation" and "17.3 Specifications" of this procurement documentation;

The tenderer shall enclose with the tender the documents referred to in this section, as well as all other documents required under individual sections of this public procurement documentation. All documents submitted electronically shall meet the requirements and adhere to the instructions of the procurement documentation.

Tenderers that submit tenders in the e-JN system shall upload their own ESPD to the "ESPD – Tenderer" section and ESPDs from other participants to the "ESPD – Other participants" section. Tenderers that submit tenders in the e-JN system shall upload an electronically signed ESPD in XML form or an unsigned ESPD in XML form, whereby, in the latter case, in line with the General Terms and Conditions of Use of the e-JN Information System, a legally binding document will be deemed to have been submitted with the same validity as a signed document.

For other participants (all economic operators) in the tender, tenderer shall submit a signed ESPD under "ESPD – Other participants" in PDF format or in the form of an electronically signed XML file.

Tenders shall be submitted in English. Unless stated otherwise, foreign tenderers shall demonstrate their compliance with the requirements by means of copies of documentary evidence from official records demonstrating the required legal and factual status. If the competent authority of a foreign country does not issue such documentary evidence, or if such documentary evidence does not include all the required information, the person or economic operator shall submit a sworn statement or, if such statement is not provided for in the tenderer's country, a statement from the relevant person given before a competent judicial or administrative authority, notary-public or professional or trade organisation in that person's home country or in the country in which the economic operator is established. On the Contracting Authority request, Tenderers are obliged to translate documentary evidence from competent institutions and certified statements which are not in Slovenian or English into Slovenian by a sworn Slovenian translator.

Tenderers may submit brochures, certificates, confirmations and other technical documentation in a foreign language. If deemed necessary by the Contracting Authority, tenderers shall have any document provided in a foreign language translated into Slovenian (if so requested by the Contracting Authority by a sworn translator) at their own expense by a deadline set by the Contracting Authority.

The tender documentation shall be submitted on the forms annexed to these documents, or on forms produced by the tenderer that are identical in content. Where supporting documents are required, tenderers shall not be required to provide originals, and may submit a photocopy of any such document. The Contracting Authority may ask a tenderer to submit the original for inspection at any time during the tender review procedure. All documents submitted by tenderers shall reflect the current legally relevant situation (as on the day determined for the receipt of tenders), except where documents relating to a specific period or documents of a specific age are explicitly required. The age of documents may not exceed that stipulated by the individual provisions of this documentation. The Contracting Authority may subsequently (after the opening of tenders and at the tender review stage) request any documents demonstrating compliance with requirements or authorisations to obtain documents from public records. In that case, the Contracting Authority shall ask the tenderer to deliver all the documents required to demonstrate compliance with the relevant requirements by specified deadline. If a tenderer fails to deliver the requested authorisations or supporting documents by the deadline or fails to deliver the requested authorisations or supporting documents in accordance with the Contracting Authority's requests, the Contracting Authority shall exclude the tenderer's tender as inadmissible.

All expenses incurred in the process of drafting and submitting the tender shall be borne by the tenderer. In the event of suspension of the procedure, the exclusion of a tenders, the rejection of all tenders or withdrawal from the performance of the public contract, the Contracting Authority shall not reimburse

tenderers for any expenses incurred in the drafting of the tender. In no case shall the Contracting Authority be liable for any damage incurred as a result of such expenses, irrespective of the progress of the procurement procedure and the final selection of a tenderer. Tenderers shall be aware of this fact and signal their explicit consent to the provisions in question by submitting a tender.

5 Period of validity of a tender

A tender shall be valid for at least three (3) months after the deadline or the submission of tenders, which the Tenderers confirm by completing and submitting an »17.1. Basic information on the tender and Tenderer« form. Tenders with a shorter period of validity shall be rejected as inadmissible.

The Contracting Authority may ask a Tenderer to extend the period of validity of its tender for a specified additional period that exceeds three months. Should the Tenderer fail to comply with the request, the tender shall be deemed to have been withdrawn.

6 Trade secrets and protection of confidential data

Tenderers may designate documents or certain information as a trade secret, for example by appending "CONFIDENTIAL" or "TRADE SECRET" in the upper right-hand corner. If only certain information in a form or document is to be deemed confidential, the confidential part should be underlined in red and "CONFIDENTIAL" or "TRADE SECRET" appended on the same line in the right-hand margin. Tenderers shall also enclose with their tender a valid decision on trade secrecy. The Contracting Authority may not disclose any information submitted to it by an economic operator and designated a trade secret as stipulated by the law governing trade secrets, unless the same or another law provides otherwise. The Contracting Authority shall ensure that any information deemed to be personal or confidential data according to the laws governing the protection of personal data and the protection of confidential data is protected. Tenderers that learn of any confidential data in the course of participating in the procedure or performing contractual obligations shall protect such data in accordance with the applicable regulations.

Notwithstanding the first paragraph of Article 35 of the ZJN-3 on data protection and confidentiality, the following information shall always be public: specifications of the tendered goods, services or works and quantities in the specification, price per unit, the value of an individual item and the total value of the tender, and all information that has an effect on the ranking of the tender according to other criteria.

Enclosures and documents that a tenderer justifiably designates as confidential or a trade secret, or that is defined as such by the Contracting Authority, and personal data shall be accessible and usable only for the purposes of this public contract (i) by the Contracting Authority's personnel involved in this public procurement procedure, (ii) by the National Review Commission for the review of public procurement procedures (hereinafter: "National Review Commission") if it handles a request for review, and (iii) at the request of a competent state authority or court.

7 Joint tender

A joint tender from groups of contractual partners shall be permitted. Section 14 (Qualitative selection criteria and supporting documents) stipulates the requirements that shall be satisfied by each partner in a joint tender and those that may be satisfied by all the partners cumulatively. There may be no grounds for the exclusion of an individual joint tenderer.

In the case of a joint tender, legal persons shall specify all the participants in the joint tender in the ESPD, and provide appropriate signed copies of the ESPD for each contractual partner. Tenderers participating in a joint tender may also designate one legal person as the legal person with which the Contracting Authority will communicate until the adoption of the public contract award decision. Otherwise, the Contracting Authority shall address all documents to the lead party.

A contract on joint performance shall be enclosed with the tender in the case of a joint tender. An contract on joint performance shall include:

- the appointment of the lead party in the performance of the public contract;
- the authorisation conferred on the lead party and responsible person to sign the tender and the contract;
- a statement to the effect that all tenderers in the joint tender are familiar with the instructions to tenderers, the tender requirements and the criteria for the award of the public contract, and that they agree with them in their entirety;
- a statement to the effect that all the tenderers are familiar with the payment terms set out in this documentation;
- provisions regarding payment via the lead party;
- a statement to the effect that all the partners are jointly and severally liable to the Contracting Authority for the entire liability and for each of its parts.

The tender shall be signed by the lead party. The lead party is simultaneously the signatory of the contract and the main point of contact with the Contracting Authority.

8 Tender with subcontractors

Pursuant to the ZJN-3, a Subcontractor is an economic operator that is a legal or natural person that supplies services directly related to the subject of this public contract for the Tenderer with whom the Contracting Authority has concluded an Contract under the ZJN-3.

If a tenderer performs a public contract with subcontractors, it shall:

- list the names and registered offices of all the subcontractors, and every part of the public contract that the tenderer intends to subcontract, in the tender;
- list the contact details and statutory representatives of the proposed subcontractors in the tender;
- enclose ESPDs completed by the proposed subcontractors in accordance with Article 79 of the ZJN-3;
- enclose a subcontractor's request for direct payment if a subcontractor is requesting direct payment (in this case, such subcontractor shall complete and sign the Subcontractor's request for direct payment form (Annex 17.2)).

During the performance of the public contract, the lead contractor shall notify the Contracting Authority of any changes to the information referred to in the previous paragraph, and deliver the relevant information on any new subcontractors it plans to include subsequently in the performance of the works or services at least thirty days before the change. When including new subcontractors, the lead contractor shall also deliver with the notification the information and documents referred to in the second, third and fourth indents of the preceding paragraph.

The tenderer shall be liable vis-à-vis the Contracting Authority for the performance of the public contract.

The deadlines for payment to the lead contractor and its subcontractors (if the latter have requested direct payment) shall be identical.

The requirements laid down in Section 14. of the documentation may not be satisfied with subcontractors, unless explicitly stated or required in relation to a specific requirement. There may be no grounds for the exclusion of a subcontractor, i.e. each subcontractor is required to meet all the criteria set out in the procurement documentation forms. Should grounds exist for a subcontractor to be excluded or if a subcontractor does not meet the relevant requirements for participation laid down in Section 14 of the documentation, the Contracting Authority shall reject the subcontractor and request that they be replaced.

Should the selected tenderer replace subcontractors after the public contract is awarded, it shall obtain the Contracting Authority's written consent prior to such replacement, in which case any new subcontractor is obliged to meet the requirements set out in the documentation, as well as the requirements satisfied by the tenderer with the replaced subcontractor. The provisions applicable to

subcontractors shall also apply to subcontractors of subcontractors of the lead contractor and to subcontractors further along in the chain of subcontractors.

UTILISATION OF THE CAPACITIES OF OTHER OPERATORS

Should an economic operator state that it will be utilising the capacities of other operators, the Contracting Authority shall act in accordance with Article 81 of the ZJN-3. The economic operator may, where appropriate and permitted in accordance with the ZJN-3, refer to the capacities of other economic operators, irrespective of the legal nature of its relationship with them. A tenderer that wishes to utilise the capacities of other operators shall submit proof to the Contracting Authority that it has the necessary resources at its disposal to perform the contract. The Contracting Authority shall deem a written document proving the intent of the two operators (all relevant operators) to provide the necessary resources for the performance of this public service contract as appropriate proof.

Should the operators whose capacities the tenderer intends to utilise fail to meet the relevant selection criteria set out in these procurement documents and/or should there be grounds for exclusion, the Contracting Authority shall require the replacement of the operator that fails to meet the criteria, if the law so allows. Should the replacement not be successful or not be permitted, the Contracting Authority shall reject the tender.

9 Supplements, corrections, amendments or clarifications of tenders

If the Contracting Authority finds that any information or documents to be delivered by an economic operator are or appear to be incomplete or erroneous, or if individual information or documents are missing, the Contracting Authority may request that the economic operator submit the missing documents or supplement, correct or clarify the relevant information or documents by an appropriate deadline. The Contracting Authority shall only request that an economic operator supplement, correct, amend or clarify its tender if the Contracting Authority is unable to verify a given fact by itself. The tender shall be supplemented or amended in writing. The submission of a missing document or the supplementation, correction or clarification of information or documents may relate solely to those elements of the tender whose existence prior to the expiry of the deadline set for the submission of an application or tender can be objectively verified. Should the economic operator fail to submit a missing document or fail to supplement, correct or clarify the relevant information or documents, the Contracting Authority shall exclude the economic operator and/or reject the tender. Obvious or insignificant errors by the Tenderer can be overlooked.

Except in the case of the correction or supplementation of an obvious error, if the correction or supplementation does not entail the *de facto* submission of a new tender, the tenderer may not supplement or correct:

- its prices per unit (net of VAT), the values of items (net of VAT), the total value of the tender (net of VAT), except when the total value is being changed in accordance with the seventh paragraph of Article 89 of the ZJN-3, and the tender in terms of its criteria;
- that part of the tender tied to the technical specifications of the subject of the public contract;
- the elements of the tender that have the effect or could have the effect of changing the ranking of its tender relative to other tenders received by the Contracting Authority in the public procurement procedure.

Without prejudice to the previous paragraph, only the Contracting Authority may, with the written consent of the tenderer, correct errors in calculations identified during the examination and evaluation of the tenders. Such corrections may not include changes to the quantity and price per unit net of VAT. If it is established during the examination and evaluation of tenders that a calculation error has occurred on account of an incorrectly predetermined mathematical operation by the Contracting Authority, the Contracting Authority may, with the tenderer's written consent, correct the calculation error by applying the correct mathematical operation to calculate the value of the tender, taking prices per unit (net of VAT) and quantities offered by the tenderer into account. Without prejudice to the previous paragraph,

the Contracting Authority may, with the tenderer's written consent, correct an erroneously listed VAT rate.

The Contracting Authority may, in checking whether the requirements laid down in the documentation have been met, request that the tenderer submit an additional authorisation to obtain information from official records to enable the verification of information from official records.

10 Contract

The Contracting Authority shall conclude a contract on the performance of the subject of the public contract with the selected tenderer that meets the requirements laid down in this documentation after the public contract award decision becomes final. The content of the contract is set out in the Sample contract form (Annex 17.10).

After the contract award decision becomes final, the Contracting Authority shall send the selected tenderer an contract to sign whose content is identical to the Sample contract form (Annex 17.10). The Contracting Authority shall not permit the selected tenderer to alter the contractual provisions. Prior to its signature, the contract shall be adjusted to take account of agreed amendments that have been done during negotiations and whether the tenderer has submitted a joint tender or engaged subcontractors. If the selected tenderer fails to sign the contract by the deadline specified by the Contracting Authority, the Contracting Authority may deem the tenderer to have withdrawn from the contract.

The contracting authority will also conclude an 'Exit Plan' with the selected tenderer, as specified in point 17.11 (Exit Plan template) of the procurement documentation."

Pursuant to the sixth paragraph of Article 14 of the Integrity and Prevention of Corruption Act (Official Gazette of the Republic of Slovenia, No 69/11 [UPB2], hereinafter: "ZIntPK"), the selected tenderer shall, at the Contracting Authority's request and prior to signing the contract, submit a declaration or information on the participation of natural persons and legal persons in the ownership of the candidate, including the participation of silent partners, and on the economic operators that, according to the provisions of the law governing companies, are deemed to be affiliates of the candidate. If the tenderer submits a false declaration or provides false information with regard to the aforementioned facts, the contract shall be declared null and void.

At the Contracting Authority's request, the selected tenderer shall submit the following information in the public procurement procedure or in the course of the performance of the public contract within eight (8) days of receiving the request:

- its founders, partners, shareholders, limited partners or other owners, and details of their respective ownership shares;
- any economic operators deemed to be its affiliates under the provisions of the law governing companies;
- partners participating in the performance of the public contract, their founders, partners, shareholders, limited partners or other owners, and details of their respective ownership shares.

In the event of the withdrawal of the most advantageous tenderer from an admissible tender or the contract, the Contracting Authority reserves the right to select the next most advantageous tenderer, on condition that its tender is admissible.

In accordance with Article 90 of the ZJN-3, the Contracting Authority reserves the right not to select any tender.

11 Criterion

The Contracting Authority shall select the most advantageous tender on the basis of the criterion of the most economically advantageous tender.

The most economically advantageous tender shall be the admissible tender with the highest total score based on the following criteria:

1. The Contracting Authority shall award up to 5 points for the **criterion "Price for implementation/integration of a software solution including training"**, whereby the lowest-priced tender shall receive the highest number of points, i.e. 5 points. Each subsequent tender shall receive proportionally fewer points based on the lowest tender, according to the following formula: »The price for implementation/integration of the software solution including training (excluding VAT, in EUR)" of the lowest tenderer / "The price for implementation/integration of the software solution including training (excluding VAT, in EUR)" of the evaluated tenderer X 5 points.

The price to be taken into account as a criterion will be the price indicated under the heading "The price for implementation / integration of the software solution including training (excluding VAT (in EUR))" – cell 1F in "17.4 Tender pro-forma invoice" form.

2. The Contracting Authority shall award up to 20 points for the **criterion "Licences for use (the Contractor shall specify in a separate document the specification of the licences required and included in the price) for approx. 70 named users licences or 10 concurrent licences, for up to 10,000 insights/inquiries in accordance with the requirements of form 17.3 Specifications"**, whereby the lowest-priced tender shall receive the highest number of points, i.e. 20 points. Each subsequent tender shall receive proportionally fewer points based on the lowest tender, according to the following formula: "The price for the first year for user licences or software licences or concurrent licences (excluding VAT (in EUR))" of the lowest tenderer / "The price for the first year for user licences or software licences or concurrent licences (excluding VAT (in EUR))" of the evaluated tenderer x 20 points.

The price to be taken into account as a criterion will be the price indicated under the heading The price for the first year for user licences or software licences or concurrent licences (excluding VAT (in EUR)) – cell 2C in "17.4 Tender pro-forma invoice" form.

3. The Contracting Authority shall award up to 20 points for the **criterion "Licences for use (the Contractor shall specify in a separate document the specification of the licences required and included in the price) for approx. 70 named users licences or 10 concurrent licences, for between 10,001 and 15,000 insights/inquiries in accordance with the requirements of form 17.3 Specifications"**, whereby the lowest-priced tender shall receive the highest number of points, i.e. 20 points. Each subsequent tender shall receive proportionally fewer points based on the lowest tender, according to the following formula: "The price for the second year for user licences or software licences or concurrent licences (excluding VAT (in EUR))" of the lowest tenderer / "The price for the second year for user licences or software licences or concurrent licences (excluding VAT (in EUR))" of the evaluated tenderer x 20 points..

The price to be taken into account as a criterion will be the price indicated under the heading The price for second year for user licences or software licences or concurrent licences (excluding VAT (in EUR)) – cell 3D in "17.4 Tender pro-forma invoice" form.

4. The Contracting Authority shall award up to 10 points for the **criterion "Licences for use (the Contractor shall specify in a separate document the specification of the licences required and included in the price) for approx. 70 named users licences or 10 concurrent licences, for between 15,001 and 20,000 insights/inquiries in accordance with the requirements of form 17.3 Specifications"**, whereby the lowest-priced tender shall receive the highest number of points, i.e. 10 points. Each subsequent tender shall receive proportionally fewer points based on the lowest tender, according to the following formula: "The price for the third year for user licences or software licences or concurrent licences (excluding VAT (in EUR))" of the lowest tenderer / "The price for the third year for user licences or software licences or concurrent licences (excluding VAT (in EUR))" of the evaluated tenderer x 10 points.

The price to be taken into account as a criterion will be the price indicated under the heading The price for third year for user licences or software licences or concurrent licences (excluding VAT (in EUR)) – cell 4E in "17.4 Tender pro-forma invoice" form.

5. The Contracting Authority shall award up to 5 points for the **criterion "Additional services during regular working hours"**, whereby the lowest-priced tender shall receive the highest number of points, i.e. 5 points. Each subsequent tender shall receive proportionally fewer points based on the lowest tender, according to the following formula: "Total price for the duration of the Contract (price per hour (excluding VAT (in EUR) x estimated hours)" of the lowest tenderer / "Total price for the duration of the Contract (price per hour (excluding VAT (in EUR) x estimated hours)" of the evaluated tenderer x 5 points.

The price to be taken into account as a criterion will be the price indicated under the heading Total price for the duration of the Contract – cell 5F in "17.4 Tender pro-forma invoice" form.

6. If the Tenderer marks "Yes" in row No. 7 of the "17.4 Tender pro-forma invoice" form under **"The source from which the data are obtained"** and appropriately indicates the source of data (Watchlist, World Check or Dow Jones Watchlist), shall receive 5 points. If the tenderer marks "No", they shall receive 0 points.

The Contracting Authority shall verify compliance with the criterion based on the completed forms and submitted supporting documents relating to compliance with the requirements laid down in 17.3 Specifications of this procurement documentation.

7. If the Tenderer marks "Yes" in row No. 8 of the "17.4 Tender pro-forma invoice" form under **"Minimum data set (Software solution provides Information on sanctions of companies or natural persons in the ownership structure of the client (indirect sanctions – for example companies implicated as sanctioned under the OFAC and EU Ukraine/Russia Guidelines and other sanctions lists where the minimum ownership is 10%/25%)"**, shall receive 10 points. If the tenderer marks "No", they shall receive 0 points.

The Contracting Authority shall verify compliance with the criterion based on the completed forms and submitted supporting documents relating to compliance with the requirements laid down in 17.3 Specifications of this procurement documentation.

8. If the Tenderer marks "Yes" in row No. 9. of the "17.4 Tender pro-forma invoice" form under **"Advance Sanctions List Search Functionality (Software solution provides functionality for ad hoc searches and continuous processing based on the International Securities Identification Number (ISIN) through international sanctions lists and other official watchlists—including those published by OFAC (U.S. Department of the Treasury), the United Nations, the United Kingdom, and the European Union, and lists of terrorists organizations and individuals)"**, shall receive 10 points. If the Tenderer marks "No", they shall receive 0 points.

The Contracting Authority shall verify compliance with the criterion based on the completed forms and submitted supporting documents relating to compliance with the requirements laid down in 17.3 Specifications of this procurement documentation.

9. If the Tenderer marks "Yes" in row No. 10 of the "17.4 Tender pro-forma invoice" form under "**API requirements (Software solution within API requirements provides functionality for the transfer of screening results regarding sanctions and PEP/SOE or Software solution within API requirements provides functionality for the transfer of all screening results as specified in section 17.3.1 General information)"** and indicate that he will provide functionality for the transfer of screening results regarding sanctions or PEP/SOE, shall receive 5 points. If the Tenderer indicate that he will provide functionality for the transfer of screening results for all dataset as described under point C. Definition of dataset (minimum dataset) (Section 17.3.1), shall receive 10 points. If the Tenderer marks "No", they shall receive 0 points.

The Contracting Authority shall verify compliance with the criterion based on the completed forms and submitted supporting documents relating to compliance with the requirements laid down in 17.3 Specifications of this procurement documentation.

10. If the Tenderer marks "Yes" in row No. 11 of the "17.4 Tender pro-forma invoice" form under **"Process Automation and Client Data Modification Capability (Tenderer ensures that the service operates primarily through automated processes, requiring user data validation only when necessary (as specified in point H. Automatization and client data changes, Section 17.3.1) and/or Tenderer ensures further modifications of client name changes (as specified in point H. Automatization and client data changes, Section 17.3.1)"** and indicate that the service operates primarily through automated processes, requiring user data validation only when necessary (as specified in point H, Section 17.3.1), shall receive 3 points. If the Tenderer also enables further modifications of client name changes in accordance with the same section, this shall receive another 2 points. If the Tenderer marks "No", they shall receive 0 points.

The Contracting Authority shall verify compliance with the criterion based on the completed forms and submitted supporting documents relating to compliance with the requirements laid down in 17.3 Specifications of this procurement documentation.

The Most Economically Advantageous Tender (maximum 100 points) = criterion 1 (maximum 5 points) + criterion 2 (maximum 20 points) + criterion 3 (maximum 20 points) + criterion 4 (10 points) + criterion 5 (maximum 5 points) + criterion 6 (maximum 5 points) + criterion 7 (maximum 10 points) + criterion 8 (maximum 10 points) + criterion 9 (maximum 10 points) + criterion 10 (maximum 5 points)

In the event that a tenderer offers a price of zero EUR excluding VAT in whichever pro-forma invoice item, they shall be awarded the same number of points for that criteria as the tenderer offering the (second) lowest price for that criteria.

If two or more tenderers score the same number of points, the Contracting Authority shall regard the most advantageous tenderer as the tenderer that receives a higher number of points under the "Price" criterion (criterion 1 + criterion 2 + criterion 3 + criterion 4 + criterion 5).

If the Contracting Authority is unable to select the most advantageous tenderer based on that criterion, it shall select the most advantageous tenderer by means of a public drawing of lots. The date of the drawing of lots shall be set by the Contracting Authority. The contract shall be awarded to the tenderer that is drawn first.

12 Tender price

The tender shall encompass all the services being tendered as in 17.3 Specifications. Tenderers shall compile their tenders using the Tender pro-forma invoice form (Annex 17.4), which is an annex to this documentation.

Tenderers may not alter the content of the forms. Tenderers shall specify a price in EUR for every item in the pro-forma invoice rounded to a maximum of two (2) decimal points in the Tender pro-forma invoice form (Annex 17.4), and enclose the Tender pro-forma invoice form (Annex 17.4) with their tender. If the tenderer enters the price of zero (0) euros, it shall be deemed to be offering a specific item free of charge. If any item is already included in another item of the pro-forma invoice, the tenderer shall clearly indicate this in the pro-forma invoice (e.g. by writing "already included under item XY" in the relevant field). If the Contracting Authority identifies an obvious calculation error when reviewing and evaluating a tender, it shall act in accordance with the seventh paragraph of Article 89 of the ZJN-3. If a tenderer fails to enter a price (leaves a field empty or marks it with a slash) for a certain item in the Tender pro-forma invoice form (Annex 17.4), it shall be deemed to not be offering that item. In that case, the Contracting Authority shall reject the tender.

In the event of discrepancies between the data indicated under the "Total tender price" section the e-JN system and in the document that was submitted to the "Pro-forma invoice" section the e-JN system, the data in the document submitted to the "Pro-forma invoice" section shall be deemed valid.

The tender price net of VAT shall include all the elements of which it is comprised and all costs (labour costs, equipment costs, travel costs and all other costs that could arise in relation to the performance

of contractual works for the entire duration of the contractual period), fees and other levies (except for VAT), and any discounts or commissions, tax burdens and tax obligations waived so that the Contracting Authority is not liable for any costs connected with the subject of the public contract.

The prices in the tender pro-forma invoice shall be fixed until the completion of the public contract, unless the contract provides otherwise. The prices per unit shall remain the same as in the submitted tender in the event of any increase or reduction in the scope of equipment or services.

Tenderers shall upload the Tender pro-forma invoice (Annex 17.4) to the "Pro-forma invoice" section of the e-JN system in PDF format. The tender estimate, which is uploaded to the " Total tender price" section, is fully visible at the public opening of tenders and thus must not contain business secrets, personal or secret data.

The tendered services shall be in full compliance with the requirements set out in the documentation. Should the Contracting Authority determine that a tendered service does not meet the requirements set out in the Specifications form (Annex 17.3) and the other requirements set out in the documentation, it shall exclude the tender from further consideration.

13 Guarantees

Financial security is not required.

14 Qualitative selection criteria and supporting documents

Tenderers shall meet the requirements laid down in the ZJN-3 and the requirements laid down in this procurement documentation in order to be regarded as having capacity. Where a tenderer is participating in a joint tender or is to perform the public contract with subcontractors, the qualitative selection criteria, where stipulated in the procurement documentation, shall be met by each of the partners in the joint tender or each of the subcontractors listed by the tenderer in its tender. To determine capacity, the tenderer, individual members of a group of tenderers presenting a joint tender and nominated subcontractors shall complete, sign and submit a completed copy of the ESPD, annexed to the procurement documentation, in English.

In the submission of tenders, the Contracting Authority shall, in place of certificates issued by public authorities or third parties, accept the ESPD, which includes an up-to-date self-declaration as preliminary proof that the economic operator in question:

a) is not in one of the positions set out in Article 75 of the ZJN-3 that could exclude it from taking part in a public procurement procedure;
b) meets the relevant conditions for participation set out in Article 76 of the ZJN-3.

If an economic operator utilises the capacities of other entities under Article 81 of the ZJN-3, the ESPD information referred to in the previous paragraph shall also contain the required information in connection with the entities whose capacities are to be utilised by the economic operator.

The Contracting Authority may, at any time during the procedure, request that tenderers submit all relevant authorisations, supporting documents or parts of supporting documents relating to the statements made in the ESPD. Prior to awarding the public contract, the Contracting Authority may request certificates, declarations and other supporting documents as referred to in Article 77 of the ZJN-3 as proof of the absence of any grounds for exclusion under Article 75 of the ZJN-3 and as proof of compliance with the conditions for participation under Article 76 of the ZJN-3.

If a Member State or a third country does not issue documents and certificates, or if they do not cover all the cases referred to in the first and second paragraphs, point b) of the fourth paragraph and point b) of the sixth paragraph of Article 75 of the ZJN-3, these documents or certificates may be replaced by a sworn statement or, if this is not provided for in the Member State or third country, by a statement from the relevant person given before a competent judicial or administrative authority, notary-public or

professional or trade organisation in that person's home country or in the country in which the economic operator is established.

Information that is held in official records and for which the tenderer itself has not submitted supporting documentation may be verified by the Contracting Authority in the single information system (a database of tenderers and their tenders kept by the ministry responsible for administration), instead of in the official records, if the tenderer approves the Contracting Authority in this system.

If any grounds exist for exclusion, if a tenderer does not meet the conditions for participation, or if a tenderer's tender does not satisfy the Contracting Authority's needs and requirements as set out in the technical specifications (Specifications form, Annex 17.3) and the procurement documentation, the Contracting Authority shall reject such a tenderer or tender as inadmissible.

14.1 Grounds for exclusion

14.1.1 Absence of criminal record

The Contracting Authority shall exclude an economic operator from the public procurement procedure if, after performing checks pursuant to Articles 77, 79 and 80 of the ZJN-3, it determines or is otherwise apprised that a final judgment that includes elements of any of the criminal offences listed in the first paragraph of Article 75 of the ZJN-3 has been imposed on the economic operator, a member of an administrative, management or supervisory body of the economic operator, or a person empowered to represent or carry out decision-making or supervisory tasks at the economic operator.

Supporting document(s): Economic operators shall satisfy this requirement by submitting a completed ESPD in which the tenderer refers to **all persons** who are members of the administrative, management or supervisory body of the economic operator, including all persons who have powers of representation, decision or control therein. Economic operator must in the ESPD form in part II. Information concerning the economic operator, Section B: Information about representatives of the economic operator in the last section (If needed, pleas provide detailed information on the representation (its forms, extent, purpose, personal registration number,…)) state personal registration number for each member of an administrative, management or supervisory body of the economic operator, or a person empowered to represent or carry out decision-making or supervisory tasks at the economic operator.

The Contracting Authority reserves the right to request an appropriate supporting document or appropriate authorisation in accordance with the ZJN-3 after the deadline for the submission of tenders.

14.1.2 Settlement of mandatory tax and other non-tax financial liabilities

The Contracting Authority shall exclude an economic operator from participation in the public procurement procedure if, after performing checks pursuant to Articles 77, 79 and 80 of the ZJN-3, it determines that the economic operator has failed to settle mandatory tax or other non-tax financial liabilities under the law governing financial administration that are levied by the tax authority in accordance with the regulations of the country in which the tenderer is established, or the regulations of the Contracting Authority's country. An economic operator shall also be deemed not to have performed the obligations referred to in the preceding sentence if it has failed to submit all its withholding tax returns for employment earnings for the last five years by the day the tender or application is submitted. An economic operator is not excluded if it by the deadline for the submission of tenders or applications settles unpaid overdue obligations amounting to 50 euros or more and submits all its withholding tax returns for employment earnings for the period of the last five years from the deadline to submit an application or tender.

Supporting document(s): Economic operators shall satisfy this requirement by submitting a completed ESPD.

The Contracting Authority reserves the right to request, after the deadline for the submission of tenders has passed, that an economic operator submit appropriate authorisation or supporting document.

14.1.3 Non-inclusion in the list of economic operators with negative references and compliance with the conditions regarding remuneration for work

The Contracting Authority shall exclude an economic operator from participation in the public procurement procedure:

a) if on the day the deadline for submitting tenders expires, it has been excluded from public contract award procedures due to inclusion in the list of economic operators with the imposed side sanctions of exclusion from public contract award procedures;

(b) if during the three years prior to the deadline for the submission of tenders or requests, any fine has been imposed on the economic operator twice or more by virtue of one or more final decisions rendered by a competent authority of Slovenia, another Member State or a third country for a misdemeanour in connection with remuneration for work, work time, rest periods, performance of work on the basis of civil law contracts despite the existence of elements of an employment relationship, or undeclared work.

Where the economic operator is in the position referred to in point b) of the above paragraph, they may, in accordance with the ninth paragraph of Article 75 of the ZJN-3, no later than by the end of the deadline to submit an application or tender submit to the Contracting Authority evidence that they have taken sufficient steps, whereby they are able to demonstrate their reliability despite the existence of grounds for exclusion.

Supporting document(s): Economic operators shall satisfy this requirement by submitting a completed ESPD. If an economic operator answers YES in "Part III: Exclusion grounds, Section D: Purely national exclusion grounds", and is making use of the corrective mechanism, they should state, in the "Describe them" field, the breaches and the measures that enable them to demonstrate their reliability despite the existence of grounds for exclusion.

The Contracting Authority reserves the right to request, after the deadline for the submission of tenders has passed, that an economic operator submit appropriate authorisation or supporting document.

14.1.4 Other grounds for exclusion

The Contracting Entity will also exclude an economic operator from participation in the public procurement procedure in the following cases:

a) if insolvency or compulsory composition proceedings have been initiated against the economic operator under the law governing insolvency and compulsory composition proceedings, liquidation proceedings have been initiated against the economic operator under the law governing companies, the assets and operations of the economic operator are under the administration of a liquidator or the court, the business activities of the economic operator have been suspended, proceedings have been initiated against the economic operator in accordance with the regulations of another country, or a situation of equivalent legal consequences has arisen;

Supporting document(s): Economic operators shall satisfy this requirement by submitting a completed ESPD.

The Contracting Authority reserves the right to request, after the deadline for the submission of tenders has passed, that an economic operator submit appropriate authorisation or supporting document.

b) The Contracting Entity will exclude the Economic operator from participation in the public procurement procedure on the basis of the first paragraph of Article 5k COUNCIL REGULATION (EU) 2022/576 of 8. April 2022 amending Regulation (EU) No 833/2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine, if during the verification, he finds that he is an Economic operator;

- A Russian national, or a natural or legal person, entity or body established in Russia;
- b) a legal person, entity or body whose proprietary rights are directly or indirectly owned for more than 50 % by an entity referred to in point (a) of this paragraph; or

- c) a natural or legal person, entity or body acting on behalf or at the direction of an entity referred to in point (a) or (b) of this paragraph and any of the circumstances from points a), b) or c) are met.
- d) including, where they account for more than 10 % of the contract value, Subcontractors, suppliers or entities whose capacities are being relied on within the meaning of the public procurement Directives.

Supporting document(s): Economic operators shall satisfy this requirement by submitting a completed and signed »17.1 Basic information on the tender and Tenderer« for all Economic operators in the tender.

The Contracting Authority reserves the right to request, after the deadline for the submission of tenders has passed, that an economic operator submit appropriate authorisation or supporting document.

All the conditions set out in point 14.1 Grounds for exclusion must be fulfilled by each Economic operator to be included in the performance of the public contract.

Pursuant to the eighth paragraph of Article 75 of the ZJN-3, the Contracting authority shall exclude an economic operator (a tenderer, a tenderer in a joint tender, a subcontractor or operator whose capacity are to be used by a tenderer) from the public procurement procedure at any time during the procedure if it proves that, before or during the procedure during the procurement procedure, that economic operator was, by reason of acts committed or not committed, in one of the situations referred to in point 14.1 Grounds for exclusion.

14.2 Terms and conditions of participation

14.2.1 Capacity to pursue a professional activity

The economic operator shall be registered to pursue the activity that is the subject of this public contract in accordance with the rules of the country in which they are incorporated, and must have existed for at least five years.

Supporting document(s): Economic operators shall satisfy this requirement by submitting a completed ESPD and must submit an extract form the register or other proof.

The economic operator must satisfy the requirement for its part of the Contract.

The Contracting Authority reserves the right to request, after the deadline for the submission of tenders has passed, that an economic operator submit appropriate authorisation or supporting document.

14.2.2 Economic and financial standing

The average annual overall turnover of the economic operator in the last 3 financial years (2022, 2023, 2024) is at least 0,5 MIO EUR.

Supporting document(s): Economic operators shall satisfy this requirement by submitting a completed ESPD form (Economic operators are not required to complete the ESPD form in Part IV: Conditions for Section B: Economic and financial situation) and the closed balance sheets for each financial year. If the economic operator does not have a closed balance sheet for 2024, economic operator shall submit an uncompleted balance sheet or a self-declaration giving the annual overall turnover for the year 2024.

In the case of a joint tender, partners can meet the requirement together - the turnover of partners is aggregated; the Contracting Authority requires joint liability of the other party in case of utilising the capacities of other operators.

The Contracting Authority reserves the right to request, after the deadline for the submission of tenders has passed, that an economic operator submit appropriate authorisation or supporting document.

14.2.3 Professional capacity

a) References

A tenderer shall be required to demonstrate the following in order to have its capacity recognised:

- that in the last three (3) years, before the submission deadline tenders, it has successfully (in terms of quality, professionalism and in accordance with a contract) carried out at least three (3) similar software solution projects set up in the cloud and interfacing with the banking system via VPN, where they have ensured uninterrupted delivery of data and services of AML and restrictive measures to economic operators in the financial sector in the EU (bank, savings bank, insurance company, financial intermediary, fund, etc.).

A tenderer may not simultaneously be a reference client.

The Contracting Authority reserves the right to verify the detailed contents and quality of implementation/ integration of the project directly with the reference client, or to request that the tenderer submit to it for inspection any contracts or other documents that unequivocally prove the authenticity of the references.

Supporting document(s): Economic operators shall satisfy this requirement by submitting a completed References form (Annex 17.5).

In the case of a joint tender, partners can meet the requirement together.

14.2.4 Suitability of a Tenderer with regard to an assessment of reputation and compliance risk

In order to satisfy the requirement regarding the suitability of a tenderer with regard to an assessment of reputation and compliance risk, the tenderer shall be required to satisfy all the compliance criteria laid down by the questionnaire in the 17.6 Questionnaire to assess reputation and compliance risk form.

The tenderer shall be required to satisfy and maintain all compliance criteria for the entire duration of the contract.

Supporting document(s): Economic operators shall satisfy this requirement by submitting a completed ESPD and a completed 17.6 Questionnaire to assess reputation and compliance risk form.

The requirement must be met by every economic operator that will be involved in the execution of the public procurement.

14.2.5 Suitability of the Tenderer with regard to an evaluation of the status of information security

In order to satisfy the requirement of suitability with regard to an evaluation of the status of information security, the Tenderer shall enclose with the tender a valid ISO/IEC 27001 certificate or other equivalent certificate or standard. In the case of an equivalent certificate, the Tenderer shall specify the name of the certificate.

The selected Tenderer shall be required to maintain the standard or renew the certificate on a regular basis for the entire period of performance of the Contract.

If the Tenderer does not have the aforementioned certificates, the Tenderer's suitability must be met in order to fulfil the condition according to the evaluation of the state of information security when filling out the questionnaire in the form "17.7 Questionnaire on methodology for evaluating the state of information security at the provider" by obtaining at least 105 points. The Tenderer must give an unequivocal answer to each question (circle the appropriate answer).

In case of selection, the Tenderer is obliged to maintain the specified standard throughout the duration of the contract and to renew the certificate on a regular basis. In the event that the Tenderer demonstrates its compliance by fulfilling "17.7 Questionnaire for the evaluation of the state of

information security at the provider" the Tenderer must maintain at least the minimum required number of points (105 points) throughout the duration of the contract.

Supporting document(s): Economic operators shall satisfy the requirement by submitting a completed ESPD, a copy of a valid certificate for the ISO/IEC 27001 standard or another equivalent certificate or standard. In the case of an equivalent certificate or standard, they shall state the name of this certificate or standard. If the condition is met with a sufficient number of points, the Tenderer must submit a completed form "17.7 Questionnaire on methodology for evaluating information security«.

In the case of a joint offer, the condition must be met by the provider and each of the partners. In the case of bids with Subcontractors the condition must be met by the Tenderer and also each of the notified Subcontractor must submit the completed "17.7 Questionnaire on methodology for evaluating information security" from which it must be clear that Subcontractor has obtained at least 90 points. In the case of using the capabilities of others entities, the condition must be fulfilled by the Tenderer, and also each of the notified entities whose capacity will be used must submit the completed "17.7 Questionnaire of the methodology for the evaluation of the situation of information security at the provider", from which it must be clear that entity has obtained at least 90 points.

14.2.6 Suitability of the Tenderer with regard to an evaluation of the status using cloud services (SaaS)

In order to satisfy the requirement of suitability with regard to an evaluation of the status of using cloud services for the purpose of running the application (SaaS), the tenderer shall obtain at least 19 points when filling in questionnaire on cloud services in the "17.8 Questionnaire regarding cloud data processing controls" form (each answer YES in column "Checkpoint (YES/NO)" counts 1 point). Alternatively, the tenderer can meet this criteria by presenting valid ISO/IEC 27017 or ISO/IEC 27018 certificate.

The tenderer shall be required to satisfy and maintain all compliance criteria for the entire duration of the contract.

Supporting document(s): Economic operators shall satisfy the requirement by submitting a completed ESPD and a completed and singed "17.8 Questionnaire regarding cloud data processing controls" form or at least one of ISO/IEC 27017 or ISO/IEC 27018 certificate.

In the case of a joint tender, this requirement shall be satisfied by all partners. In the case of a tender using subcontractors or in the case of using the capabilities of others entities, all subcontractors offering cloud services or entities, shall satisfy this requirement.

14.2.7 Suitability of the Tenderer regarding data protection

In order to meet the suitability requirements for data protection, the Tenderer must complete "17.9 Questionnaire for Personal Data Protection" form and, if available, submit their most recent Privacy Policy/Statement.

Supporting document(s): Economic operators shall satisfy the requirement by submitting a completed and singed "17.9 Questionnaire for Personal Data Protection" and, if available, their most recent Privacy Policy/Statement.

In the event that the provider does not have a Privacy Policy/Statement, the parties shall conclude an appropriate personal data processing agreement.

The requirement must be met by every economic operator that will be involved in the execution of the public procurement.

15 Legal protection

Pursuant to Article 25 of the ZPVPJN (Official Gazette of the Republic of Slovenia, No 43/11 with changes: hereinafter referred to as »ZPVPJN«), a request for review that relates to the content of the

notice, invitation to tender or this documentation shall be lodged within ten (10) business days of the date of publication of the contract notice or notice of additional information, information on an incomplete procedure or a correction, if such notice serves to amend or supplement a requirement or criterion for the selection of the most advantageous tenderer. A request for review as referred to in the preceding sentence may not be lodged after the tender submission deadline, unless the Contracting Authority has set a tender submission deadline in the procurement procedure that is shorter than ten business days. In that case, a request for review may be lodged within ten (10) business days of the date of publication of the contract notice. After the tender submission deadline, the applicant may not allege breaches that were or should have been known to the applicant before the expiry of the deadline, except where permitted by the ZPVPJN and in cases where the applicant proves that it was objectively impossible to identify the alleged breaches before the deadline.

A request for review shall contain all the information and supporting documents laid down in Article 15 of the ZPVPJN: the name and address of the applicant and the contact person; the name of the contracting authority; the designation of the public contract or the public contract award or capacity recognition decision; the subject of the public contract; the authorisation to represent in the pre-review and review procedure (if the applicant is acting through proxies); and confirmation of the payment of the administrative fee under Article 71 of the ZPVPJN. The applicant's request shall include the alleged breach and the facts and evidence that prove that a breach occurred.

Pursuant to the first paragraph of Article 71 of the ZPVPJN, a fee of EUR 2,000 shall be paid to a bank account held with the Bank of Slovenia, Slovenska cesta 35, 1505 Ljubljana, Slovenia, no SI56 0110 0100 0358 802, SWIFT code BS LJ SI 2X, IBAN SI56011001000358802 and reference 11 16110-7111290-XXXXXXLL (in place of XXXXXXLL, enter the public contract number from the public procurement portal).

A request for review shall be lodged, along with proof of payment of the fee, via the eRevizija portal (www.portalerevizija.si).

16 Content of the tender documentation

A tenderer shall enclose with its tender the properly completed forms and other documents required in the "Instructions for tenderers", including a completed ESPD in English.

A tenderer shall also enter the required information in the blank fields of all the required forms.

17 Annexes

17.1 Basic information on the tender and Tenderer

Name of Tenderer: _____

Company's registered office: _____

Transaction account opened at the bank : _____

Registration number of the Tenderer: _____

Identification number of the Tenderer for VAT:_____

Person authorised to sign the tender and Contract: _____

As a Tenderer in the procedure for the awarding of public contract **JN-0581/2025 »Software services/solutions in the field of AML and restrictive measures«**, we are submitting a tender as per the enclosed documentation, whereby we intend to perform the contract (circle and/or write as appropriate):

Tender number: _____

We submit this tender (circle as appropriate):

(a)independently (b)with partner(s) (c)with the Subcontractor (d)capacity utilization other subjects

List of joint performance partners / Subcontractors / other subjects whose capabilities it uses economic operator (without business owner):

Number	Name of the economic operator	The role of the subject (circle as appropriate)
1.		PARTNER SUBCONTRACTOR ANOTHER SUBJECT, WHOSE CAPACITY IS USED ECONOMIC OPERATOR Description of the role (work, % of work, value):_____
2.		PARTNER SUBCONTRACTOR ANOTHER SUBJECT, WHOSE CAPACITY IS USED ECONOMIC OPERATOR Description of the role (work, % of work, value):_____
3.		PARTNER SUBCONTRACTOR ANOTHER SUBJECT, WHOSE CAPACITY IS USED ECONOMIC OPERATOR Description of the role (work, % of work, value):_____

Details of the contact person of the tender, who will also be the administrator of the contract:

Name and surname:	
Phone number:	
E-mail address:	

We declare:

- that the electronically submitted tender in the e-JN information system is considered dated and signed by us (except where a signature is specifically required for individual) and all parts of tender are binding for us as a Tenderer in relation to the Contracting Authority,
- that we accept all the conditions and requirements set out in the public procurement procedure (Specifications, Contract sample, Exit plan sample,...),
- that all information in our tender is true and non-misleading and that all copies of documents are identical to the original,
- that we will not transfer the awarded public tender to another Contractor ,
- that we will submit all necessary proofs at the Contracting Authority's request,
- that the tender is valid for at least three (3) months from the deadline set for tender submission,
- that we do not meet the conditions of the first paragraph of Article 5k COUNCIL REGULATION (EU) 2022/576 of 8. April 2022 amending Regulation (EU) No 833/2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine;
- that we will perform all contractual ICT functions and services in the territory of _____ and that we will process and store data in the territory of _____(*The tenderer shall complete appropriately*).

For the information in the tender, its accuracy and appropriateness, we assume full responsibility.

A form submitted electronically to the e-JN information system shall be considered to be dated and signed by the tenderer's responsible person. It is therefore binding on the tenderer vis-à-vis the Contracting Authority.

17.2 Subcontractor's request for direct payment[1]

Name of subcontractor: _____

Full address: _____

Transaction account opened at the bank : _____

Identification number of the Tenderer: _____

We request that the Contracting Authority, rather than the Tenderer, settle our claims against the lead Contractor, under the provisions of ZJN-3.

I, the undersigned legal representative _____ hereby request that the Contracting Authority make direct payment into our current account for the work that we performed for the public contract **JN-0581/2025 »Software services/solutions in the field of AML and restrictive measures«** in question in the amount stated in the tender, i.e. on the basis of an invoice issued by the Tenderer to the Contracting Authority. We agree with the deadlines and other payment terms referred to in the contract.

Details of the contact person on the Subcontractor's side:

Name and surname:	
Phone number:	
E-mail address:	

Place and date: Subcontractor's signature:

[1] *Complete only in the case of a tender involving a subcontractor that is requesting direct payment.*

17.3 Specifications

17.3.1 General information

The Tenderer must provide an IT solution that enables the Bank to carry out activities related to anti-money laundering and counter-financing of terrorism (AMLCF), as well as the implementation of restrictive measures. The solution must support the following functionalities:

- Verification of individuals (natural and legal persons) with regard to:
    - inclusion on sanctions lists,
    - politically exposed person (PEP) status,
    - presence of negative information.
- Capability for regular daily monitoring and ad hoc insight/inquiry.
- After a request is initiated and the check is performed, the solution must clearly indicate whether there is a match or not, returning either a positive or null result.
- In the event of a match (positive or null result), the solution must enable:
    - user review of the hit/result, and
    - determination of whether the match is a true positive or a false positive.
- The solution must support:
    - manual access and monitoring within the application, including manual upload of client data files and manual review of hit/results with decision-making; and
    - automated monitoring or access via API, including uploading client data files and/or receiving feedback on hits/results.

During the term of the contract, the contracting authority shall determine when to use either manual access as ad hoc insight/inquiry and manual regular monitoring within the application or assess (as ad hoc insight/inquiry)/regular monitoring via API, depending on its operational needs.

Regardless of whether the review and decision-making regarding hits/results is performed within the Tenderer's application or within the Bank's internal systems, the solution must support both scenarios.

The Tenderer must ensure that the tender price includes access to official sanction and compliance lists, such as (but not limited to) Watchlist, World Check, or Dow Jones Watchlist, or other equivalent sources.

The estimated number of service users on the part of the Contracting Authority is 70 named user licenses or 10 concurrent user licenses.

The Tenderer must clearly and comprehensively present its software solution in the submitted tender documentation, demonstrating compliance with all requirements specified below. As the Contracting Authority has not provided a standardized form, the Tenderer must submit the solution in its own format, ensuring that it is properly described and documented to allow for a thorough assessment of its compliance with the Contracting Authority's specifications.

A. Definition of client

Clients are all companies and individuals that are the subject to insight/inquiry.

B. Definition and execution of insight/inquiry and their hits/results

An *insight/inquiry* refers to a request to obtain a dataset for a specific client. The structure and content of the dataset are defined in Point C of this specification.

Each insight/inquiry must include a dataset corresponding to the client, as specified in Point C.

The minimum required input for conducting an insight/inquiry is:

- the business name of a legal entity, and/or
- the first name and surname of a natural person.

Additional criteria may be applied depending on the capabilities of the Tenderer's solution.

All insights/inquiries conducted for the same client within a minimum period of one (1) year (defined as 365 calendar days) shall be counted and charged as a single insight/inquiry, regardless of the number of requests/insights/inquiries or the results obtained for the same client during that period.

A *positive result* occurs when there is a match between the client and any part of the dataset obtained through the service.

- A true positive is a validated match confirmed by SID Bank.
- A false positive is a match deemed invalid by SID Bank.

A *null result* occurs when there is no match or insufficient correlation between the client's information and the dataset obtained through the service, as defined in Point C.

Example of counting of first year:

The first year means the period of one year counted from the day of the initial use of the service in the production environment.

Example: the day of initial use of the service in the production environment is 10 December 2025. The one-year period means 10 December 2025 to 9 December 2026 inclusive.

Example of counting of next year:

The next year means the period of one year from the end of the one-year period following the initial use of the service in the production environment.

Example: the day of initial use of the service in the production environment is 10 December 2025. The next one-year period means 10 December 2026 to 9 December 2027 inclusive.

Example of counting of insights/inquiries for client in one-year period:

An insight/inquiry for client A is first conducted on 5 January 2026. Over the course of one year, i.e. by 4 January 2027, 20 new insights/inquiries are conducted for this client A. Because all the insights/inquiries are conducted for the same client, all the insights/inquiries are included in the quota of insights/inquiries for client A, and are consequently counted as a single insight/inquiry for billing purposes, regardless of the result (positive result/null result).

C. Definition of dataset (minimum dataset)

The Tenderer must ensure that the solution provides access to and supports screening against the following minimum dataset:

- Sanctions Information – data on individuals and entities listed on international and national sanctions lists.
- Special Interest Persons (SIPs) – individuals flagged due to elevated risk profiles or associations.
- Politically Exposed Persons (PEPs) – including their related parties and close associates.
- Negative Media Reports – adverse media coverage relevant to financial crime, reputational risk, or regulatory concerns.

C.1 Information about sanctions

Watchlists must include individuals, companies, organizations, entities, vessels listed on international sanctions lists and other official watchlists. These must cover sources such as OFAC (U.S. Department of the Treasury), the United Nations (UN), the United Kingdom (UK), the European Union (EU), as well as lists of terrorist organizations and individuals.

C.2 Special interest persons

Special Interest Persons (SIPs) are typically well-known individuals with a documented history of financial crimes or other activities that pose significant risk. This category includes persons who present

an elevated risk profile and have been officially accused, charged, or convicted of any of the following types of criminal offences:

- Threats to national security,
- Financial crime,
- Organized crime,
- Terrorist financing,
- War crimes,
- Bribery and corruption,
- Human trafficking,
- Smuggling,
- Counterfeiting.

C.3 Politically exposed persons, their related parties and their close associates

The watchlist must include Politically Exposed Persons (PEPs), defined as government officials, politicians, and individuals with political influence globally, as well as their family members and close associates.

C.4 Negative media reports

The Tenderer must ensure that the solution includes access to negative or adverse media information concerning individuals, organizations, or entities (clients). This information must be publicly accessible and sourced from a variety of open resources, including but not limited to:

- News articles,
- Social media platforms,
- Regulatory publications,
- Court records,
- Other publicly available sources.

Negative information about clients relates to all negative news about the client in connection with:

- measures and fines imposed on the client by the competent regulator
- a history of money laundering, fraud, and other criminal offences of a financial nature
- involvement in terrorist financing
- a history of financial crime
- appearance on a sanctions list, past or present
- accusations of fraud
- involvement in cyber crime
- a history of violent or sexual crime
- human trafficking, illegal arms trading and drug trafficking
- non-compliances with ESG standards
- other negative information that damages the client's reputation

Each result containing negative media must include:

- the full content of the media report, and
- a direct link to the original source (e.g. webpage URL).

D. Process types

The IT solution must support both types of processes:

- Ongoing (scheduled) processes, such as regular daily monitoring and automated screenings via API, and
- Ad hoc (on-demand) processes, such as manual and automatic insights/inquiries or one-time checks initiated by the user.

The solution must ensure seamless execution of both process types, whether initiated manually within the application or automatically via API integration.

D.1 Ongoing process

The Tenderer must ensure that the IT solution supports and automates the ongoing daily screening process, with the following minimum capabilities:

- The solution must perform daily screening of SID Bank's entire set of clients eligible for such screening.
- Screening means obtaining results (positive result/null result) through insights/inquiries across the required data described under point C (the dataset).
- Screening must involve generating results (positive or null) through insights/inquiries based on the dataset defined under Point C.
- The set of clients eligible for daily screening is determined by SID Bank and must be accessible via API or uploaded manually on predefined form. The API must allow the Tenderer's system to retrieve or receive the list of eligible clients.
- The solution must allow SID Bank to initiate reviews of screening results at any time.
- The process must be automated as follows:
  - The Tenderer's system must either receive the list of eligible clients via API or access it directly.
  - The system must generate screening results for the client set and enable SID Bank to download the results package, either through the Tenderer's application or via (API) the Bank's internal system.
  - The Tenderer must describe its proposed data exchange approach in the tender submission. Technical integration details will be agreed upon at project kick-off.
- The solution must support user classification of positive results as:
  - True positive,
  - False positive.
- Clients classified as false positives must remain in the daily screening process. If new relevant information arises (e.g. inclusion on a sanctions list or newly assigned PEP status), the system must generate updated results accordingly.
- The solution must support execution of user decisions either within the Tenderer's system/application or within SID Bank's core system.

D.2 Ad hoc search

The Tenderer must ensure that the IT solution supports and automates ad hoc screening processes with the following minimum capabilities:

- The solution must support ad hoc (manual and automatic*) insights/inquiries for both new and existing clients of SID Bank;
- Each ad hoc screening must generate results (positive or null) based on the dataset defined under Point C;
- The ad hoc process must be automated as follows:
  - SID Bank sends client-specific information to the Tenderer's system via API or enter them manually within Tenderer's system.
  - The Tenderer's system generates screening results for the specified client and enables SID Bank to download the results package, either through the Tenderer's application or the Bank's internal system.
  - The Tenderer must describe its proposed approach to data exchange in the tender submission. Technical integration details will be finalized at project kick-off.
- Automatic insights/inquiries must be supported via integration with the Contracting Authority's systems. The integration method (e.g. online services) will be agreed upon at project kick-off.
- The solution must allow users to classify positive results as:
  - True positive,
  - False positive.
- The solution must support execution of user decisions either within the Tenderer's system/application or within SID Bank's core system.

*The Tenderer must ensure that automatic ad hoc insights/inquiries are supported via integration with the Contracting Authority's systems. The integration method (e.g., online services) shall be agreed at project kick-off.

E. The volume of insights/inquiries

The Tenderer must provide pricing in the "17.4 Tender Pro-Forma Invoice" for the first contract year and each subsequent year, stated per year and excluding VAT (in EUR), based on the following ranges of insights/inquiries performed via the ongoing and ad hoc processes:

- Up to 10,000 insights/inquiries per year
- From 10,001 to 15,000 insights/inquiries per year
- From 15,001 to 20,000 insights/inquiries per year

The pricing must be quoted for:

- User licences, or
- Software licences, or
- Concurrent licences

The Tenderer must take into account that the application will be used by approximately 70 named users or 10 concurrent users.

F. Reporting

The Tenderer must ensure that the IT solution provides the following reporting functionalities:

- A report must be available at all times upon user request and must include:
    - Defined dataset information
    - Date of last insight/inquiry
    - Positive and null results per dataset category
    - Decision on each positive result (true positive or false positive), including:
        - ○Date of decision
        - ○User comment (regardless of result classification)
    - Date when the person/entity was added to the relevant list
    - Identification of the list that triggered the result (e.g., EU list, OFAC list, PEP status, Ukraine list)

This report must be generated regardless of the process type (ongoing or ad hoc), as defined under Point D.

An excerpt per individual client must be available at all times upon user request and must include:

- Defined dataset information
- Date of last insight/inquiry
- Positive and null results per dataset category
- Decision on each positive result (true positive or false positive), including:
    - ○Date of decision
    - ○User comment (regardless of result classification)
- Date when the person/entity was added to the relevant list
- Identification of the list that triggered the result (e.g., EU list, OFAC list, PEP status, negative news, Ukraine list)

The excerpt must be exportable in .pdf format and must include the date of excerpt generation.

The Tenderer must ensure that the IT solution provides, upon user request, a report containing all inputs, changes, and actions/decisions made by any user.

Reports must be available in .csv, .xlsx, or any other format that enables further data processing by the user *Example of report:*

Example of report:

	Dataset			
Insight/inquiry	Information about sanctions	Special interest persons	Politically exposed persons, their related parties and their close associates	Negative media reports
Result	X or 0	X or 0	X or 0	X or 0
Date of insight/inquiry (regardless of result)	DD/MM/YY	DD/MM/YY	DD/MM/YY	DD/MM/YY
Decision	TP or FP	TP or FP	TP or FP	TP or FP
Comment of decision	Content or blank	Content or blank	Content or blank	Content or blank
Decision date	DD/MM/YY	DD/MM/YY	DD/MM/YY	DD/MM/YY
Type of list	Description or blank	Description or blank	Description or blank	Description or blank
Date of inclusion in the list	DD/MM/YY	DD/MM/YY	DD/MM/YY	DD/MM/YY
User	User ID/name	User ID/name	User ID/name	User ID/name

Note on Table Indicators and Format:

- "X" indicates that screening has been conducted and a positive result was returned. This may represent either a true positive (e.g., the PEP is a client) or a false positive (e.g., the PEP is not a client).
- "0" indicates that screening has been conducted and a null result was returned (e.g., no relevant match in the dataset for the client).
- Date and Decision Date: The date format shown is for illustrative purposes only. Other valid formats (e.g., MM/DD/YY) may be used.
- "TP" stands for a true positive decision.
- "FP" stands for a false positive decision.

The table layout in the example is intended to illustrate the required dataset content and does not prescribe the exact format for data presentation.

G. User interface – client view

Regardless of process type as defined in point D, namely ongoing process or ad hoc process, the bank wishes to always obtain identical data and information on a specific client in user interface, including results of insights/inquiries (positive result/null result, including information on true positive/false positive decision).

Example of client view in user interface:

If a result (null and/or positive) is issued for a client within the ongoing process, this result must be visible every time the client is viewed in user interface, the same applies to a result issued through the ad hoc process.

H. Automatization and client data changes

The Tenderer must ensure that the service operates primarily through automated processes (whenever client data was put in the system manually or via API), with user validation required only where necessary. The solution must support the following:

- Automated Processes:
  - Daily insights/inquiries for clients (whenever data was entered manually or via API), returning null or positive results.
  - Automatic assignment of PEP/Sanctions labels to clients based on true positive results, with optional user validation (if available).
  - Direct automated email notification to a designated address when a positive result is obtained, sent within minutes and without user involvement.
  - Automated detection of client data changes (e.g., name/surname changes or changes in legal representatives of a client company) when client data is checked via API or when changes are entered manually.
- User Confirmation Requirements
  - Manual decision on each positive result, determining whether it is a true positive or false positive.
  - Validation of automatically assigned PEP/Sanctions labels (if available).
- Client Data Modification
  - The service must allow modification of a client's name, middle name (if applicable), and surname without requiring full re-entry of client data.
  - The history of name changes must be recorded in the audit trail, as defined in Section 17.3.2.
  - When viewing a client in the user interface, all records—both before and after the name change—must remain visible and accessible.

17.3.2 Audit trail and data storage

The Tenderer must ensure that the IT solution provides a comprehensive audit trail for each insight/inquiry performed through the dataset, with the following minimum capabilities:

- The audit trail must be accessible to users directly within the service.
- A report of the audit trail must be available to users on demand.
- For each system-generated insight/inquiry, the audit trail must include:
  - Date of the insight/inquiry
  - Type of result (null or positive)
  - Comment (if available)
- For each user-generated input, change, or decision (including classification of positive results as true or false positive), the audit trail must include:
  - Date of the activity
  - Type of activity
  - Comment (if available)
  - Identification of the user (e.g., full name, unique user ID, email address, or equivalent)
- All data obtained through insights/inquiries (the dataset) must be stored and retained in accordance with applicable data retention policies.
- The audit trail must support basic filtering and sorting of events (e.g., by date, user, activity type).
- The solution must support integration with a System Incident and Event Management (SIEM) system for centralized logging of key events, including:
  - Date and time
  - User identification
  - Login and logout events
  - Other relevant system actions
- The Tenderer must guarantee full operability of the solution in compliance with the General Data Protection Regulation (GDPR) at all times.

The Tenderer must ensure that the software solution provides adequate audit trails in all components where personal data, financial data, or security scheme data (e.g., access rights) are processed.

Audit trails must be sufficiently detailed in terms of content, storage, and monitoring mechanisms to serve as evidentiary material before judicial bodies. The solution must enable audit trail reports to be viewed and transcribed for internal and external audit purposes using an appropriate tool.

Audit trails must comply with all applicable legislation, particularly the General Data Protection Regulation (GDPR). The solution must adhere to the following definition of an audit trail.

The software solution must implement all statutory elements of personal data protection, including:

- Data masking
- Pseudonymisation and/or anonymisation
- Data deletion options in accordance with GDPR
- Definition of grounds for viewing and/or processing personal data

The solution must include procedures (scripts and processes) for preparing and anonymising test data in development, test, and pre-production environments. These procedures must include automated scripts for transcription and preparation of test data.

17.3.3 Functional specifications

Obligatory software solution functionalities:

	Obligatory software solution functionalities	**The tenderer's software solution meets the requirement (Tenderer indicates Yes/No)**	**Tenderer must specify from which document in tender (page, paragraph, ...) is evident that the tenderer's software solution meets the requirement**
1.	**in the area of ongoing processes and insights/inquiries:** • the software solution must support the screening of the entire set of SID bank's clients and the process described in subpoint D.1 (Section 17.3.1).	Yes / No	
2.	**in the area of ad hoc searches and insights/inquiries:** • of daily ad hoc searches of SID bank's clients and the process described in subpoint D.2 (Section 17.3.1) .	Yes / No	
3.	**in the area of reporting:** • software solution must support the generation of excerpts per client and reports per set of clients on the aforementioned insights/inquiries incorporating requirements as	Yes / No	

	described in point F (Section 17.3.1).		
4.	**in the area of audit trails and data storage:** • software solution must include audit trail and data storage functionality as defined in Section 17.3.2.	Yes / No	
5.	**user interface – client view** • the user interface must incorporates the features and capabilities as specified in point G (Section 17.3.1).	Yes / No	
6.	**software solution's compliance** • software solution must be compliance with the General Data Protection Regulation as described under Section 17.3.4 Technical specifications	Yes / No	
7.	**API integration with bank system** • API must provide data retrieval and update operations relevant to software's core functionality as described in "API requirements" under Section 17.3.4.	Yes / No	

17.3.4 Technical specifications

The Contractor will be required to implement/ integrate the tendered software solution using a software as a service (SaaS) solution linked to the Contracting Authority's information system as agreed and in line with the Contracting Authority's requirements. The tendered SaaS solution must ensure that all data including daily changes and system logs is processed and stored in the cloud, with physical storage and processing in the EU. Data storage (i.e. backup procedures) and processing must be provided in the EU for the entire duration of the contract.

The Tenderer must ensure the software solution's full compliance with the General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016) in the area of personal data protection. Procedures for personal data protection must be put in place (provable by ISO certification or a completed form 17.8 Questionnaire regarding cloud data processing controls).

Requirements with regard to data:

- encrypted storage of sensitive data;
- communications for data exchange and for triggering mutual software processing or downloading/uploading of data between the Tenderer (SaaS) and the Contracting Authority are encrypted via a virtual private network (VPN), the tenderer putting in place a site-2-site VPN connection with the Contracting Authority for this purpose (technical security details to be agreed between the Contracting Authority and the Tenderer);
- if data is transferred within the cloud via public networks, the communications are secured by encrypted connections and by the use of secure and sufficiently strong encryption algorithms, e.g. strict TLS 1.2 or higher;
- the physical location for personal data storage must be in the EU, for the primary and backup environments alike;
- personal data is simple to cancel;

- full transfer of the data stored in the application to the Contracting Authority based on a demand by regulatory body or supervisory authority (national or European) after termination of the contract regarding cloud services is ensured;
- the option of the permanent deletion of the Contracting Authority's data stored in the application after termination of the contract regarding cloud services is ensured.

API requirements

Bank needs to integrate its own internal application with Tenderer's software service via APIs. Internal application supports onboarding of clients. For all legal entities involved in onboarding process (the borrower, their affiliated legal entities, and all associated natural persons), it is necessary to obtain dataset information (point C, Section 17.3.1) which is obtained through the software service as already described in previous sections.

Internal application supports also process of regular monitoring of clients and conducting of additional business relationships where the client is already onboarded. Also this process requires to obtain dataset information (point C, Section 17.3.1) which is obtained through the software service as already described, but this is not considered as new insight/inquiry as the first insight/inquiry during the onboarding of the client was already performed. It is necessary that process via API allows to obtain results of any insight/inquiry.

The goal of the integration is to enable bank users, through the internal application, to retrieve screening results via API after entering all required data. These results are displayed on-screen i.e. user interface (in internal application), and the decision on whether to proceed with onboarding is sent back to the software service via API integration. Additionally, information about the user who performed the screening and confirmed the decision (for audit trail purposes: user, date, action, comment if applicable) is also transmitted via API integration to the software service.

For the purpose of daily process of screening bank needs to assure connection to the set of clients that are eligible for ongoing daily process of screening via API. Results of daily process of screening and confirmation of the decision taken have to be available withing the application.

The API must enable the entry of clients into the set of clients and their subsequent removal for this set.

The data exchange is conducted through requests and responses managed by each application. The Tenderer must also supply relevant technical documentation to enable the bank's application to prepare for the desired integration.

API must be exposed as either RESTful API or SOAP based Web service. It should use standard data formats (JSON for REST, XML for SOAP).

Complete API documentation must be provided, including but not limited to:

- Description of all available endpoints and operations;
- Required parameters and their data types;
- Expected responses;
- Description of Error messages;
- Authentication and authorization requirements.

Monitoring requirements:

- the Contracting Authority or its supervisory body may conduct an audit of the cloud application at the Contracting Authority's location;
- the Contractor of the cloud application must conduct audits of the cloud service at its own initiative;
- the Contractor of the cloud application must arrange for external audits of the cloud service at its own initiative;
- the Contracting Authority has access to the reports on the external audits of the cloud service;

- the Contractor of the cloud application undertakes to inform the Contracting Authority regarding security incidents within 24 hours of learning of the incident;
- the Contractor of the cloud application undertakes to disclose information to the Contracting Authority regarding the architecture and security of the leased rights;

Test environment

The tendered software solution must provide for the option of putting in place:

- a test environment[2], and
- a user acceptance test (UAT).

Network connections

The software solution must be described in the tender and equipped with a network diagram (network scheme) to clearly illustrate and list the data flows and the inclusion of the solution in the computer network, and which communication protocols or ports are used in the computer network. In the tender the Tenderer must submit, in its own format (**the Contracting Authority has not prepared a form**), a description of the network connections, a list of the data flows and a network diagram or scheme with instructions for the approach to service provision.

User authentication and authorisation

The tendered software solution must provide for the central administration of user rights.

Two-factor authentication (2-FA) is required for the cloud software solution. MFA must be compatible with Microsoft 2FA within the 365 solutions and with the Microsoft Authenticator mobile application.

The user authentication and authorisation method (two-factor authentication) must be described in the tender. In the tender the Tenderer must submit, in its own format (**the Contracting Authority has not prepared a form**), a description of the method of user authentication and authorisation (two-factor authentication) and the approach to service provision.

Upgrades and updates

The Tendered software solution must provide for periodic upgrades and updates with the aim of continually maintaining the latest technological and functional standards. The upgrades and updates must be implemented without any impact on the existing functionality. Each new issue or version must come with a changelog and instructions for installation. The Contractor must provide all versions of regular upgrades of software solutions to the Contracting Authority.

	Technical specifications	**The tenderer's software solution meets the requirement (Tenderer indicates Yes/No)**	**Tenderer must specify from which document in tender (page, paragraph, ...) is evident that the tenderer's software solution meets the requirement**
1.	**Network connections** • software solution must be described in the tender and equipped with a network diagram (network scheme)	Yes / No	

[2] The test environment should comply with standards and best practices as used in financial institutions, and be aligned with DORA and EBA guidelines. This means it should use test data, maintain appropriate audit trails and event logs, have separate identity authentication (users) from the production environment, and maintain at least an equivalent state (version) as production.

	to clearly illustrate and list the data flows and the inclusion of the solution in the computer network, and which communication protocols or ports are used in the computer network as described above.		
2.	**User authentication and authorisation** • Two-factor authentication (2-FA) is required for the cloud software solution. MFA must be compatible with Microsoft 2FA within the 365 solutions and with the Microsoft Authenticator mobile application as described above	Yes / No	

17.3.5 Implementation (timetable and action plan)

Implementation includes installation, configuration, testing, training of key users, and initiation of full use of the software solution, and will take place at the Contracting Authority's location or as defined in contract.

The training of key users will encompass the training of 15 of the Contracting Authority's employees.

In the tender the Tenderer must submit, in its own format (**the Contracting Authority has not prepared a form**), a rough plan of phased implementation with time deadlines, which must comply with the deadlines cited below, the anticipated engagement of the Contracting Authority's employees, and the approach to service provision, in particular the integration of the Contracting Authority's system with the Tenderer's system.

The Contracting Authority will provide technical support in the area of AML and restrictive measures via three of its expert personnel in the amount of five (5) person days per month.

The implementation of the software solution will generally proceed according to the following deadlines (the implementation deadlines will be precisely coordinated with the Contractor in the kick-off meeting with regard to the Contracting Authority's time availability):

- as a general rule, the basic system shall be implemented within four months from the date of signing the Contracting Authority's contract, and shall be made available for testing in the test environment by the Contracting Authority;
- the full system is put in place in accordance with the technical and functional specifications within one month of the confirmation of a successful test.

The Contractor undertakes to implement the solution for the Contracting Authority in accordance with the timetable and action plan, and according to the deadline agreed by the Contracting Authority and the Contractor during kick-off.

	Timetable and action plan	**The tenderer's software solution meets the requirement (Tenderer indicates Yes/No)**	**Tenderer must specify from which document in tender (page, paragraph, …) is evident that the tenderer's software solution meets the requirement**

1.	• the Tenderer must provide a rough plan of phased implementation with time deadlines, which must comply with the deadlines cited below, the anticipated engagement of the Contracting authority's employees, and the approach to service provision, in particular the integration of the Contracting authority's system with the Tenderer's system	Yes / No	

17.3.6 Support and maintenance

Licenses and maintenance of the implemented application begins on the day of the signing of the record of handover for the supply and implementation of the software solution, and lasts for 36 months or until the expiry of the third (final) annual renewal of licences.

Maintenance regime

Maintenance services must encompass:

- assistance in system settings and upgrades of the software solution (regular upgrades are included in the licence price),
- assistance in installation of security and security-critical revisions and other system upgrades published by the producer of the system and software solutions,
- rectification of incidents and/or problems on the basis of a defect report by the Contracting Authority,
- technical support,
- assistance in the maintenance and configuration of the software solution.

Support and defect reporting

An interruption in the operation of the software solution can be of either technical or content-related nature. If an interruption in the software solution is identified, the Contracting Authority will, at its own discretion, send a notification to the Contractor containing the information detailed below. In the notification, the Contracting Authority categorizes the interruption according to the following criteria:

- **Critical Interruption**
  The Contracting Authority is unable to use the software solution, which critically impacts the performance of its activities. Examples include: corrupted data; no workaround available; resolution requires major configuration changes in the software solution; the interruption causes significant damage to the operating system or hardware; loss of key functionality.
- **Serious Interruption**
  The Contracting Authority can use the software solution but with significant limitations. No temporary workaround is possible. Examples: frequent program crashes or shutdowns; workaround is inadequate or ineffective. A failure may be classified as a serious rather than critical interruption if caused by unusual or irregular command sequences.
- **Moderate Interruption**
  The software solution can be used by the Contracting Authority but with limitations. A temporary solution is required. Examples: interruptions with acceptable alternatives that do not seriously affect operations; interruptions that prevent usage of a specific procedure; misleading user interface.
- **Minor Interruption**
  The Contracting Authority can avoid the minor interruption and continue to use the software without issues. Examples: a workaround becomes a permanent solution; correct usage is evident; cosmetic flaws; slight loss of flexibility.
- **Negligible Interruption**
  Negligible interruption does not affect the Contracting Authority's work. For example: the user notices the interruption but does not use the affected functionality and therefore experiences no consequences.

The response time in case of interruptions and the time required to resolve each type of interruption or error within the software solution (as part of maintenance services) is determined based on the interruption severity, as outlined in the following table:

Severity of Interruption	Response Time (from receipt of Contracting Authority's report)	Resolution Time (from receipt of Contracting Authority's report)
Critical or Serious Interruption	Within two (2) working hours	Within eight (8) working hours
Moderate Interruption	Within four (4) working hours	Within twelve (12) working hours
Minor or Negligible Interruption	Within eight (8) working hours	Within twenty-four (24) working hours

RESPONSE TIME – the time from the moment the incident is reported to when the Contractor begins diagnosing and resolving the error. Hours are counted as Contractor's working hours.

RESOLUTION TIME – the time from the incident report until restoration of the software solution's functionality. Hours are counted as Contractor's working hours.

The response time in the case of a telephone report begins after receiving a written report (via email or the Contracting Authority's protocol). If the Contracting Authority submitted the report during working hours, it is considered that the Contractor received the report on the first full hour after the time the email was sent. If the Contracting Authority submitted the report outside of maintenance hours, it is considered that the Contractor received the report at 8:00 AM on the first maintenance day following the date the report was submitted

Support and defect reporting is undertaken primarily via email and/or by phone or via the Contracting Authority's portal, which the tenderer will be able to access.

The Contractor is available to the Contracting Authority as follows when providing support:

- working hours (8:00 AM to 4:00 PM CET+1), Monday to Friday, via the phone number and email address stated in the contract.

17.3.7 Additional services

For all additional services not covered in implementation/ integration or maintenance that the Contracting Authority explicitly orders as an extra, the Contractor must provide an estimate of the cost and the workload for the ordered work, which must be approved in writing by the Contracting Authority in accordance with its bylaws for confirming and approving changes and orders.

The Contracting Authority's assessment is that over the lifetime of the contract there will be 200 hours of work on additional services, which will be performed during normal working hours. The Contractor will cite the price for a single hour in its tender quote. The hours of additional services are cited as a broad estimate, and are utilised as necessary, with regard to written requests submitted by the Contracting Authority, which for the agreed services are implementation/ integration exclusively on the basis of an order received from the Contracting Authority in writing, thereby confirming the work executed and the quantity of hours. The estimated value and quantity of hours do not commit the Contracting Authority to the use of a total quantity of hours, and merely represent an estimated maximum value and estimate of the services in question.

17.3.8 Implementation of specific services related to DORA, EBA Guidelines on Outsourcing and EBA Guidelines related to ICT and Security

The Contracting Authority is required to comply with the following regulations when awarding the public contract:

- Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011,
- Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/78/EC, based on which the Guidelines on outsourcing (EBA/GL/2019/02) and the EBA Guidelines on ICT and security risk management (EBA/GL/2019/04) were issued.

Location where data will be processed and stored

The Contractor undertakes to provide the Contracting Authority in advance with a list of countries where all contractual ICT functions and services will be outsourced or subcontracted, including locations where data will be processed and stored. The Contractor must specify the countries and locations in the form "17.1 Basic information on the tender and Tenderer".

Right to access, inspections and audits

The Contracting Authority informs the Contractor that, in accordance with the DORA regulation (Article 28, point 6), it will enforce the right to access, inspections, and audits. The frequency of audits and inspections and the areas to be audited will be defined by the Contracting Authority based on a risk assessment (before and during the contractual relationship). Auditing will be carried out in accordance with generally accepted auditing standards and all supervisory instructions on the application and inclusion of such auditing standards.

Implementation of ICT services with subcontractors

In the case of the implementation of ICT services with subcontractors, the Contractor must assess all risks associated with the location of the subcontractor providing the ICT services and the risks associated with the parent company and the location from where the ICT service will be provided.

The Contractor shall transfer its contractual obligations regarding monitoring and reporting based on the contract with the Contracting Authority in writing to the subcontractor providing the ICT service and demonstrate this to the Contracting Authority upon request.

The Contractor must ensure the continuity of ICT services that are the subject of the contract and are subcontracted throughout the entire chain of Subcontractors.

The Contractor undertakes to specify in a written contract with the Subcontractor the ICT security standards and additional security requirements that will ensure an equivalent level of security in the performance of the services that are the subject of the contract, as must be ensured by the Contractor.

A form submitted electronically to the e-JN information system shall be considered to be dated and signed by the tenderer's responsible person. It is therefore binding on the tenderer vis-à-vis the Contracting Authority.

17.4 Tender pro-forma invoice

The Tenderer shall upload this Tender pro-forma invoice Tender pro-forma invoice**form (Annex 17.4) to the "Pro-forma" section of the e-JN system separately from other tender documentation.**

The tender prices shall be drawn up in accordance with the public procurement documentation for public contract no **JN-0581/2025 "Software services/solutions in the field of AML and restrictive measures"** and cover all the required services. If any item is already included in another item of the pro-forma invoice, the tenderer shall clearly indicate this in the pro-forma invoice (e.g. by writing "already included under item XY" in the relevant field).

Tenderer: _____

A	B	C	D	E	F
No	**Title**	**The price for the first year for user licences or software licences or concurrent licences (excluding VAT (in EUR))**	**The price for the second year for user licences or software licences or concurrent licences (excluding VAT (in EUR))**	**The price for the third year for user licences or software licences or concurrent licences (excluding VAT (in EUR))**	**The price for implementation/ integration of the software solution including training (excluding VAT (in EUR))**
1.	**Implementation/ integration of the software solution including training (15 employees) in accordance with the requirements of form 17.3 Specifications (one-off cost)**				
2.	**Licences for use (the Contractor shall specify in a separate document the specification of the licences required and included in the price) for approx. 70 named users licences or 10 concurrent licences, for up to 10,000 insights/inquiries in accordance with the requirements of form 17.3 Specifications**				
3.	**Licences for use (the Contractor shall specify in a separate document the specification of the licences required and included in the price) for approx. 70 named users licences or 10 concurrent licences, for between 10,001 and 15,000 insights/inquiries in accordance with the requirements of form 17.3 Specifications**				
4.	**Licences for use (the Contractor shall specify in a separate document the specification of the licences required and included in the price) for approx. 70 named users licences or 10 concurrent licences, for between 15,001 and 20,000 insights/inquiries in accordance with the requirements of form 17.3 Specifications**				

	Title	Unit of measure	Estimated hours for the duration of the Contract	Price per hour (excluding VAT (in EUR))	Total price for the duration of the Contract (price per hour (excluding VAT (in EUR) x estimated hours)
5.	**Additional services during regular working hours***	**hour**	**200**		
6.	**Service implementation under DORA, EBA outsourcing guidelines, and EBA ICT and security guidelines****	**hour**	**10**		
		Answer Yes/No	**Tenderer indicates from which source he obtains data**	**Tenderer must specify from which document in tender (page, paragraph,...) is evident that the tenderer's software solution meets the requirement**	
7.	**The source from which the data are obtained** **Software solution obtains data from Watchlist, World Check or Dow Jones Watchlist** (Tender indicates Yes/No and indicates from which source)	**Yes / No**	**SOURCE:** **☐ Watchlist** **☐ World Check** **☐ Dow Jones Watchlist**		
8.	**Minimum data set** **Software solution provides Information on sanctions of companies or natural persons in the ownership structure of the client (indirect sanctions – for example companies implicated as sanctioned under the OFAC and EU Ukraine/Russia Guidelines and other sanctions lists where the minimum ownership is 10%/25%** (Tender indicates Yes/No and duly specify)	**Yes / No**			
9.	**Advance Sanctions List Search Functionality** **Software solution provides functionality for ad hoc searches and continuous processing based on the**	**Yes / No**			

	International Securities Identification Number (ISIN) through international sanctions lists and other official watchlists—including those published by OFAC (U.S. Department of the Treasury), the United Nations, the United Kingdom, and the European Union, and lists of terrorists organizations and individuals. (Tender indicates Yes/No and duly specify)			
		Answer Yes/No	**Tenderer must indicate accordingly**	**Tenderer must specify in which document (page, paragraph,...) this is demonstrated)**
10.	**API requirements** **Software solution within API requirements provides functionality for the transfer of screening results regarding sanctions and PEP/SOE** **or** **Software solution within API requirements provides functionality for the transfer of all screening results as specified in section 17.3.1 General information** (Tender indicates Yes/No, indicates which functionality is enabled and duly specify)	**Yes / No**	☐ functionality for the transfer of screening results regarding sanctions and PEP/SOE ☐ functionality for the transfer of all screening results as specified in section 17.3.1 General information	
11.	**Process Automation and Client Data Modification Capability** **Tenderer ensures that the service operates primarily through automated processes, requiring user data validation only when necessary (as specified in point H, Section 17.3.1)** **And/or** **Tenderer ensures further modifications of client name changes (as specified in point H, Section 17.3.1)** (Tender indicates Yes/No, indicates which functional service is enabled and duly specify)	**Yes / No**	☐ the service operates primarily through automated processes, requiring user data validation only when necessary (as specified in point H, Section 17.3.1) ☐ further modifications of the client name changes	

			(as specified in point H, Section 17.3.1)	

* Regular working hours shall be 8:00 a.m. to 4:00 p.m. on weekdays (Monday to Friday).
** The hours of additional services and for service implementation under DORA, EBA outsourcing guidelines, and EBA ICT and security guidelines shall be indicative and shall be used as required/used, according to the Contracting Authority's written requests, which shall be performed for the agreed services only upon a written order received from the Contracting Authority confirming the performance of the work and the amount of hours. The estimated value and quantity of hours does not commit the Contracting Authority to the consumption of the total quantity of hours and represents only the estimated maximum value and estimate of the services in question.

The tender price net of VAT shall include all elements, i.e. all costs (labour costs, hardware and software costs, travel costs and all other costs that could arise in relation to the performance of the services in question over the entire period of performance of the subject of the contract), fees and other levies (except for VAT), and any discounts or commissions, additional tax burdens and tax obligations waived so that the Contracting Authority is not liable for any costs connected with the subject of the public contract.

The prices per unit in the tender pro-forma invoice shall be fixed until the completion of performance of the subject of the public contract, unless the contract provides otherwise.

The Contracting Authority shall order additional services as and when the need arises. The Contracting Authority shall not be obliged to order the envisaged estimated amount of additional services or use the envisaged quantity of hours during the period of performance of the contract.

The price per unit applies to an hour of service equal to sixty (60) minutes. The price per unit applicable at the time performance commences shall be charged for services performed (for all hours not interrupted by a period of more than one (1) hour). The hours of service performed shall be rounded to thirty (30) minutes, with up to fourteen (14) minutes in excess of a full hour or half-hour being rounded downwards and fifteen (15) or more minutes being rounded upwards. The tendered prices per unit (hour) constitute the maximum price per unit charged for any additional services.

A form submitted electronically to the e-JN information system shall be considered to be dated and signed by the tenderer’s responsible person. It is therefore binding on the tenderer vis-à-vis the Contracting Authority.

17.5 References[1]

A tenderer shall be required to demonstrate the following in order to have its capacity recognised that in the last three (3) years, before the submission deadline tenders, it has successfully (in terms of quality, professionalism and in accordance with a contract) carried out at least three (3) similar software solution projects set up in the cloud and interfacing with the banking system via VPN, where they have ensured uninterrupted delivery of data and services of AML and restrictive measures to economic operators in the financial sector in the EU (bank, savings bank, insurance company, financial intermediary, fund, etc.).

Tenderer:_____

No	**Contracting Authority that ordered the reference project** (name, address) **and the Contracting Authority's contact details** (full name, email address, telephone number)	**Date of execution** (month, year)	**Brief description of the project** (description of the services to demonstrate the scope of supply, implementation/ integration and maintenance)
1.			
2.			
3.			
4.			

A form submitted electronically to the e-JN information system shall be considered to be dated and signed by the tenderer's responsible person. It is therefore binding on the tenderer vis-à-vis the Contracting Authority.

[1] A tenderer may not simultaneously be a reference client. The Contracting Authority reserves the right to verify the detailed contents and quality of implementation/ integration of the project directly with the reference client, or to request that the tenderer submit to it for inspection any contracts or other documents that unequivocally prove the authenticity of the references.

17.6 Questionnaire to assess reputation and compliance risk

Please provide the following information on your company. A tenderer that has entered all the required information from the questionnaire, answered "Yes" to all questions in Sections 2 to 7 of the questionnaire (except for point 5.3 d) or provided appropriate evidence of control of the risks of a conflict of interest in Section 4 and submitted and signed the statement contained in Section 8 of the questionnaire shall be regarded as suitable.

TENDERER'S DETAILS	
Company name	
Company's registered office (country, street and house number, settlement, municipality, postcode and town)	
Activity name and code, NACE code	
Registration number and tax number	
Are you a micro, small or medium-sized enterprise?[1]	
Contact details (email, telephone)	
Place and date of completion	
Full name of responsible person	
Handwritten signature of responsible person	
By appending a handwritten signature, the responsible person accepts responsibility for the veracity of the responses. SID Bank shall be entitled, prior to signing the contract on the outsourcing of services and for the entire duration of that contract, to verify the veracity and completeness of the responses given. In the event of false or misleading responses, SID Bank shall be entitled to terminate the contract and to demand the reimbursement of any payments made and any damage incurred.	

1. DECLARATION OF PARTICIPATION OF NATURAL AND LEGAL PERSONS IN TENDERER'S OWNERSHIP

Any ownership links should be mentioned. (Alternative: submit a declaration of ownership in accordance with the ZIntPK).

Tenderer's ownership structure

1.1 Information on the participation of natural persons in the tenderer's ownership structure:

Complete the table for every natural person with a participating interest of more than 5% in the tenderer's ownership:

Full name:	
Residence, permanent, unless the person has temporary residence in	

[1]Indicate whether you are a micro, small or medium-sized enterprise (according to the criteria set out in Commission Recommendation 2003/361/EC)

Slovenia (country, street and house number, settlement, municipality, postcode and town):	
Participating interest:	

1.2 Information on the participation of legal persons in the tenderer's ownership structure:

Complete the table for every legal person with a participating interest of more than 5% in the tenderer's ownership:

Name of the legal person:	
Registered office of the legal person:	
Participating interest in the tenderer:	
Registration number of the legal person and tax number of other legal persons not entered in the business register:	

1.3 Information on companies classed as related parties of the tenderer under the law governing companies:

Name of the legal person:	
Registered office of the legal person:	
Participating interest in the tenderer:	
Registration number of the legal person and tax number of other legal persons not entered in the business register:	
is in a mutual relationship with the tenderer in accordance with Article 527 of the ZGD-1 as follows:	

2. REFERENCES AND TECHNICAL KNOWLEDGE IN THE FIELD OF PERFORMANCE OF THE TENDERED SERVICES

State the references (if the public procurement documentation already requires the submission of proof of references, there is no need to complete Section 2 of the questionnaire).

a) Do you satisfy the requirements regarding key references in the field of the tendered services?

Yes. No.

Provide supporting evidence:

_____

_____

b) Do the key persons who will be responsible for providing the tendered services satisfy the requirements regarding references and technical knowledge?

Provide supporting evidence (list the full names, references and technical knowledge of the key persons who will be providing the services):

_____

_____

3. RESOURCES AND LICENCES FOR PERFORMANCE OF THE TENDERED SERVICES:

a) Do you have adequate capacities and resources available (human, IT, financial, etc.) for the reliable, timely and high-quality provision of the tendered service?

Yes. No.

b) Do you have the required regulatory licences or registrations for the reliable and professional provision of the tendered service? Submit copies of the supporting documents.

Yes (or "We do not need them"). No.

4. CONFLICT OF INTEREST

Do you confirm that there exists, on the part of your company, your responsible persons (members of the management and supervisory boards), and/or the key employees involved in the provision of the tendered service, no risk of a conflict of interest that cannot be adequately managed, i.e. in terms of the following:

a) Economic interests (e.g. loans to the company approved by SID Bank);

Yes. No.

b) Personal or professional relationships with the management body of SID Bank;

Yes. No.

c) Personal or professional relationships with SID Bank employees who are part of the bank's team charged with selecting the tenderer (e.g. family relationships);

Yes. No.

d) A key employee involved in the provision of the tendered service has been employed at SID Bank in the last five years;

Yes. No.

Provide supporting evidence. If any of the above-mentioned risks exist, describe how you will manage it:

_____

5. REGULATORY COMPLIANCE[2]

5.1 PERSONAL DATA PROTECTION AND TRADE SECRECY POLICY[3]

a) Does your company have a by-law/policy addressing personal data protection and trade secrecy?

Yes. No.

[2] Answer the questions with "Yes", "No", "We do not detect"/ "We do not implement" or "Annually", "Half-yearly", "When a change is noted".
[3] Circle as appropriate.

5.2 FRAUD RISK MANAGEMENT

a) Has your company adopted a zero tolerance policy (or do you have zero tolerance) with regard to fraud (including corruption, money laundering and terrorist financing)?

Yes. No.

b) Does your company take steps to uncover and prevent fraud?

Yes. No.

c) Do you systematically review and analyse identified and documented events that constitute or that could constitute (be suspected of being) fraud and, on that basis, adopt and carry out corrective measures?

Yes. No.

5.3 CODE OF ETHICS AND GOOD PRACTICE STANDARDS

a) Does your company have a code of ethics or other appropriate code of acceptable conduct?

Yes. No.

b) Do you systematically review and analyse identified and documented events that could constitute a violation of the code of ethics?

Yes. No.

c) Do you adopt and carry out corrective measures after addressing identified or suspected violations of the code of ethics?

Yes. No.

d) Has any violation of the code of ethics or acceptable conduct in the last five years had more significant negative effects for your company (e.g. extensive negative media coverage, termination of business relationships/contracts, cancellation of orders by your more significant business partners, revocation of licences)?

Yes. No.

5.4 RESPECT FOR HUMAN RIGHTS IN BUSINESS OPERATIONS

a) Do you consistently comply with the following in your business operations:

- labour legislation and workers' rights?

  Yes. No.

- prohibition of child labour?

  Yes. No.

- prohibition of corruption?

  Yes. No.

- environmental protection regulations?

  Yes. No.

6. RELATIONS WITH REGULATORS (SUPERVISORY INSTITUTIONS)

a) Do you confirm that you have not had a licence revoked by a regulator in the last five years?

Yes. No.

7. JUDICIAL PROCEEDINGS AND DISPUTES

a) Do you confirm that no legal criminal, labour law or damages proceedings are ongoing or have been concluded by final legal judgment in the last five years against your or any of your responsible persons (members of the management and supervisory boards) and deriving from the operations of the company or the professional operations of your responsible persons (such proceedings may involve a dispute regarding compensation of a greater value, i.e. payment of damages, that could jeopardise the operations of your company), or that you are not undergoing criminal proceedings on account of a suspicion of having committed an offence involving human rights and freedoms, employment and social security, property, the economy, legal transactions, the environment, space and natural resources, or that you are undergoing proceedings before a court in relation to labour law legislation as a result of a violation of workers' rights?

Yes. No.

8. DECLARATION OF TENDERER

Declarations and guarantees

_____

(company name and registered office)

1. We confirm that

a) the data and information provided in the questionnaire are true, accurate and non-misleading;

b) the deliberate giving of false data that puts SID banka, d.d., Ljubljana into a situation of grave error constitutes a serious breach of the contract and may lead to extraordinary termination of the contract.

2. We hereby declare that

a) we have fully answered every question in this questionnaire and disclosed all information that may be deemed relevant for the purpose of completing this questionnaire;
b) we undertake to inform SID banka d.d., Ljubljana without delay of any significant changes in connection with the answers, statements and other content that we have provided in this questionnaire and regarding other matters of which we become aware following the completion of this declaration and that are connected to performance of the contract on the management of an external service;
c) we shall provide all services under contract with SID Bank with due professional diligence, and with due regard to good practice and the standards of the profession, and shall observe the same values and ethical standards as SID banka, d.d., Ljubljana.

3. We hereby give our consent to and permit

SID banka, d.d., Ljubljana to carry out reasonable enquiries on the company and collect and use information from third parties for the requirements of due diligence, all in connection with the contract and in accordance with the applicable regulations.

A form submitted electronically to the e-JN information system shall be considered to be dated and signed by the tenderer's responsible person. It is therefore binding on the tenderer vis-à-vis the Contracting Authority.

17.7 Questionnaire on methodology for evaluating the state of information security at the provider

ICT: Questionnaire on methodology for evaluating information security		To be completed by the Tenderer	Maximum point score for affirmative answer
			126
	Tenderer's business name:		
	Approximate headcount:		
	Place and date of completion:		
	Name of responsible person:		
	Signature of responsible person:		
	1. Information security policy		
1.1	Does a documented information security policy exist at your organisation?	Yes No	5
1.2	Were commercial requirements and the relevant legislation and regulations in your organisation's line of business taken into account when the information security policy was being drafted, and were they written into it?	Yes No	2
1.3	Is the documented information security policy approved by the director of the undertaking or by a member of the most senior management body?	Yes No	2
1.4	Is the documented information security policy regularly reviewed, and updated as necessary?	Yes No	2
1.5	Are all employees made aware of the information security policy and any changes thereto, and is it at their disposal for the entire duration of their employment?	Yes No	3
1.6	Has the security policy been reviewed by independent experts?	Yes No	3
	2. Analysis and management of information risk and other risks		
2.1	Has your organisation conducted and documented risk analysis?	Yes No	4
2.2	What is the scope of the risk analysis?	across the organisation (2 points) / only in certain parts of the	maximum of 2

		organisation (1 point) / risk analysis is not conducted (0 points)	
2.3	Is the risk analysis conducted and updated at least once a year?	Yes No	2
2.4	Are the director of the business or members of the most senior management body made aware of the results of the risk analysis?	Yes No	2
	3. Management of IT resources		
3.1	Does your organisation have a documented IT resource management policy?	Yes No	4
3.2	Have you made an inventory of all information resources that are part your organisation's information system?	Yes No	2
3.3	Do all information resources have designated owners/custodians, and are they aware of their responsibilities?	Yes No	2
3.4	Has your organisation set out a precise procedure to ensure that employees and external contractors return all information technology resources to the organisation when ceasing their work?	Yes No	2
3.5	Has your organisation set out a policy for the use and management of external data media?	Yes No	2
	4. Existence of incident management system		
4.1	Does your organisation systematically identify and document events that have an impact on the security of your operations and your performance in general?	Yes No	4
4.2	Do you classify the identified events in terms of the criticality of their impact on your operations?	Yes No	2
4.3	Do you systematically review and analyse the identified and documented events?	Yes No	2
4.4	Do you take and implement appropriate decisions on the basis of discussion of the identified and documented events?	Yes No	2
	5. Existence of business continuity plans and their contents		
5.1	Do you have documented business continuity plans at your organisation?	Yes No	3
5.2	Which business lines are covered by a business continuity plan at your organisation?	all business lines (2 points)	maximum of 2

		/ key business lines that ensure the functioning of the business (1 point) / we do not have business continuity plans (0 points)	
5.3	Have you defined and documented the roles and responsibilities for implementing the business continuity plan (this does not refer to positions and functions relating to ordinary business processes)?	Yes No	1
5.4	Backup location: (multiple responses possible)		maximum of 2
	it is equipped with all the requisite IT infrastructure and other resources proceeding from the relevant analysis	Yes No	1
	it has equipped workstations for staff and equipped offices for management	Yes No	1
5.5	Are the business continuity plans regularly tested, the testing documented, and the plans updated on this basis?	Yes No	1
	6. Existence of information security awareness programme		
6.1	Does your organisation provide an awareness and training programme for information security and business continuity?	Yes No	3
6.2	Does at least one person in your organisation regularly attend outside training in information security?	Yes No	1
6.3	Do you provide information security awareness training for all employees working at your organisation?	Yes No	2
6.4	Do you ever use an external contractor that provides an awareness and training programme for information security or business continuity?	Yes No	1
6.5	Have you organised a documented analysis and debriefing of an extraordinary event that had a major impact on your operations to ensure that it would not occur again?	Yes No	2
6.6	Do you put security controls in place when recruiting new people?	Yes No	2
	7. IT-related security measures introduced		
7.1	Has your organisation systematically introduced IT-related information security measures in various areas based on risk analysis of your business environment?	Yes No	2

7.2	Have you introduced a documented change management system in the area of information technology?	Yes No	2
7.3	Your documentation of information systems contains (multiple responses possible):		maximum of 3
	an information system development plan	Yes No	1
	a system capacity development plan	Yes No	1
	procedures for approving systems into production	Yes No	1
7.4	Have you put in place documented procedures to prevent information leaks?	Yes No	2
7.5	Do you conduct vulnerability tests in conjunction with independent external providers to identify security deficiencies and to take appropriate technical security measures?	Yes No	2
7.6	Do you follow up the implementation of security measures?	internal and external reviews are conducted for all measures (3 points) / internal reviews only are conducted for all measures (2 points) / reviews are conducted solely for important measures (1 point) / we do not conduct reviews (0 points)	maximum of 3
	8. Fundamental security measures		
8.1	Which areas of security have been introduced at your organisation? (multiple responses possible)		maximum of 18
	physical security and access control	Yes No	1
	alarm system with connection to security service	Yes No	1
	video surveillance	Yes No	1

	fire protection	Yes No	1
	physical securing of paper documentation	Yes No	1
	protection against electricity outage	Yes No	1
	firewall protection from external networks	Yes No	1
	antivirus protection	Yes No	1
	restriction on the entry and use of mobile devices for work purposes	Yes No	1
	monitoring of remote working and network access	Yes No	1
	classification of information in terms of security level	Yes No	1
	application of clean desk and clean screen principles	Yes No	1
	logic control of access and IT-related protection	Yes No	1
	use of encryption	Yes No	1
	segregated development, testing and production environments	Yes No	1
	audit trails for key information resources	Yes No	1
	security backup	Yes No	1
	compliance with legislation (particularly law governing personal data protection and law governing electronic transactions and electronic signatures)	Yes No	1
8.2	During the implementation of security processes, records and evidence of their implementation are generated. Can it be proven in this way that the measures have genuinely been implemented?	yes, for all processes and measures (2 points) / in part (1 point) / no (0 points)	maximum of 2
8.3	Do you regularly monitor events on systems and other events that could constitute incidents?	yes, systems are monitored continuously (24/7) (3 points) / yes, systems are monitored during working hours (2 points)	maximum of 3

		/ events are not monitored regularly (0 points)	
8.4	Does the organisation earmark specific funds for information security?	Yes No	3
	9. Process arrangements and discipline		
9.1	Do you have documented business processes at your organisation?	Yes No	2
9.2	Do you have valid process management system certification at your organisation? (multiple responses possible)		maximum of 7
	yes, under the ISO 9001 standard	Yes No	3
	yes, under the BS 25999 standard	Yes No	3
	yes, under an associated or other process management standard	Yes No	1
9.3	Do you have it documented that employees are briefed on the procedures and level of information security at your organisation?	Yes No	3
9.4	Are you a regular payer, and do you settle your liabilities to employees, external contractors and suppliers with no arrears?	Yes No	1
9.5	Do all employees, contractors and Subcontractors sign a non-disclosure Agreement when commencing their work?	Yes No	2
9.6	Are all projects conducted at your organisation subject at a certain point to a security assessment or to approval by the information security officer?	Yes No	2

A form submitted electronically to the e-JN information system is considered to be dated and signed by the Tenderer's responsible person. It is therefore binding on the Tenderer in relation to the contracting authority.

17.8 Questionnaire regarding cloud data processing controls

This questionnaire is designed for the purpose of evaluating cloud data processing controls carried out by external contractors as part of the provision of cloud computing services to the contracting entity (the bank). The checkpoints that enable the bank to understand the method of controlling cloud services and the associated risks are set out below.

The impact of individual checkpoints on the bank depends on the type of cloud service that the external contractor provides to the bank. A tenderer that is only a distributor of licences for the use of cloud services is not required to complete this questionnaire.

The bank will endeavour, to a reasonably practicable extent and where relevant, to take into account several of the assurances or proof of operation of the internal controls provided by the external contractor:

- a copy of proof that its information security management system has been certified under the ISO/IEC 27017 or ISO/IEC 27018 standard, which may not be more than three years old, and a copy of the assessment report from the certification organisation, which may not be more than one year old;
- any audit reports from third parties or an internal audit report on information security or personal data protection in the cloud.

References to the coverage of individual checkpoints by subcontractors (e.g. Microsoft, Amazon Web Services) are permitted if a subcontractor rather than the tenderer is responsible for an individual checkpoint in full. In these cases, the tenderer should describe the model of cooperation with the subcontractor ('Infrastructure-as-a-service', 'Platform-as-a-service', 'Software-as-a-service').

TENDERER'S DETAILS:

Company name	
Place and date of completion	
Full name of responsible person	
Handwritten signature of responsible person	

DESCRIPTION OF SERVICE or of the MODEL OF SERVICES in the cloud that the external contractor shall provide to the contracting entity or on which the contracting entity will be directly or indirectly dependent in its cooperation with the contractor:

Item no	Checkpoint (name)	Details of how/whether the checkpoint is fulfilled	Checkpoint (YES/NO)
Contractual processing of (personal) data			
1.	The written contract with the cloud computing contractor also includes a specific contract on procedures and measures for protecting (personal) data.		
2.	A definition is available, or may be made available, in the contract of which (personal) data is processed by the tenderer and what the tenderer's authorisations are.		
3.	The contracting entity is made aware at every step of every subcontractor (e.g. Microsoft, Amazon Web Services) that processes (personal) data on behalf and for the account of the tenderer, and which processing it performs (principle of transparency).		
4.	The external contractor agrees to grant the contracting entity a reasonable period of time, prior to use of the services of a new subcontractor, in which the contracting entity is able to decide whether to withdraw from the contract if it does not agree with the use of the new subcontractor's services.		
5.	The transfer of (personal) data to a subcontractor is not permitted without the contracting entity's consent.		
6.	After expiry of the contract or at the contracting entity's request, the provider of cloud computing services destroys all (personal) data, including any copies, or return all data to the contracting entity.		

Item no	Checkpoint (name)	Details of how/whether the checkpoint is fulfilled	Checkpoint (YES/NO)
Information security (personal data protection) – compliance and audit			
7.	The physical location of (personal) data is known at all stages of (personal) data processing.		
8.	Where cloud services are leased, the tenderer provides strong authentication mechanisms (e.g. multi-factor authentication) and access controls for the purpose of preventing unauthorised access to the bank's data and back-office resources in the cloud.		
9.	Where cloud services are leased, the tenderer ensures an audit trail for all data processing that shows who processed the data, when it was processed and which data was processed.		
10.	The tenderer provides the option of transferring system logs to the bank's security information and event management (SIEM) system.		
11.	The tenderer grants the contracting entity the right to audit its information system, or the tenderer regularly conducts independent external audits of its entire information system.		
12.	The tenderer provides customers with the results of information system audits and security checks, including penetration testing, in accordance with legislation and security standards.		
13.	The tenderer encrypts data during storage, during transfer or within the cloud when this data passes through unsecured communication networks. The tenderer produces back-up copies of data and has tried and tested procedures in place for restoring them.		

Item no	Checkpoint (name)	Details of how/whether the checkpoint is fulfilled	Checkpoint (YES/NO)
14.	The tenderer uses appropriate solutions for managing encryption keys that limit the risk of unauthorised access to encryption keys.		
15.	The tenderer has in place secure mechanisms for integrating the bank's information system with cloud services.		
16.	The tenderer notifies the contracting entity of actual incidents and suspected incidents and of the methods of detecting and handling incidents, including the resources at the tenderer that are planned and described in the incident response plan.		
17.	The contracting entity is apprised of the approach that the tenderer deploys for sharing resources and of the technical and other measures by which the tenderer addresses the security aspects of multi-tenancy.		
18.	The tenderer secures its multi-tenant infrastructure and apprises the contracting entity of the method by which it is secured.		
19.	The tenderer ensures separation of the operation of the internet, application logic, the operating system, the network, the database management system (DBMS) and storage, and segregation of the process environments (e.g. test, development, production).		
20.	The tenderer ensures that rights to access data and/or cloud services can be managed by the contracting entity.		
21.	Does the tenderer have a business continuity plan? Is this plan tested regularly, i.e. at least once a year?		
Rights of the individual			

Item no	Checkpoint (name)	Details of how/whether the checkpoint is fulfilled	Checkpoint (YES/NO)
22.	The tenderer ensures that procedures ar infrastructure enable easy access t personal data, by the prescribed statuto deadlines, in the event that an individu asks to inspect the personal data pertainir to them.		
Transfers of personal data to third countries			
23.	The tenderer provides the contracting entity with information on the third countries to which it will transfer (personal) data.		

Place and date:

Signature of statutory representative:

17.9 Questionnaire for Personal Data Protection

Tenderer details (Name, Adress, Date of completion of the questionnaire and signature):

_____

The questionnaire is designed to assess the adequacy of personal data controls implemented by external contractors who process personal data on behalf of the bank. This includes, for example, processing activities related to customer satisfaction surveys, employee surveys, etc.

In accordance with the bank's internal regulations and applicable personal data protection legislation (EU Regulation 2016/679 – GDPR), we have prepared a questionnaire to assess the adequacy of personal data processing in your organization.

Your responses will help the bank to assess:

- whether the personal data for which the bank is responsible as a controller will be adequately processed and protected during the course of cooperation with your organization,
- whether improvements might be needed to ensure compliance with data protection requirements.

Please complete the questionnaire by answering the questions in order. The questionnaire must be duly completed, dated, and signed. Completed questionnaire will form part of the contractual documentation governing the relationship with the bank. Failure to complete the questionnaire may result in the rejection of your offer.

Types of questions :

- Multiple-choice questions: Please answer them by marking the appropriate answers. If more than one answer is allowed, this will be clearly indicated, and in such cases, mark all appropriate answers. For other questions select the single most appropriate one.
- Descriptive questions: . Provide brief and concise answers in your own words.

IMPORTANT! Where a descriptive answer is expected, please list only the essential points that the question asks for.

1. Contact details of Data Protection Officer (DPO). If you do not have a DPO who is the person responsible for data protection of personal data processed by your organisation?

   _____

_

2. Number of persons authorized to access or otherwise process personal data from collections related to external processing for the bank (hereinafter: collections):

   _____

3. Please list in which countries do you process personal data on bank's behalf:_____

4. Does (or would) the processing of personal data under the data processing agreement also involve the transfer of personal data to third countries (i.e., outside the European Community) or international organizations?

   ☐ YES – specify the third countries and the processing activities transferred to them:

   _____

   ☐ NO

5. If you answered "YES" in point 3, describe the intended protective measures for the protection of personal data in these third countries:

_____

_____

_____

6. Do you delegate or intend to delegate the processing of personal data from the collections to other processors or subcontractors (hereinafter: subprocessors)?
☐ YES – If yes, please provide the following details for each subprocessor: name and address, processing operation performed (e.g. storage, hosting, analytics) and types of personal data processed_____
_____

☐ NO

7. If you circled "YES" in point 5 – do you have appropriate data protection and security agreements with the subprocessor(s)?
☐ YES – specify the date(s) of conclusion and the date(s) of expiration or the duration of the agreements:

_____

☐ NO

8. If you answered "YES" in point 5, do you require and ensure that your subcontractors/subprocessors meet the same security requirements as those required by the bank for the processing of the bank's data and information? These requirements must be formalized with the subcontractor as part of the contract or annexes to the existing contract.
☐ YES

☐ NO

9. Specify the specific measures you ensure for the protection and security of personal data from the collections, including measures at the sub-processor, if applicable, in accordance with the applicable data protection legislation and the data processing agreement:

_____

_____

_____

Organizational, technical, and logical-technical procedures and measures for the protection of personal data that you ensure to prevent accidental or intentional unauthorized destruction, alteration, or loss of data and unauthorized processing are:

_____

_____

_____

10. Personal data on paper documents are stored in fireproof cabinets or appropriate premises:
☐ YES

☐ NO

☐ Not relevant

11. Personal data are stored on electronic data carriers.

☐ YES

☐ NO

☐ Not relevant

If the answer is YES, specify which carriers are used, where these carriers are located, who uses them, and how they are protected:_____

12. Access control is implemented for access to business premises (all accesses are recorded).
☐ YES

☐ NO

☐ Not relevant

13. Unauthorized viewing or other access to personal data by maintenance personnel, customers, and other visitors to the premises is prevented (accidentally or intentionally).

☐ YES

☐ NO

☐ Not relevant

If the answer is YES, describe how viewing/access is prevented:

_____

_____

_____

14. Access to the premises outside working hours is granted to employees based on a special permit/approval or otherwise.
☐ YES

☐ NO

☐ Not relevant

Describe:

_____

_____

_____

15. Is there control over printing, copying, distributing, and destroying personal data carriers?
☐ YES

☐ NO

☐ Not relevant

Describe:

_____

_____

_____

16. Is access to system software and computers controlled through password based authentication mechanisms?

☐ YES

☐ NO

☐ Not relevant

17. Is control over assigned usernames implemented based on the principle of one username per authorized user?

☐ YES

☐ NO

☐ Not relevant

18. A formalized procedure is in place to ensure that all employees and contractors are informed about personal data protection measures and procedures and their responsibilities.

☐ YES

☐ NO

☐ Not relevant

19. Employees and contractors are required to sign a statement affirming their ongoing obligation to protect personal data, including after the termination of the contractual relationship with the processor.

☐ YES

☐ NO

☐ Not relevant

20. Access to personal data is controlled through specific authorizations, ensuring that it is clearly defined which employees are permitted to access which personal data and for what purpose.

☐ YES

☐ NO

☐ Not relevant

21. Upon termination of employment or contractual relationship, all access to personal data and any copies of data carriers are revoked for employees and contractors (e.g., students).

☐ YES

☐ NO

☐ Not relevant

Comments, explanations, other:

_____

_____

_____

22. What measures are in place in order to prevent unauthorized access to personal data during their transfer, including transfer via telecommunications means and networks: (please describe)

_____

_____

_____

23. Are personal data are transferred via telecommunications means and networks.

☐ YES

☐ NO

☐ Not relevant

24. Are personal data are transferred via telecommunications means and networks in encrypted form or otherwise.

☐ YES

☐ NO

☐ Not relevant

Specify how: e.g., standard/licensed encryption software is used, an internally developed application for this purpose...

_____

_____

_____

25. Are personal data are transferred to third parties.

☐ YES

☐ NO

☐ Not relevant

If YES, please specify which data, how, to whom, and under what conditions they are transferred:

_____

_____

_____

26. Comments, Explanations, Other:

(i) Are you ensuring pseudonymization, anonymization, and encryption of personal data (specify):

_____

_____

_____

(ii) Are you ensuring effective destruction or deletion of personal data after the purpose for which they were collected or after the termination of the main contract (describe):

_____

_____

_____

27. Personal data are deleted from the processor's databases after the processing purpose is fulfilled or upon termination of the main business cooperation contract (but no later than the expiration of the prescribed retention period)..

☐ YES

☐ NO

☐ Not relevant

28. The processor's access to databases is revoked by uninstalling the software, ensuring that the processor returns or destroys any copies, transcripts, etc.

☐ YES

☐ NO

☐ Not relevant

29. Audit trail (please mark and describe):

(i) How is the audit trail of personal data processing ensured – please specify how it enables subsequent determination of when individual data were received, stored, entered into the personal data collection, used, or otherwise processed (including deletion) and who did it:

_____

_____

_____

(ii) Is the audit trail maintained automatically by the software or application used for data processing? If so, does this ensure that no parallel copies of the same data collections, or parts thereof, exist). If not please describe current set up.

☐ YES

☐ NO

☐ Not relevant

Describe:

- The audit trail is visible / maintained...

_____

_____

_____

Describe the method of maintaining the audit trail of personal data processing:

- Comments, explanations, other:

_____

_____

_____

30. Are you ensuring continuous confidentiality, integrity, availability, and resilience of systems and services for processing and the ability to timely restore the availability and access to

personal data in the event of a physical or technical incident (business continuity), including regular testing, assessment, and evaluation of the effectiveness of technical and organizational measures to ensure processing security (mark and describe):
☐ NOT IMPLEMENTED
☐ IMPLEMENTED

Please specify the measures you implement:

_____

_____

_____

31. Do you have an incident response plan in place for security incidents and unauthorized disclosures of personal data, which is regularly reviewed (mark and describe)?
☐ YES

☐ NO

Please specify the measures you implement:

_____

_____

_____

32. Is there a record of the transfer of the bank's personal data to third parties, in accordance with legal requirements? The record must include: description of the request, legal basis, name of the third party, name of the processor, date and time of processing, purpose of processing, and scope of transferred data (mark and describe).
☐ YES

☐NO

Please specify the measures you implement:

_____

_____

_____

33. Is there appropriate control over personal data processing and detection of potential violations (please describe)?

_____

_____

_____

34. Was any data protection violation identified in the past two years?
☐ YES

☐ NO

If yes, provide details:

_____

_____

_____

35. Do you comply with the requirements of the EU General Data Protection Regulation (GDPR)?

☐ YES

☐ NO

If not, provide details:

_____

_____

_____

36. Do you have a data protection policy in place??
☐ YES

If the answer is YES, describe when was the last time it was reviewed :_____

☐ NO

If NOT, provide details:

_____

_____

_____

37. Do employees in your organisation receive training on data protection and other relevant law?
☐ YES

☐ NO

If yes, please describe briefly the nature of training given:

_____

_____

_____

38. When was the last employee training on data protection conducted?

_____

Place and date:

Signature of the employee:

17.10 Sample contract

The Tenderer confirms the contents of the Annex 17.10 Sample Contract by completing and certifying the form "17.1 Basic information on the tender and Tenderer"

Prior to signing the Contract with the selected Tenderer, the Contracting Authority will enter the data indicated by the Tenderer in its tender in the Sample Contract.

SID – Slovenska izvozna in razvojna banka, d.d., Ljubljana, Ulica Josipine Turnograjske 6, 1000 Ljubljana, company registration no: 5665493000; VAT registration no: SI82155135), represented by Borut Jamnik, Chairman of the Management Board, and Stanka Šarc Majdič, Member of the Management Board ("SID bank" or the "Contracting Authority"),

and

_____ (registration no: _____; VAT registration no: _____; bank account no: _____ with _____), represented by _____ (the "Contractor"),

hereby enter into the following

CONTRACT NO JN-0581/2025

" Software services/solutions in the field of AML and restrictive measures "

I. PREAMBLE

Article 1

The parties agree and acknowledge that:

- pursuant to the Public Procurement Act (Official Gazette of the Republic of Slovenia, No 91/15, with changes: hereinafter referred to as »ZJN-3«), SID bank has conducted a procedure to award the public contract "Software services/solutions in the field of AML and restrictive measures" under a small value order procedure award procedure no _____ ("public contract");
- in accordance with the public contract award decision of _____, SID bank shall conclude Contract no JN-0581/2025 "Software services/solutions in the field of AML and restrictive measures " (hereinafter: "Contract") with the Contractor;
- the Contract defines all the essential requirements regarding the software services/solutions in the field of AML and restrictive measures;
- the Contract shall prevail over any provisions contained in any correspondence, request for quotation, the Contractor's preliminary quotation, tender, purchase order or other document and/or of the Contractor and/or the Contracting Authority and any oral statement or representation made by the Contractor and/or the Contracting Authority and the Contractor's general terms and conditions;
- the terms used in this Contract shall have the same meaning as ascribed to them in the procurement documentation and the Contractor's tender documentation, unless this Contract provides otherwise.

II. SUBJECT OF THE CONTRACT

Article 2

The Contractor undertakes to establish implementation/ integration of software services/solutions in the field of AML and restrictive measures of the services to support the compliance function in accordance with the technical an functional specification of the applications as in 17.3 Specification and the maintenance of the applications for a period of three (3) years from the signing of the record of handover for the supply and implementation/ integration of the software solution in the field of AML and restrictive measures. The Contracting Authority shall pay the agreed price to the Contractor for the above mentioned services of this Contract.

The subject and services of the Contract is specified in detail under Specification (Annex 17.3) in the Documentation on the awarding of the public contract.

Article 3

In the event that the content of the above-mentioned documents contradicts itself and if the will of the contracting parties is not clearly expressed, the provisions of the Contract shall apply to the interpretation of the will of the contracting parties first, and then the documents in the order that follows in the preceding paragraph.

The contracting parties agree that in case of doubt or ambiguity, all contractual provisions shall be understood and executed in such a way that none of the Contract provisions limits the Contracting Authority's ability to control ICT services and that they are not in conflict with the DORA regulation (Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 - https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng). The term ICT or ICT services mentioned in the Contract refers to one or more information and communication technologies or services and is used in the Contract to define software solution in the field of AML and restrictive measures.

III. METHOD OF PERFORMANCE AND DEADLINES

Article 4

The Contractor shall provide the maintenance services included in the price for licenses in accordance with the requirements specified in the Specifications form (Annex 17.3) and by the deadlines imposed by the Contracting Authority. The Contractor shall provide any additional services by the deadline set by the Contracting Authority in the invitation, unless the Contractor and the Contracting Authority agree otherwise.

Article 5

The Contractor undertakes to perform all Contractual functions and ICT services, outsourced or Subcontracted, exclusively in the territory of _____. It also commits to processing and storing data exclusively in the territory of _____.

In the event that the Contractor wishes to change the location of the provision of services and/or data processing, they must notify the Contracting Authority in writing at least thirty (30) days before the planned change. The Contractor must ensure compliance with all relevant legal requirements. The change of location is only allowed with the explicit prior written consent of the Contracting Authority.

Article 6

The Contractor is obliged to strictly follow the deadlines specified in the Contract or coordinated with the Contracting Authority in the manner specified by the Contract. The Contractor may exceed the agreed deadlines only if the Contracting Authority does not adhere to the accepted obligations regarding the timely communication of data, the provision of operating systems and conditions for the integration of the software solution in question on the Contracting Authority 's information system, payment terms and deadlines, determined by Contract or due to force majeure.

If the Contractor is unable to fulfil the agreed obligations on time, he must immediately inform the Contracting Authority in writing of the reasons why there will be or has been a delay, and explain in writing the time frame within which, if possible, he will fulfil the contractual obligations.

Extension of a specified or agreed term is possible only before its expiration. The Contracting Authority decides on the extension of the Contract term based on his own assessment of the justification of the reason for the delay. If the extension of the deadline does not make sense for the Contracting Authority in relation to the subject of the Contract, the Contracting Authority is entitled to withdraw from the Contract.

Article 7

The Contractor undertakes to carry out the work under this Contract (especially with regard to safety, reliability and orderliness in the implementation of maintenance activities) with the care of a good expert.

Article 8

The Contractor will provide services for the Contracting Authority at the Contracting Authority's premises or remotely. In case of implementation remote service, the services are performed via secure remote access, in accordance with the client's security requirements and protocols. The subscriber acquires the right to control remote performance session recording service via VPN to ensure an audit trail and information security.

Article 9

The services performed shall comply with the Contracting Authority's order. If the Contracting Authority determines in its review of the services performed and the testing of the services that the quality of those services does not meet its requirements, it shall notify the Contractor and the Contractor shall remedy such deficiencies at its own expense after receiving the Contracting Authority's request (proposal for quality improvement, manner of implementation, corrective measures, etc.). In such an event, the Contracting Authority may refuse to accept the services. In the case of minor deficiencies, the Contracting Authority may accept the services and may either withhold payment until the services have been performed properly in their entirety, or reduce the payment to reflect the value of the unperformed or improperly performed services.

If the Contractor fails to perform the services properly, in a timely manner and to the required standard of quality, and if any of the Contractor's obligations are breached, the Contracting Authority shall be entitled to withdraw from the Contract. The Contractor shall ensure full compliance with all deadlines and the performance of all other contractual obligations it has assumed.

In all cases, the Contracting Authority shall be entitled to claim damages in accordance with the general rules of liability for damages.

Article 10

A record of handover shall be drawn up for the implementation/ integration of the software solution and for the performance of a service. In that record, the parties shall record any identified deficiencies and set deadlines for rectifying them. The Contractor shall rectify any identified deficiencies at its own expense by the deadlines set by the Contracting Authority in the handover record.

The handover record shall specify:

- the obligations assumed under this Contract and the specifications;
- the obligations that have been performed and referred to in the preceding indent;
- any defects identified in connection to the performance of the obligations, any unperformed obligations, and the deadlines for the rectification of defects and the performance of unperformed obligations;
- whether the obligations assumed under this Contract have been performed in a timely manner, in accordance with the specifications, to the required standard of quality and in accordance with the rules of the profession.

Article 11

The Contracting Authority shall order additional services (education/training not included in the Contract without the Contracting Authority incurring additional costs, consulting, other services) as and when the need arises.

The Contracting Authority shall order additional services by electronic means via the communication channels laid down in Article 14 of this Contract. The Contracting Authority shall draft a request in which it specifies the subject of the request and the specifications for the upgrade, the manner of collaboration, the implementation deadline and the deadline for the submission of the offer.

The Contractor shall be solely responsible for continuously monitoring the Contracting Authority's request submission and error reporting application for received orders.

Article 12

The Contractor shall deliver the offer for additional services by the deadline for its submission as specified in the request, in writing using the Contracting Authority's request submission and error reporting application.

After expiry of the deadline for the submission of offers for additional services, which is normally no longer than seven (7) business days, the Contracting Authority shall verify whether the offer is acceptable in terms of content and price.

If the offer is acceptable, the Contracting Authority shall accept the Contractor's offer by means of a written confirmation of the order, which shall serve as the basis for the performance of the additional

services. If the offer is not acceptable, the Contracting Authority shall notify the Contractor of the identified deficiencies or errors, and request it to submit a new offer for the same order.

The Contractor shall perform any additional orders by the deadline set by the Contracting Authority in the invitation to submit an offer, unless the Contractor and the Contracting Authority agree otherwise.

Article 13

In determining the price for individual orders, the Contractor shall determine the number of hours required to complete the order and the price per hour. The Contractor shall use an hourly rate for the price of additional services as referred to in Article 19 of the Contract. The Contractor may also offer a new lower price per hour. If the price per hour exceeds the price per unit offered in the tender pro-forma invoice, the offer will be rejected.

The Contractor shall not be entitled to request from the Contracting Authority an increase of the price for an individual order due to wrong estimation of the time required to complete the work.

The Contractor, acting with due professional diligence, shall notify the Contracting Authority of any objective absolute inability to complete an individual order (e.g. conflict of interest, impaired objectivity and independence).

Article 14

The Contractor shall ensure that services are maintained at the highest level of security and operational resilience, in accordance with applicable legislation, professional standards, and best practices in the field of software services/solutions in the field of AML and restrictive measures.

The Contractor undertakes to guarantee 99% availability and responsiveness of the software solution subject to the contract (hereinafter: ICT service).

The Contractor shall notify the contracting authority at least seven (7) working days prior to implementing significant changes (e.g. major updates or upgrades of the system, replacement or enhancement of servers and network devices, introduction of new security solutions, etc.).

All updates and/or fixes must be documented in writing and shall comply with requirements related to security and digital operational resilience (Regulation (EU) 2022/2554), as well as applicable legislation governing data processing and protection against cyber threats. Updates and/or fixes must not negatively impact the performance of ICT services, cause data loss, or result in service disruptions.

In the event of an error related to the ICT service, both the client and the contractor must act in accordance with the procedures defined in "17.3.6 Specifications" form, which is an integral part of the tender documentation. These procedures include notification, response and resolution times to resolve the error. The notification must include a description of the nature of the error, corrective actions taken, and a report on data protection measures. The Contractor must resolve the error, whether detected independently or notified by the Contracting Authority as defined in "17.3.6 Specifications" unless otherwise agreed upon by both parties due to the scope or impact of the error on the operation of the Contracting Authority. The Contractor shall ensure that the corrective actions taken prevent recurrence of the error.

The Contractor shall be at the Contracting Authority's disposal:

for system administration and maintenance during regular working hours (8 am to 4 pm) on all business days in Slovenia:

by telephone at: _____;
by email at: _____;
through the Contracting Authority's request submission and error reporting application: _____.

If the application is unavailable, errors are to be reported simultaneously by telephone and email at the specified number and address.

The Contractor undertakes to immediately notify the Contracting Authority of any change in its phone number or email address.

The Contractor shall regularly monitor the performance of ICT services and shall report to the contracting authority on a monthly basis regarding service availability (expressed as a percentage), the number and type of errors, response and resolution times, and the effectiveness of recovery procedures.

Article 15

The Contractor commits to notifying the Contracting Authority about the measures taken for the rapid resolution of any ICT-related incidents, data protection, service recovery, and ensuring smooth operations, striving to address the incident's consequences as quickly as possible. The Contractor also commits to documenting all procedures undertaken and issuing a report to the Contracting Authority on the corrections made, data protection, and other necessary actions.

IV. PERFORMANCE USING SUBCONTRACTORS

Article 16 [4]

The Contractor may also perform the contractual services with Subcontractor(s) in the manner specified in the documentation related to the public procurement and the Contractor's tender.

The Contractor undertakes to:

- monitor the services that have been subcontracted;
- ensure continuous and timely fulfilment of all contractual obligations to the Contracting Authority;
- obtain prior written consent from the Contracting Authority before subcontracting the service and data to the subcontractor and specify the location of the data that will be processed or stored by the Subcontractor;
- immediately notify the Contracting Authority of any changes in the performance of contractual obligations by its Subcontractors which affect or could affect the provision of the ICT service;
- be fully accountable to the Contracting Authority for the execution of the received order;
- ensure that the Subcontractor of ICT services grants the Contracting Authority and the relevant competent authorities the same rights of access, inspection, and audit as the Contracting Authority has with the Contractor;
- be responsible for the execution of ICT services performed by Subcontractors of ICT services;
- regularly monitor ICT service Subcontractors and regularly report to the Contracting Authority on the implementation of these services with Subcontractors and any risks associated with Subcontractors;
- when replacing or including a new Subcontractor, assess all risks associated with the location of the Subcontractor, the parent company, and the location from which the ICT service will be provided;
- provide the Contracting Authority with information on the location of the data processed or stored by the Subcontractor, where appropriate, and ensure that these locations comply with applicable regulations and data protection requirements. In the event of a location change, the Contractor must notify the Contracting Authority in writing at least thirty (30) days before the intended change. The Contractor must ensure compliance with all applicable legal requirements. The location change is permitted only with the express prior written consent of the Contracting Authority;
- ensure that the Contracting Authority has the contractual right to terminate the Contract in the event of improper subcontracting (e.g., if the risks for the Contracting Authority significantly increase due to subcontracting; if the external Contractor subcontracts the service without prior written consent from SID bank, etc.) or in the event of violations in the performance of ICT services by the Subcontractor.

The Contractor undertakes to conclude a written contract with the ICT services Subcontractor that complies with the provisions of the Contract. Within this contract, the Contractor must:

- transmit in writing its contractual obligations regarding monitoring and reporting to the Subcontractor providing the ICT service and demonstrate compliance with these obligations to the Contracting Authority upon request;

[4] *Applies only if the Contractor has enclosed a subcontractor's request for direct payment with its tender.*

- ensure the continuity of ICT services even in the event that the Subcontractor fails to fulfil its contractual obligations, which include the requirements for contingency plans in business continuity. The contingency plans requirements must be equivalent to the requirements that the Contracting Authority has towards the Contractor;
- ensure that the Subcontractor's commitments regarding ICT service security standards and, where applicable, any additional security requirements are equivalent to the requirements that the Contracting Authority has toward the Contractor.

In the event that there are significant changes in the relationship between the Contractor and the Subcontractor during the Contract execution, the Contractor must notify the Contracting Authority of these changes within a timeframe that allows the Contracting Authority to adequately assess the risks and impact of the changes on the Contractor's ability to fulfil contractual obligations regarding Subcontractor monitoring and Subcontractor changes. The Contractor may implement changes related to subcontracting only after prior approval from the Contracting Authority. In the event that Subcontractor-related changes are not approved, the Contracting Authority has the right to terminate the Contract.

The Contractor must notify the Contracting Authority in advance of any changes related to Subcontractors during the execution of the public procurement. The replacement of a Subcontractor or the inclusion of a new subcontractor is possible only if the new subcontractor meets all the conditions of this Contract, the documentation related to the public procurement, and legal regulations, and with the prior written consent of the Contracting Authority. In this case, the Contractor must submit the following to the Contracting Authority at least thirty days before the change:

- contact details and legal representatives of the proposed new Subcontractors,
- completed forms (as indicated in point "14.2 Conditions for participation") of the documentation related to the public procurement,
- specify each part of the public procurement that is intended to be subcontracted,
- attach the Subcontractor's request for direct payment, if the Subcontractor requests it,
- the Contractor's written statement and the written statement of the replaced Subcontractor that this Subcontractor has received payment for the performed contractual obligations and that both the Contracting Authority and the Contractor have paid all undisputed claims,
- other requirements as requested by the Contracting Authority in the specific case.

In the case that the risk assessment of the existing Subcontractor increases, the Contracting Authority has the right to demand that the subcontractor makes improvements. If the Subcontractor does not achieve improvement or the risk level does not decrease, the Contracting Authority has the right to request the replacement of the Subcontractor. If the Contractor does not carry out the required replacement of the Subcontractor, the Contracting Authority has the right to terminate the Contract.

When the Contractor intends to execute the public procurement with a subcontractor who requires direct payment in accordance with this article, the Contractor must:

- authorize the Contracting Authority with this Contract to pay the Subcontractor directly on the basis of the Contractor's confirmed invoice or situation,
- the Subcontractor must submit consent, on the basis of which the Contracting Authority settles the Subcontractor's claim against the Contractor instead of the Contractor,
- the Contractor must attach the subcontractor's invoice or situation to its invoice or situation, which was previously confirmed by the Contractor.

V. CONTRACTOR'S OBLIGATIONS

Article 17

The Contractor shall:

- perform all services and works in accordance with the specifications laid down in the Specifications form (Annex 17.3);
- cooperate with the Contracting Authority in the manner set out in the procurement documentation and the Contract;
- perform the works assumed with due professional diligence (in particular in terms of security, reliability and organisation in the performance of implementation, integration and routine maintenance activities);

- perform activities in accordance with the applicable law and regulations;
- perform the works assumed using suitably qualified staff and in accordance with the requirements of the Contracting Authority's procurement documentation;
- notify the Contracting Authority or its supervisory body without delay of the occurrence of any materially important circumstances that it knows about or should have known about and that affect or might affect the performance of the public contract;
- notify the Contracting Authority in the manner provided in this Contract;
- perform the works with due professional diligence, conscientiously and in good faith, in accordance with the applicable regulations, standards and norms and the applicable legislation (including information security regulations, EBA Guidelines,..) in force in Slovenia and the European Union, and by the agreed deadlines;
- use the latest information technologies and methods in the performance of its contractual obligations;
- allow the Contracting Authority and Contracting Authority's competent authorities (and any other person appointed by them) to access, inspect and supervise the execution of the works at any time, and comply with its instructions;
- allow the Contracting Authority and Contracting Authority's competent authorities (and any other person appointed by them) to audit its data in relation to the performance of services under this Contract;
- provide the Contracting Authority with any necessary clarifications regarding the performance of the services, and notify it promptly of anything that might affect the implementation of its contractual obligations;
- deliver the documentation necessary for performance of this Contract to the Contracting Authority;
- include, without changing the price and in accordance with the principles of due professional diligence, any other necessary works not specifically provided for in the public contract but forming an integral part of the ordered works in substantive or technical terms, and necessary to the successful and proper performance of the works;
- act on its own behalf and for its own account vis-à-vis third parties participating in the performance of individual activities, and only act on behalf of the Contracting Authority with the latter's prior written authorisation;
- comply with information security standards (ISO/IEC 27017, ISO/IEC 27018 or equivalent) the certificate obtained will be maintained or renewed by the Contractor throughout the duration of the contract, at its own expense;
- protect all information it acquires under this Contract in accordance with personal data protection and trade secrecy regulations;
- report any vulnerabilities and threats and any detected deviations from regular and established processes in connection with the services in question;
- participate as an external member of a team appointed by the Contracting Authority to handle security incidents arising out of or in relation to this Contract at the Contracting Authority's request;
- deliver written reports on the progress of the performance of the services in accordance with the project design activities and on the actual work performed (who, when, what, how much and why);
- enable the Contracting Authority to verify that the Contractor is protecting its data adequately at the physical and logical levels;
- ensuring the highest level of security in the processing, transfer, or storage of all data, including personal data, in accordance with the Contracting Authority's internal policies and European Union legislation;
- ensuring a high level of data availability and uninterrupted access to it in the event of technical problems or emergencies by using backups, recovery procedures, and other necessary measures;
- taking appropriate preventive measures to reduce the risk of disruptions in data availability, including system resilience to attacks and failures;
- ensuring that all data is authentic and allowing the verification of its integrity at any time;
- treating all data, including personal data, as confidential and taking all necessary measures to prevent unauthorized access, disclosure, alteration, or destruction of data;

- fully cooperating with the Contracting Authority's competent authorities and rescue authorities in case of Contracting Authority resolution;
- participating in ICT security awareness programs and digital operational resilience training organized by the Contracting Authority ;
- monitoring technological developments in the ICT field and establishing an effective and reliable framework to ensure digital operational resilience that enables the smooth and secure provision of ICT services;
- submitting and participating in the annual update of the forms from Chapter 14. Terms and conditions of participation od the Public Procurement and other attachments submitted when signing the Contract, demonstrating compliance with DORA, the EBA Guidelines on Outsourcing (EBA/GL/2019/02), and the EBA Guidelines on ICT and Security Risk Management (EBA/GL/2019/04);
- immediately notifying the Contracting Authority of any changes that could significantly impact the ability to provide ICT services in accordance with Appendix to the Contract (18.5 Specifications) and, if necessary, submitting regular annual reports on its operations (the article specifying service levels);
- implementing and regularly testing emergency business plans that include procedures for the rapid recovery of services in the event of errors or incidents in accordance with regulations that ensure adequate protection against cyber threats and enable the Contracting Authority 's continuous operation;
- if the ICT service Contractor subcontracts, this requirement also applies to the Subcontractor and must be specified in the written contract between the Contractor and the Subcontractor;
- establishing appropriate security measures, tools, and policies in the ICT field to ensure the appropriate level of security, enabling the uninterrupted provision of services in accordance with the legal framework, including the requirements of Regulation (EU) 2022/2554, and must ensure adequate protection against cyber threats and the continuous operation of the Contracting Authority;
- actively participating in the penetration test conducted by the Contracting Authority or an authorized third party, providing all necessary support and information, and participating in the preparation of the test results report;
- ensuring that the Contracting Authority's auditors and competent authorities have effective access to data and premises related to the use of ICT services;
- providing alternative assurances when necessary to protect the rights of the Contracting Authority and the Contracting Authority's customers. In the event of errors or issues with the services covered by the Contract that affect the rights of the Contracting Authority and its customers, the Contractor will ensure appropriate measures, such as uninterrupted access to services or data, maintaining the reliability and security of ICT services;
- submitting performance monitoring reports as requested by the Contracting Authority, including information on the conduct of inspections and audits of the services covered by the Contract and the method of ensuring compliance with contractual and legal requirements. The Contractor will provide details on the scope of the inspections (e.g., which systems, processes, or services were inspected), the procedure used during the inspection (e.g., steps, methods, and approaches), and the frequency of inspections (e.g., monthly, quarterly, annually), including the submission of internal or external audit reports relevant to the services covered by the Contract;
- fully complying with all applicable European Union regulations when providing ICT services and ensuring that the processing of all personal data is carried out in accordance with data protection legislation (this provision applies if the Contractor is from a third country);
- using the latest and highest quality information security standards in the provision of the services covered by the Contract.«.

The Contractor must ensure the Contracting Authority unrestricted access to all relevant information, systems, and documentation necessary for conducting inspections, audits, and obtaining documentation on-site, and must also allow the Contracting Authority to monitor and inspect the manner of service provision at the Contractor's premises, regardless of any other contractual contracts or internal policies.

The Contractor is obliged to grant full access to the Contracting Authority's supervisory functions (including employees in compliance, internal audit, risk management, and balance sheet departments, ...), external auditors of the Contracting Authority, and third parties authorized by the Contracting

Authority to conduct supervision, inspection, or audit of data related to the performance of contractual obligations.

The Contractor is obliged to allow the competent authority for the exercise of prudential supervision powers over credit institutions access to relevant data and its business premises, if necessary, e.g., in the case of an inspection and audit review.

The Contractor must report on the provision of services annually by January 10 for the previous twelve (12) months. The report must indicate the services provided and who performed them, the errors detected and their causes, whether the errors were corrected and within what timeframe, and other circumstances that significantly influenced or could influence the performance of the Contract. In the event of material circumstances that affect or could affect the provision of services, the Contractor is obliged to immediately inform the Contracting Authority.

VI. CONTRACTING AUTHORITY'S OBLIGATIONS

Article 18

The Contracting Authority shall:

- enable the Contractor to execute the works under this Contract;
- provide the Contractor with all information connected in any way with the subject of this Contract or required to ensure the high-quality performance of the Contractor's obligations under this Contract;
- cooperate with the Contractor for the purpose of performing the contractual obligations in a timely fashion, in their entirety and in accordance with the documentation relating to the public contract;
- regularly inform the Contractor of any significant changes related to performance of the contractual obligations;
- accept the general licence conditions for use. In case that there is a conflict between the provisions of the General Licence Conditions and the provisions of the Contract, the provisions of the Contract shall prevail;
- meet its payment and other obligations in accordance with the documentation relating to the public contract;
- work with the Contractor to ensure that contractual obligations are performed in a timely manner, in full, and in accordance with the procurement documentation and the Contractor's tender;
- promptly notify the Contractor of any material changes relating to the performance of its contractual obligations;
- notify the Contractor of any necessary changes to the services resulting from legislative changes, changes to the business environment or the internal needs of the Contracting Authority as soon as such information becomes available, and deliver all the necessary associated specifications and instructions to the Contractor;
- notify the Contractor of any planned changes to linked systems as soon as such information becomes available, deliver a specification of the changes to the Contractor, and consult with the Contractor on the deadline for the implementation of all the necessary modifications;
- continuously monitor and supervise performance of the works;
- perform its payment and other obligations in accordance with this Contract.

VII. CONTRACT VALUE

Article 19

The Contractor undertakes to perform services that are the subject of this contract at the tender prices set in the sample form Pro-forma invoice (Annex 17.4 to the Documentation on the awarding of the public contract).

The indicative contract value is _____ EUR (without VAT). Tender prices shall remain unchanged throughout the term of this Contract.

(The Contracting Authority shall insert appropriate tables or data from the tender pro-forma invoice here.)

The tender prices net of VAT shall include all elements, i.e. all costs (labour costs, hardware and software costs, travel costs and all other costs that could arise in relation to the performance of the contractual works over the entire period of the Contract), fees and other levies (except for VAT), and any discounts or commissions, additional tax burdens and tax obligations waived so that the Contracting Authority is not liable for any costs connected with the subject of the public contract.

With regard to individual orders for additional services, the Contractor shall define any additional costs separately and clearly when compiling its offer for a specific request or upon receiving an order. If the Contracting Authority agrees with the costs stated and also approves them in writing, and if these costs are actually incurred by the Contractor, the Contracting Authority shall pay those costs.

The Contractor shall not be entitled to any additional payments or costs increases, and shall ensure functional operation of the subject of the Contract within the terms of the contractual price.

VIII. PAYMENT METHOD

Article 20

The Contractor shall issue an invoice for the implementation/ integration of a service within 30 days after the implementation/ integration of the service with the signed record of handover for the successful implementation/ integration of a service.

The Contractor shall issue an invoice for licenses for first year within 30 days after the implementation/ integration of the service with the signed record of handover for the successful implementation/ integration of a service.

All invoices shall include a reference to the Contract and the Contractor's VAT registration number.

The Contracting Authority shall pay licenses for first year of use up to 10,000 insights/inquiries. On the anniversary, the Contracting Authority will choose which licenses will he order for the next year. The Contractor must submit a report from the application on past actual insights to the Contracting Authority 30 days before the anniversary. The Contracting Authority will inform the Contractor about the new licenses 10 days before the anniversary.

Additional services will be invoiced by the Contractor after the work has been carried out. The invoice must be accompanied by a report on the work carried out, showing the date and time, the content of the work and the amount of time spent.

Article 21

The Contracting Authority shall make payments on the basis of invoices correctly issued by the Contractor to the Contractor's bank account no:

_____ with _____ within thirty (30) days of receiving each correctly issued invoice. The Contractor shall send invoices to the Contracting Authority in e-invoice form to the Contracting Authority's email address at e-racun@sid.si.

If the last day for payment is not a business day, the Contracting Authority shall make the payment on the following business day.

If the tender includes or the Contracting Authority subsequently receives a subcontractor's request for direct payment and a completed and signed form 17.2 ("Subcontractor's request for direct payment") of the procurement documentation, the Contracting Authority shall pay invoices issued by subcontractors and approved by the Contractor for individual types of works directly to the bank account(s) of the relevant subcontractor(s) by the payment deadline laid down in the preceding paragraph.

For nominated subcontractors not requiring direct payment, the Contracting Authority shall ask that the Contractor send it the following within 60 (sixty) days of payment of the final invoice or statement: its own written declaration and the written declaration of the subcontractors to the effect that they have received payment for the work performed. Should the Contractor fail to act in accordance with this provision, the Contracting Authority shall submit a proposal to the National Review Commission to initiate the misdemeanours proceedings referred to in point 2 of the first paragraph of Article 112 of the ZJN-3.

IX. CONTRACTUAL PENALTY AND LIABILITY FOR DAMAGES

Article 22

If the Contractor breaches a contractual obligation, the Contracting Authority shall be entitled to enforce a contractual penalty.

If the Contracting Authority cannot use the application due to a reason at the Contractor's side, the Contractor must pay a contractual penalty of 500.00 (five hundred) EUR per day for each day of non-operation, but not in excess of 20% of the contractual value for actual licenses.

If the Contractor fails to abide by the contractual provision of additionally ordered services, the Contracting Authority shall charge a contractual penalty amounting to 2% of the value of the order (net of VAT) for every day of delay commenced, but not in excess of 20% of the value of the order (net of VAT). The Contracting Authority shall, in this case, be entitled to request fulfilment of the obligation as well as a contractual penalty.

The right to charge a contractual penalty for a delay is not conditional upon damage being incurred by the Contracting Authority. The Contracting Authority shall claim reimbursement for damages incurred under the general principles of liability for damages and independently of whether a contractual penalty for delay is imposed. The Contracting Authority shall offset the contractual penalty and any damage incurred as a result of a delay against the next payment to the Contractor under this Contract or, if this is not possible, issue a separate invoice, which the Contractor is obliged to pay within 15 (fifteen) days of receiving it.

Article 23

If the Contractor is late in providing contractual services under this Contract such that it could cause damage to the Contracting Authority or would render provision of the services meaningless, the Contracting Authority may order a replacement service from another Contractor, with the costs of this being borne by the Contractor that is late, and may demand compensation for the actual damage incurred.

Article 24

The Contractor shall not be held liable for indemnification that may occur if the services are not available due to:

- Contracting Authority’s delay or failure of using the timely delivered instructions for using alternative access paths,
- Contracting Authority’s delay or failure of using the installation of the application
- changes to the Contracting Authority’s firewall system and/or configuration of the Contracting Authority’s network, which may lead to lack of ability to use the access paths for the services provided by the Contractor.

X. TERMS OF THE QUALITY OF PROVISION OF SERVICES

Article 25

If, upon inspection of the services performed, the Contracting Authority finds that the quality of the performed services does not meet the Contracting Authority requirements, he informs the Contractor about this and at the same time gives requests for improving the quality of the services (implementation method, corrective measures, etc.), which he prepares on the basis of the Contractor's data. The defined requirements for improving the quality of service delivery are binding for both contracting parties. The Contractor is obliged to correct errors at the Contracting Authority's request. The Contracting Authority reserves the right to not pay the invoice for a poorly performed service, for the part of the invoice that refers to the poor quality of the service, and until the error is eliminated.

X. WITHDRAWAL FROM THE CONTRACT FOR FAULTY REASONS

Article 26

The contracting party may terminate this Contract if the other party of the contract (the defaulting party) breaches its contractual obligations and fails to remedy such breaches within a reasonable period after receiving a written notice from the other party describing the violations, calling for their rectification, and providing an appropriate deadline for compliance.

Such notice must be sent to the defaulting party at the email address of the contract supervisor designated by the defaulting party.

If the first contracting party does not receive an automatic response that the notice was not delivered to its address, it shall be deemed that the defaulting party received the notice.

In the event that the Contractor unjustifiably withdraws from the Contract, the Contracting Authority has the right to charge contractually penalty in the amount of 20% of contract value.

Article 27

The Contracting Authority may, under the conditions and in the manner stipulated in Article 26 of this Contract, terminate this Contract if the Contractor breaches its contractual obligations, especially the obligations specified in Article 17 of this contract, and also in the event that:

- the Contractor fails to accede to the implementation of this Contract;
- the Contractor breaches the applicable legislation;
- the Contractor fails to satisfy the criteria of the questionnaire to assess reputation and compliance risk;
- the Contractor does not meet standards in the field of information security (ISO/IEC 27017, ISO/IEC 27018 or equivalent certificates or standards);
- the Contractor performs the works improperly, negligently and in an untimely manner;
- the Contractor fails to meet its obligations under this Contract even after being reminded to do so by the Contracting Authority
- the Contractor does not comply with the provisions of the Information Security Policy, security regulations, procedures and standards of the Contracting Authority;
- the Contractor fails to declare Subcontractors in the manner provided in Article 16 of this contract;
- the Contractor acts on account of the Contracting Authority vis-a-vis third parties without prior written authorisation by the Contracting Authority or exceeds such authorisation;
- the Contractor is found in a situation preventing it from performing the obligations arising from this Contract;
- the Contractor stops work without the written consent of the Contracting Authority;
- the Contractor performs its contractual work in a negligent manner;
- the Contractor fails to meet its obligations under this Contract even after being requested to do so by the Contracting Authority;
- the Contractor fails to protect the Contracting Authority’s business secrets;
- the Contractor delays the performance of works to such an extent that the entire contractual penalty defined in this Contract has fallen due;
- the Contractor in the event of instructions being issued by the competent body of SID Bank, e.g. if the competent authority is no longer able, on account of the Contract with the Contractor, to exercise effective supervision of SID Bank;
- circumstances arise that could affect the provision of Contractual services or the position of the Contractor, or present a risk to the Contracting Authority 's compliance with regulations or digital operational resilience;
- weaknesses in risk management in the IT field are demonstrated, especially in ensuring the availability, authenticity, integrity, and confidentiality of data (personal or otherwise), which poses a risk to the Contracting Authority's digital operational resilience;
- the competent authority can no longer effectively supervise the Contracting Authority due to the terms of the Contract or circumstances related to it, which poses a risk to compliance with regulations and digital operational resilience;
- the Contractor makes substantial changes to the written contract with the subcontractor, despite the Contracting Authority's objection or non-compliance with the Contracting Authority 's requirements and the period, which allows the Contracting Authority an appropriate assessment of the risks and the impact of the changes;
- part of the IT service is subcontracted, even though the Contract does not allow subcontracting.

In case of termination by the Contracting Authority, the Contractor shall not be entitled to any compensation. The Contractor is obliged to compensate all damages suffered by the client as a result of the termination and this within 30 (thirty) days from receiving a written claim from the Contracting Authority.

Article 28

Without prejudice to the provisions of the law governing obligational relationships, the Contracting Authority may withdraw from this Contract during its period of validity in the following circumstances:

- the public contract is substantially changed, requiring a new contract award procedure;
- at the time the public contract was awarded, the Contractor was in one of the positions that compels the Contracting Authority to exclude it from the public procurement procedure, but the Contracting Authority was not made aware of this fact during the public procurement procedure;
- if owing to serious breaches of the obligations set out in the TEU, the TFEU and this act, identified by the Court of Justice of the European Union in accordance with Article 258 of the TFEU, the public contract should not have been awarded to the Contractor;
- in the event of a decision by the competent Contracting Authority, if the competent authority determines that due to the Contract can no longer effectively control the Contracting Authority.

XI. TERMINATION OF CONTRACT

Article 29

Notwithstanding the provision on the duration of the contract, either contracting party may unilaterally and prematurely terminate the contract without stating a reason, by sending a notice of termination to the email address of the contract administrator appointed by the counterparty. The mutual notice period shall be 90 days.

In the event of a request by the competent regulatory authority, the Contracting Authority shall have the right to terminate the contract within the notice period determined by the said regulatory authority.

Article 30

The Contractor must, in the event of termination of the Contract, during the notice period, ensure the provision of ICT services specified in the Contract in a manner that minimizes the risk of disruptions for the Contracting Authority, ensuring compliance with legal requirements, limiting damage to the continuity and quality of services provided to the Contracting Authority and the Contracting Authority's customers, and enabling effective resolution and restructuring of the ICT services specified in the Contract. The Contractor must allow the Contracting Authority to transition to another ICT service Contractor or to an internal solution that corresponds to the complexity of the ICT services specified in the Contract during the notice period.

In the process of termination, the Contractor must strictly adhere to the Contracting Authority's security policy and rules and perform activities in accordance with applicable legislation and banking regulations, particularly ensuring data protection and information security.

The Contracting Authority will define key exit strategy activities according to internal strategy and business decisions, and the Contractor will ensure the following during the exit process:

- at least two (2) members to carry out exit activities, namely one for management and coordination and another for technical and content-related tasks,
- comprehensive technical and functional documentation, including a description of the last state before the activation of the exit plan,
- enable the transfer of the Contracting Authority's data in an easily accessible form and provide the Contracting Authority with all professional and technical assistance, especially concerning data stored in the cloud,
- transfer all licenses and maintenance of the subject of the Contract to the Contracting Authority or to a Contractor designated by the Contracting Authority,
- collaborate with other Contractors authorized or hired by the Contracting Authority to implement the exit plan.

XII. TEMPORARY OR PERMANENT INABILITY TO PERFORM SERVICES

Article 31

If either party becomes unable to perform its obligations, the party that is unable to perform its obligations shall notify the other party by the following business day of the obstacles preventing the

performance of its contractual obligations and the additional period of time it will require to perform its obligations, if performance is possible.

Liability for any inability to perform obligations shall be determined in accordance with the Code of Obligations (Code of Obligations (Official Gazette of RS, No 97/07, 64/16 - odl. US, 20/18)).

XIII. ANTI-CORRUPTION CLAUSE

Article 32

The Contract shall be void if it is established that the Contractor alone or anyone on its behalf or for its account promised, offered or gave any undue advantage to a representative or intermediary of SID Bank to obtain the Contract or conclude the Contract under more favourable terms and conditions or to omit due surveillance over the implementation of contractual obligations or any other action or omission that causes damage to SID Bank or allows a representative of SID Bank, its intermediary, the other Contracting Party or its representative or its representative, agent or intermediary to obtain undue advantage pursuant to Article 14 of the Integrity and Prevention of Corruption Act (Official Gazette of the Republic of Slovenia, No. 45/10 with amendments).

Pursuant to the sixth paragraph of Article 14 of the ZIntPK and in order to ensure the transparency of the transaction and to prevent the risk of corruption, the Contractor shall be obliged to submit to the Contracting Authority a declaration or information on the participation of natural persons and legal entities in the ownership of the Contractor, including the participation of silent partners, and on the economic operators which, with regard to the provisions of the law governing companies, are considered to be affiliates of the Contractor, prior to entering into any contract valued at over EUR 10,000 net of VAT. For natural persons, the declaration shall give the first name and surname, the residential address and the share of ownership. If a Tenderer submits a false declaration or provides inaccurate information regarding the above facts, this shall result in the Contract being declared null and void.

XIV. SOCIAL CLAUSE

Article 33

The Contract is concluded under a resolutory condition, which shall be exercised if the Contractor is aware that:

- a court has established by a final decision that the contractor or its Subcontractor has breached the obligations referred to in Article 3(2) of the Public Procurement Contract;
- the competent public authority has established at least two infringements by the contractor or its subcontractor during the performance of the contract relating to remuneration for work, working time, rest periods, the performance of work on the basis of contracts governed by civil law despite the existence of elements of an employment relationship, or to undeclared work, for which the contractor or its subcontractor has been sentenced by a final decision or several final decisions a fine for an offence.

In the event of knowledge of the infringement, the contracting authority shall inform the contractor thereof within ten days and shall act in accordance with the third indent of the fourth paragraph of Article 67 of the Law on Contracts for Contracts for Employment. The condition precedent shall be fulfilled provided that at least six months have elapsed between the date on which the Contracting Authority became aware of the infringement and the expiry of the contract. In the event that the termination condition is fulfilled, the contract shall be deemed to be terminated as from the date of conclusion of a new public procurement contract for the contract in question. If the contracting authority does not initiate a new procurement procedure within the period laid down by law, the contract shall be deemed to have been terminated on the sixtieth day following the date on which the infringement was brought to its attention.

XV. PROTECTION OF TRADE SECRETS AND PERSONAL DATA

Article 34

The contracting parties undertake, during the performance of this Contract and after its expiry, to safeguard all personal data, trade secrets, classified information and other confidential data (hereinafter: confidential data) referred to in this Contract, or confidential data of which they have learned in connection with this Contract or of which they will learn during the performance of this

Contract, as data to which the rules for the safeguarding of confidential data apply with regard to the particular type of confidential data, and not to use it for their own purposes or for third parties, or to disclose it to third parties. This obligation shall not apply to information classed as public in accordance with applicable regulations.

The Contractor undertakes to safeguard and process the Contracting Authority's confidential data in accordance with the applicable legislation governing in any way the protection of data, in particular, the Personal Data Protection Act, the Trade Secrets Act, the Banking Act, the Financial Instruments Market Act and, as a rule, with the recommendations of the ISO/IEC 27001 and ISO/IEC 27002 standards, as well as with other standards and good practices governing data protection. The Contractor undertakes to separate the Contracting Authority's confidential data from the data of other partners with which it does business in such a way as to not disclose confidential data. In the event that, during the execution of the Contract, it is necessary to disclose confidential information of the Contracting Authority to the Contractor, the Contractor, at the request of the Contracting Authority, undertakes to enter into a non-disclosure Contract (NDA) with the Contracting Authority in accordance with the Contracting Authority's internal acts.

The Contractor shall use the Contracting Authority's confidential data exclusively for the performance of contractual obligations in accordance with this Contract.

Before commencing work, the Contractor undertakes to issue the Contracting Authority, at its request, with a list of the persons who will directly perform the works, have knowledge of the Contracting Authority's confidential data and be obliged to sign a confidential data protection or other statement in accordance with the applicable legislation and/or the Contracting Authority's by-laws. The Contractor shall expand the obligation to safeguard confidential data to all those who are to directly perform works under this Contract such that, before commencing works and at the Contracting Authority's request, they deliver to the Contracting Authority a signed confidential data protection statement.

The obligation to safeguard confidential data shall apply during and after the performance of this Contract, unless the parties agree otherwise.

The Contractor shall ensure that those persons who are to directly perform contractual obligations are informed that they are required to safeguard data confidentiality at all times, even after the termination of their employment or other legal relationship with the Contractor. The Contractor shall bear liability if the disclosure or unauthorised use of the confidential data referred to in this Contract occurs, either through its fault or the fault of persons who directly perform works.

The Contractor undertakes to:

- carry out all activities necessary to ensure that confidential data remains confidential, and secure it from theft or any unlawful appropriation;
- use data sent solely for the purpose of performing this Contract;
- return to the Contracting Authority or destroy all data acquired from the Contracting Authority during the period of validity of this Contract, including any copies thereof, after the Contract expires.

Should the contracting parties learn of personal data during the performance of this Contract, each contracting party shall be required to safeguard and process the personal data that they possess as the controller in accordance with European and national personal data protection legislation. The contracting parties shall ensure that individuals whose personal data they hold are granted the rights of individuals pursuant to the law binding on the contracting party. The contracting parties hereby agree that they shall not process personal data acquired on the basis of this Contract on behalf of the other contracting party, and that neither contracting party is a contractual processor for the other contracting party, as the processing of personal data is not the subject of this Contract. The personal data of individuals who participate in the performance of this Contract or are otherwise important to the performance of the Contract shall be exchanged between the contracting parties so that an individual contracting party may perform its contractual obligations or exercise its rights under this Contract (i.e. each contracting party shall process personal data on its own behalf). The contracting parties shall process personal data only in a manner indispensable for the performance of the Contract, store it only for such time as is required for the performance of this Contract and its legal safety, and safeguard it with appropriate technical and organisational measures that protect it against unauthorised or unlawful processing, accidental loss, destruction or damage.

The contracting parties shall ensure that they have a lawful legal basis for the communication of the personal data of an individual to the other contracting party.

The Contracting Authority's general privacy statement (on the protection of personal data) is published on its website at https://www.sid.si.

At the Contracting Authority's request, the Contractor shall also be required to carry out additional procedures that constitute a necessary security standard for the needs of the Contracting Authority's work. The Contracting Authority shall have the right to record and monitor all activities carried out by the Contractor in connection with the Contract.

The Contractor hereby declares that it has been apprised that records are kept of the use of the Contracting Authority's data or data resources, and that persons authorised by the Contracting Authority may use such records as evidence in the event of a breach, in accordance with the relevant commercial and security provisions.

Upon signing this Contract, the Contracting Authority shall brief the Contractor, as required and according to circumstances, regarding the content of its security policy and data protection procedures in mutual communications in order to ensure the effective performance of contractual obligations and the safeguarding of confidential data. In the event of a finding or an amendment to legislation requiring the signing of a special data processing contract, the Contractor undertakes to sign such an contract. The Contractor undertakes to uphold the security policy and the data protection procedures communicated in accordance with the previous sentence.

The Contracting Authority may forward to the competent authorities and organisations data in connection with this Contract and public contract as requested pursuant to regulations. The Contracting Authority may publish the entire content of the Contract, if so required by regulations.

If personal data protection is breached, the Contractor shall immediately inform the Contracting Authority by contacting the Contracting Authority's contract administrator, sending an email to the data protection officer (povop@sid.si) and handing over to them all the necessary data and information relating to the breach.

The Contractor shall be required to notify the Contracting Authority without delay of any breach or security incident relating to the unauthorised use or disclosure of personal and other confidential data under this Contract. In the event of a breach of the obligation to safeguard confidential data, the Contractor shall be required to pay the Contracting Authority the contractual penalty referred to in Article 33 of this Contract. If damage is incurred, it shall also pay for all direct damage in excess of the aforementioned sum.

The Contractor shall immediately inform the Contracting Authority of any breaches of security or security incidents in connection with the unauthorised use or disclosure of personal and other confidential data referred to in this Contract.

In the event of a breach of confidentiality obligations, the provider is obliged to compensate the Contracting Authority for any damages in accordance with this Contract.

The provider undertakes that in the event of insolvency, resolution or termination of business, or termination of the Contract, they will ensure access, recovery, and restoration of all personal and non-personal data of the Contracting Authority. The data must be delivered in an easily accessible format that allows the Contracting Authority to continue processing and using the data without interruption. Unless otherwise agreed, the provider must deliver the data within the termination period.

XVI. ADMINISTRATOR OF THE CONTRACT

Article 35

The administrator of this Contract for the Contracting Authority is:

_____

Telephone: _____

Email: _____

The administrator of this Contract for the Contractor is:

_____

Telephone: _____

Email: _____

The contracting parties shall inform each other of any replacement of the representatives specified in the first paragraph of this article within 3 (three) business days of the replacement. A written notice from either party to the other shall suffice for any change to the contact details or Contract administrator.

All notices in connection with this Contract shall be deemed to have been received on the day they are delivered in person, or on the day they are dispatched by email if sent to the addresses specified above by 5 pm on a business day in Slovenia; otherwise, notices shall be deemed to have been received on the following business day. Any shipment delivered by registered mail shall be deemed to have been delivered at the end of the eighth (8th) day after the day of posting by registered mail if sent to the most recent address provided.

Any amendments to this Contract shall be made in writing, approved by the administrators of the Contract and signed by the authorised signatories to the Contract. The document shall indicate the Contract to be amended, the amendments agreed and which parts of the existing valid Contract are to be amended, and the effect of the agreed amendments on the contract price.

XVII. HANDLING CONFLICT OF INTEREST

Article 36

The Contracting parties declare that there are no circumstances related to the conclusion of this Contract that constitute or could constitute a conflict of interest. Each Contracting party shall immediately notify the other party of any existing or potential conflict of interest, as well as any perceived conflict of interest, arising during the execution of this Contract.

The Contracting parties agree to take all necessary measures to manage the risks that may arise from a conflict of interest, including but not limited to:

- Excluding individuals with a conflict of interest from all further procedures related to the execution of the Contract, or taking other measures that effectively prevent these individuals from influencing the execution of the Contract,
- Implementing control procedures over actions already taken by individuals with a conflict of interest,
- Engaging another person to continuously check and approve all actions taken in relation to the execution of the Contract by the individual with a conflict of interest.

Each Contracting party is responsible for implementing measures concerning individuals acting on its behalf and/or for its account. The measures taken must be communicated to the other party. When necessary measures cannot be implemented without the involvement of the other Contracting party, the parties shall agree on the implementation of such measures.

A conflict of interest on the part of any Contracting party represents any private interest of key employees or employees involved in the conclusion or execution of this Contract, or the private interest of close family members of these employees, which could negatively affect the diligent, economical, fair, and effective execution of this Contract.«.

The Contracting parties agree to protect, within the framework of applicable law, all data and information obtained in connection with the disclosure of conflicts of interest as confidential, and to process any personal data in accordance with applicable data protection regulations.

XVIII. DISPUTE RESOLUTION

Article 37

The Parties agree that the Slovenian law shall apply to the assessment of rights and obligations under the Contract law. The Parties shall settle any disputes by mutual contract. In the absence of a disputed

issue cannot be resolved amicably, either party may bring the dispute before a court having subject-matter jurisdiction in Ljubljana.

XIX. OTHER PROVISIONS

Article 38

By signing this contract, the contractor agrees to the publication of this contract and publicly accessible information of public nature from this contract on the national portal dedicated to public procurement notices, in accordance with the provisions of the law regulating access to public information and the provisions of the regulation governing the publication of contracts in the field of public procurement, concessions, and public-private partnerships.

Article 39

Any matters not specifically covered by this Contract shall be subject to the provisions of the Code of Obligations (Code of Obligations (Official Gazette of RS, No 97/07, 64/16 - odl. US, 20/18)) and the applicable regulations governing the subject of this Contract.

Article 40

The Contract is concluded when it is signed by both contracting parties and lasts for 36 months from the signing of the record of handover for the implementation/ integration of the software solution in the field of AML and restrictive measures or until the date of the last annual license renewal.

The Contract can terminate in the following ways:

- upon the expiration of the agreed-upon time period;
- through termination of the contract by one of the parties in accordance with this contract;
- through withdrawal from the contract by a loyal party to the contract in accordance with this contract;
- by mutual contract of the contracting parties;
- as specified by law.

Article 41

The parties agree that the Contract is concluded only in electronic form and digitally signed with a qualified certificate and that the Contract concluded in this way has the same validity and effects as a contract signed by hand.

Article 42

The following documents shall form an integral part of this Contract:

- the publication of the public contract notice on the public procurement portal and the TED portal;
- the procurement documentation, including any amendments, corrections or supplementations;
- the Contractor's tender documentation and tender pro-forma invoice;
- documentation relating to any additional orders;
- a list of the Contractor's partners/subcontractors.

Contracting Authority:	Contractor:
SID bank, d.d., Ljubljana	_____
Date: _____	Date: _____
Borut Jamnik Chairman of the Management Board	_____ Director/ Chairman of the Management Board

Stanka Šarc Majdič, MSc
Member of the Management Board

_____
Director/Member of Management Board

17.11 Sample of the Exit Plan

EXIT PLAN

I. GENERAL PROVISIONS

1. article

(Content of the Exit Plan)

The Exit Plan is used in the case of outsourcing, where the bank has entered into an outsourcing agreement with a third party, and this agreement meets the conditions for outsourcing, while the outsourced function is at the same time defined as a critical or important function.

The Exit Plan is prepared by the order submitting party ie. outsourcing custodian with the aim of ensuring that, in the event of exiting the agreement, the process runs without major disruptions and as smoothly as possible. The plan must be comprehensive, documented, and, if necessary, appropriately tested (e.g., through an analysis of potential costs, impacts, resources, and time-related consequences of transferring the outsourced service to an alternative provider).

For the purpose of the Exit Plan, the bank should also define alternative solutions and prepare a transition plan that enables it to retrieve the outsourced functions and data from the service provider and transfer them to alternative providers or back in-house, or to take other measures to ensure the continuous performance of a critical or important function in a controlled and appropriately tested manner. In doing so, the bank shall take into account conditions that may arise due to the location of the data and shall implement the necessary measures to ensure business continuity during the transition phase.

II. EXIT PLAN

2. article
(Composition of the exit team)

The composition of the exit team must consist of experts performing the outsourcing and must be adapted to the organizations representing the bank's function outsourced and the outsourcing service provider.

The exit team will include:

- the outsourcing agreement custodian, responsible for assembling and leading the exit team (exit team leader);
- a representative of the Risk Management and Asset/Liability Management Department, accountable to the Director of the Risk Management and Asset/Liability Management Department;
- a representative of the bank responsible for _____, accountable to the Director of _____ (bank representative in the exit team);
- a representative of the bank responsible for _____, accountable to the Director of _____ (member of the bank's team in the exit team);
- a representative of the bank responsible for _____, accountable to the Director of _____ (member of the bank's team in the exit team);
- a representative of the outsourcing service provider responsible for _____, accountable to _____ at the outsourcing provider (outsourcing provider representative in the exit team);
- a representative of the outsourcing service provider responsible for _____, accountable to _____ at the outsourcing provider (member of the outsourcing provider's team in the exit team);

- a representative of the outsourcing service provider responsible for _____, accountable to _____ at the outsourcing provider (member of the outsourcing provider's team in the exit team).

3. article
(Exit Process)

The Exit Plan is intended for use in the event that it becomes necessary to transfer the outsourced function from the external service provider back to the bank or to another external service provider. The process starts when the conditions leading to the initiation of the process are fulfilled, as specified in the contract with the external service provider (which may also be set out in the service level agreement).

During the exit process, the function is expected to be performed uninterruptedly by the external service provider.

As part of the Exit Plan, the external service provider is obliged, in the transition plan, to:
1. Prepare a comprehensive transfer of technical and functional documentation related to the outsourcing;
2. Transfer data related to the outsourcing;
3. Deliver to the bank all documentation that is essential for the bank to ensure the uninterrupted performance of the function.

During the exit process, compliance with banking regulations must be ensured, with particular emphasis on data protection and information security.

The transition is considered successful if:
- all data related to the outsourcing have been transferred to the bank,
- all documentation essential to the bank has been delivered,
- the transition has been completed within the timeframe specified in Article 5 of this annex

4. article
(Post-Exit Process)

The external service provider is obliged to comply with the agreed standards during and after the performance of the outsourced function.

5. article
(Responsibilities)

The exit team leader is obliged to:
- define the duration of the exit from the agreement;
- coordinate and execute the exit plan.

The representative of the external service provider in the exit team is obliged to:
- define the duration of the exit;
- prepare all agreed documentation;
- regularly report to the exit team leader.

The representative of the bank's team in the exit team is obliged to:
- define the duration of the exit;
- receive all agreed documentation;
- ensure the performance of the function within the bank;
- regularly report to the exit team leader.

The representatives must submit the exit timeline no later than 5 business days after the conditions for exiting the outsourcing agreement have been met. The exit team leader is obliged to coordinate

the timeline and, within 10 days of the conditions being met, forward it to all parties involved in the exit process. In any case, the exit timeline must be submitted to:

- the Bank's Management Board;
- the Director of the Risk Management and Asset/Liability Management Department;
- the Director of the Compliance Department;
- the Director of the Internal Audit Department.

In the event of exiting the agreement, the outsourcing agreement custodian is responsible for the execution of the Exit Plan.

6. article
(Effective Date and Termination of validity)

This Exit Plan becomes effective on the date it is signed by all responsible parties and thus approved by the outsourcing agreement custodian, the responsible director, and the Director of Risk Management. The plan must also be signed by the external service provider, unless the elements of the plan are already covered in the contract with the external service provider.

Name	Date	Signature
Outsourcing Custodian		
Responsible Director for Outsourcing		
Director of the Risk Management and Asset/Liability Management Department		
Outsourcing Service Provider		