GENERAL BUSINESS TERMS OF COOPERATION IN THE AREA OF PROCUREMENT

of the Financial Group of Česká spořitelna
(version 9/2024)

1. General provisions

These General Business Terms of Cooperation in the Area of Procurement are issued in accordance with the provisions of Section 1751 of the Civil Code, and define the basic rights and obligations of the respective member of the Financial Group of Česká spořitelna entering into an agreement for delivery of goods or provision of services as the customer, and of its contractual partner, as the provider, during their mutual cooperation in the area of delivery of goods and/or provision of services.

2. Definition of basic terms

Unless explicitly stipulated otherwise, the following terms used in these business terms and in the Agreement have the following meaning:

Acceptance: procedure of handover and takeover of the Performance, which, depending on the nature of the Performance and arrangements between the parties, is contained in the Agreement or in Art. 8 of these business terms. During handover and takeover of the Performance, the provisions of Sections 1949 through 1951 of the Civil Code will not be applied.

Copyrighted work: the work in the meaning of Section 2 of the Copyright Act. A Copyrighted work also refers to a computer program in the meaning of Section 2(2) of the Copyright Act.

Copyright Act: Act No. 121/2000 Coll., on copyright, rights related to copyright and the amendment of certain laws, as amended.

Cloud services or **cloud solution**: cloud computing based services for remote access to HW and SW.

Member of the Financial Group of Česká spořitelna: Česká spořitelna, a.s., registered office: Prague 4, Olbrachtova 1929/62, Postal Code 140 00, ID Number: 452 44 782, CZ45244782, registered in the commercial register administered by the Municipal Court in Prague, File number B 1171, or any other company under the control of Česká spořitelna, a.s.. The information about the list of members of the Financial Group of Česká spořitelna is available on www.csas.cz. For the avoidance of any and all doubts it is agreed that the fact that the customer is no longer a member of the Financial Group of Česká spořitelna does not affect the application of these business terms on the already concluded Agreements.

CNB: Czech National Bank

DDP: "Delivered Duty Paid" delivery conditions according to Incoterms 2010.

Provider: the customer's contractual partner according to the respective Agreement.

DORA: Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector.

VAT: value added tax

Confidential Information: all information in oral or written form (including information in electronic form), which one contractual party provides to the other contractual party in connection to the Agreement, regardless of the form of its depiction, including but not limited to information for which a special confidentiality regime is stipulated by legal regulations (in particular banking secrets, personal data of the customer´s clients), regardless of whether the providing party explicitly identified it as confidential.

However, Confidential Information does not include information that has become publicly known, if this did not occur through violation of the obligation to protect it, information obtained based on a procedure independent of the Agreement and the other contractual party, if the contractual party that obtained the information is able to prove this fact, and information provided by a third party that did not obtain such information by violating one of the contractual parties' obligation to protect such information.

Invoice: a tax document corresponding to the relevant tax and accounting legislation of the Czech Republic.

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

HW, or hardware: technical devices or their parts, especially computers, monitors, printers, servers, active components, peripherals, etc.

Hosted software: usage of software, when software is located on servers of the provider, who performs its administration and maintenance and provides the customer with access to the software via internet connection or virtual private networks (a.k.a. Software as Service, or Application Service Providing).

IT, ICT or information technologies: HW, SW or their functional interconnection; this term includes also (according to the context) communication technologies and related services (e.g. consulting services).

IT Security/Security defect: it refers in particular to, but is not limited to defects, design and implementation, which may lead to an unexpected and/or an undesirable event which may pose a threat to the security of IT systems, networks, applications or used protocols.

Software Implementation: it refers to a set of activities connected with software installation on hardware of customer, performance of a settings and integration into existing IT infrastructure of the customer for the purpose of achieving of the purpose of the software implementation stated in the Agreement. If no purpose of the software implementation is stated in the Agreement, then it is always understood as a launch of a flawless software.

Incident: a cyber security incident that significantly compromises or has the potential to significantly compromise the security of information in information systems, the security of the Performance provided and/or the integrity of electronic communications networks.

License: an authorisation to exercise the right to use a copyrighted work to the stipulated extent.

Workaround: temporary removal of the impacts of defect (without removal of their source), which enables the change of categorization of the defect to the defect of lower category.

Civil Code: Act No. 89/2012 Coll., Civil Code, as amended.

Business terms: these general business terms of cooperation in the area of procurement.

Customer: the respective member of the Financial Group of Česká spořitelna, a.s. which enters into an Agreement incorporating these business terms by attachment or by reference.

Authorised user of Confidential Information: in relation to the relevant contractual party, its appointed proxies, employees, governing bodies and controlling entities, as well as potential tax, accounting or legal advisors of the contractual parties bound by a legal or contractual nondisclosure obligation. In relation to the provider the authorised users of Confidential Information are the subcontractors who participate in accordance with the Agreement in the Performance and who are contractually bound to protect the customer's Confidential Information. In relation to the customer these are particularly appointed employees, representatives or advisors of any Erste Group company, other entities in a similar position who need to be familiar with the provider's Confidential Information, and the customer's supervisory authorities.

Outsourcing: the customer's activity which is ensured for the customer by a third party on a contractual basis. Unless stipulated otherwise by the relevant legal regulations, significant outsourcing is in question if the following activities are outsourced:

a) activities of such importance that a deficiency or failure in their provision could have a major impact on the customer's ability to fulfil prudential rules or the continuity of its activity,

b) activities, the provision of which by the customer is conditioned by the granting of authorisation for the activity by the relevant overseeing authority,

c) activities that have a major impact on management of the customer's risks, or management of risks related to the aforementioned activities.

Performance: a service, delivery of HW, software or provision of related performance or provision of related activities, which are performed by the provider for payment based on the Agreement.

Pull-request: a specific request and mechanism by which a developer (a person creating the source code) requests a connection and inclusion of changes made to the source code to the main storage of a software project or project application.

Source code repository: a system with a secure storage that is used to manage produced source code, control particular development branches, and their merging into the final version of the software product. The Source code repository is also known under its English term "Version Control System".

Erste Group: i.e. a group of commercial corporations directly or indirectly controlled by Erste Group Bank AG, registered office: Am Belvedere 1, A-1100 Vienna, Austria, including this company. In this case, control refers to the holding of an ownership interest of more than 50% in the given company or holding of more than half of the voting rights, directly or indirectly.

SLA, or Service Level Agreement: an agreement on the guaranteed level of provided Performance, e.g. warranted level of certain parameters, availability of services, operability of SW or HW, maximum time to reaction on the reported defaults, maximum time to fix the reported default, etc.

Agreement: the agreement concluded between the customer and provider, which refers (directly or through another agreement between the customer and provider) to these business terms, and makes these business terms a part thereof. To eliminate doubts, the term Agreement also includes these business terms, in the scope in which the provisions of the Agreement do not contain divergence from the content of these business terms. The Agreement may also be concluded based on a written order (e.g. customer's SAP order). In these cases, it applies that if the customer's order according to the previous sentence contains information beyond the scope of the provider's original offer, stating that the obligation established by the order will be governed by these business terms, this constitutes valid acceptance of the offer, unless the provider rejects such acceptance without undue delay, at latest within 5 business days, in accordance with Section 1740(3) of the Civil Code. If the provider commences fulfilment according to the order before the passing of the deadline according to the previous sentence, it is understood that the provider does not reject such acceptance of the offer by the customer and waives its right to rejection.

Contractual parties, also the **parties**: the customer and provider collectively; the term in singular form indicates the customer, provider or either of them individually depending on the context.

Software, computer program or **SW:** order of instructions which describes the realization of the task given by a computer or similar technical device. This term includes all forms of a computer program, including those that are part of hardware. This term includes all components of a computer programs, its source and object code, related preparatory conceptual materials and documentation, as well as graphical and other elements of the user´s interface; this term does not include data processed by the software, unless expressly specified otherwise.

COTS Software: Commercial Off-The-Shelf Software: ready-made software product offered on the market to the public. The respective documentation and data carriers form always part of the delivery of COTS Software. In case of doubts it applies that the software subject of the Agreement is not considered to be the COTS Software.

Subcontractor: a contractor or other contractual partner to the provider, who participates in the Performance based on a different obligation towards the provider than employment or similar, the subject of which is the performance of dependent activity.

Defect: a condition where the provided Performance does not correspond to the specifications agreed upon in the Agreement, or the level of provision of the Performance guaranteed by the provider is not fulfilled If neither of those are agreed upon in Agreement, then a defect is a condition where the provided Performance and / or guaranteed level of providing the Performance does not correspond to quality and design suitable for the purpose stated in the Agreement. If no purpose is stated in the Agreement, then the achievement of the usual purpose for which the Performance usually serves, is understood as a purpose of the Agreement. A legal defect is a situation in which the Performance is encumbered with third-party rights contrary to the Agreement, the Performance or its use by the customer or provision by the provider is contrary to the relevant legal regulations, or if provision or use of the Performance is prevented by something other than a technical obstacle, for which the provider is liable.

Software development: the process of designing, specifying, documenting, creating, testing, and repairing software, software components and applications. The main part of software development is the creation (also referred to as programming) of source code or executable artifacts, but as a whole software development includes all the necessary activities, inputs, and outputs necessary to create the final software product, from design, through creation to deployment.

Essential function: 'essential or critical function' within the meaning of Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector means a function the disruption of which

would significantly impair the financial performance of a financial entity or the orderly conduct or continuity of its services and activities, or the interruption or an erroneous or unsuccessful course would significantly impair compliance with the financial entity's conditions and obligations under its authorisation or its other obligations under applicable financial services law.

Principles of personal data processing: customer's document containing information under art. 13 and 14 of GDPR, which is accessible on customer's web site or available on request from the customer.

VAT Act: Act No. 235/2004 Coll., on value added tax, as amended.

CS Act: Act No. 181/2014 Coll., on Cyber Security and on Amendments to Related Acts (Cyber Security Act), as amended.

CC Act: Act No. 90/2012 Coll., on Commercial Companies and Cooperatives (Act on Commercial Corporations), as amended.

UBO Act: Act No. 37/2021 Coll., Act on registration of ultimate beneficial owners, as amended.

3. Basic representations and obligations of the contractual parties

3.1 The customer is a company duly incorporated and existing in accordance with the legal code of the Czech Republic, and as such has the right to conclude the Agreement and duly fulfil its obligations arising therefrom.

3.2 By signing the Agreement, the provider confirms that: it is a business entity duly incorporated and existing according to the legal code of the country of its registered office; it has a license to operate in the territory of the Czech Republic in the necessary scope; and it has the right to conclude the Agreement and fulfil its obligations arising therefrom. The provider confirms that it has the skills and capacities allowing it to provide the customer with the Performance in the highest attainable quality, and that it is capable and will act with expertise and care usually associated with the subject of its activity, occupation or such situation.

3.3 By signing the Agreement, the provider confirms that it is not under criminal prosecution. The provider is obligated to immediately inform the customer, if any criminal proceedings have been initiated against him. The provider undertakes to submit a statement from the criminal records not older than 3 months from the date of the customer's request, immediately upon request from the customer at any time throughout the duration of the Agreement.

3.4 By signing the Agreement, the provider confirms that it is not in bankruptcy or liquidation, that insolvency proceedings have not been commenced against it, and that a petition to commence insolvency proceedings against the provider was not rejected due to a lack of assets. By signing the Agreement, the provider also confirms that no execution of a decision or distrainment has been imposed against its assets. The provider declares that it is not an unreliable payer according to the VAT Act and that it is not a subject of proceedings conducted by the tax administrator for the purpose of issuing a decision stating that the provider is an unreliable payer according to the VAT Act. Should proceedings be conducted against the provider for the purpose of issuing a decision stating that it is an unreliable payer according to the previous sentence, the provider is obliged to disclose this fact to the customer within a deadline of 15 business days from the day when the provider learns of this fact.

3.5 The provider undertakes:

a) to comply in the performance of the Agreement with all applicable and effective laws of the Czech Republic and the European Union that apply to its activities, including but not limited to laws on the protection of personal data, protection of classified information, cyber security and other relevant legal standards. Provider further expressly undertakes to comply with all obligations set out in the CS Act and related implementing regulations, including the adoption and maintenance of appropriate technical and organisational measures to ensure the protection of information and communication technologies and minimise the risks of cyber threats. Provider also declares that it has in place and properly maintains all the procedures and mechanisms required by the CS Act and that these will be up-to-date and operational throughout the duration of the contractual relationship.

b) to maintain the validity and effectiveness of all the necessary permits and licences required for its existence and due performance of the provider's business activity in the Czech Republic;

c) to preserve and/or to acquire all the trademarks, permits, licences, patents or other subject of intellectual property required for fulfilment of the Agreement;

d) to fulfil duly and punctually its tax obligations arising in connection to payments received from the customer,

e) to inform the customer of its bankruptcy or impending bankruptcy, about the commencement of insolvency proceedings against the provider or imposition of execution of a decision or distrainment against the provider's assets, or the risk of such situation

(issuance of an effective court decision, which under the given circumstances will probably not be fulfilled by the provider within the deadline stipulated by such decision),

f) to inform the customer that it has become an unreliable payer according to the VAT Act;

g) at the customers's request, provide documents from credible sources (e.g. an extract from the commercial register or similar records, annual report, list of shareholders, etc.) within 30 days of receipt of the request to prove the ownership structure and beneficial owner of the provider within the meaning of the UBO Act. Where the provider is subject to registration in the register of beneficial owners within the meaning of the UBO Act or similar register, it shall also provide an extract from such records or register.

3.6 By signing the Agreement, the provider confirms that as of the date of conclusion of the Agreement, he and/or the person controlling the provider within the meaning of the business corporation act and/or a person on its or their statutory and/or controlling bodies and/or a person acting on behalf of the provider are not included on sanctions and other similar lists maintained by the European Union, the USA, the United Nations and the Czech Republic. The provider undertakes to inform the customer without delay of the fact that he and/or a person controlling the suppler within the meaning of the business corporation act and/or a person on its or their statutory and/or controlling bodies and/or a person acting on behalf of the provider have been placed on sanctions and other similar lists maintained by the European Union, the USA, the United Nations and the Czech Republic.

3.7 For the purposes of the Agreement, the provider's obligations and representations according to Art. 3.2 through 3.6 of these business terms are considered to be fundamental, and their violation or falseness (albeit partial) constitutes a substantial breach of the Agreement, which is sufficient reason for immediate withdrawal from the Agreement by the customer.

4. Purpose and subject of the Agreement

4.1 If the customer is interested in the provider's Performance, the provider and customer will conclude an Agreement which specifies the relevant Performance, its price and other conditions of its provision, whereas the obligation established by the Agreement is governed by these business terms, in the scope in which the Agreement does not diverge from these business terms.

4.2 If the purpose of the Agreement is not set out therein, it is always the customer's interest in the due and timely provision of the provider's Performance, so that this Performance brings the customer the benefits usually associated with it, as well as those that the provider was potentially informed of during negotiations on conclusion of the Agreement.

4.3 Under the Agreement, the provider undertakes to provide the customer with the Performance, which is specified in detail in the Agreement, under the conditions stipulated in the Agreement. The Performance must always correspond to the conditions set out in Art. 6.1 of the business terms.

4.4 The customer undertakes to provide the provider, based on a time request, with the cooperation needed for due fulfilment of the provider's obligations. It is the provider's obligation to request this cooperation in time and specify it sufficiently. The customer is obliged to provide only such cooperation that cannot be ensured by other means, and only in a reasonable scope. In the event of delay in providing cooperation, which prevents the provider in its Performance, the provider is obliged to inform the customer's responsible person of this fact in writing; if this situation lasts longer than 14 days, the provider is obliged to send a notice also to the persons authorised to bind the customer in contractual matters.

4.5 The customer undertakes to pay the agreed price for duly delivered Performance under the conditions stipulated in the Agreement.

5. Subcontractors and provider's employees

5.1 During provision of the Performance, the provider is not authorised to use a subcontractor, unless agreed otherwise in the Agreement. If the Agreement allows the use of a subcontractor, the provider is responsible for the part of the Performance delivered by the subcontractor as though it was delivered by the provider itself. Failure of the subcontractor to fulfil its contractual obligations to the provider does not affect the provider's obligations or liability, and the provider remains fully liable to the customer for the fulfilment of its obligations.

5.2 If subcontractors are used, the provider is obliged to inform the customer upon request and without undue delay about the identification data of the subcontractors participating in the Performance and the scope of Performance entrusted to them. The customer reserves the right to reject a specific subcontractor without stating its reasons, but undertakes to exercise this right in a non-abusive manner.

5.3 In justified cases, the customer is authorised to request a change in the composition of the team of persons participating in the Performance for the provider. The provider is obliged to accommodate such request immediately and replace the given person with a different person whose qualifications correspond to the replaced person. The customer undertakes to exercise this right in a non-abusive manner.

5.4 The provider is obliged to ensure that all the persons participating in the fulfilment of its obligations from the Agreement, who remain on the customer's premises or workplaces or enter into the customer's IT infrastructure comply with the effective legal regulations on occupational health and safety regulations, effective rules and standards for use of IT, safety of IS/IT, protection of the customer´s data and all of the customer's internal regulations, with which the customer has familiarised the provider in advance or with which these persons were familiarised.

5.5 In the case of the Agreement for the provision of services by consultants (specialists) in the form of purchase of man-hours or man-days, the provider guarantees the stability of the team for the entire duration of the provision of the Performance. The provider shall be entitled to make a change in the assignment of specific specialist providing a specific Performance under the Agreement only if the vacant position is occupied by another suitably qualified specialist. The provider will provide training and information handover to the new specialist at his own expense. The new specialist must be approved in advance by the customer, and the provider is required to request such consent from the customer at least 1 month before the change of the specialist is to take place. The customer will not deny the consent without due cause. The customer reserves the right to a three-week trial period for each new specialist, during which he may terminate the co-operation with such specialist without being obligated to pay for the time worked by the new specialist. In the event that the provider's specialist at any time after the trial period does not meet the Customer's qualitative requirements, the Customer has the right to require the termination of cooperation with such specialist and the provider is obliged to provide adequate substitute and training for this substitute at his own expense.

5.6 If using a subcontractor, the provider undertakes to ensure that none of its contracts with this subcontractor are contrary to these business terms or the Agreement, and evade their purpose.

5.7 The provider undertakes to compensate the customer for all damages caused by the persons (employees, subcontractors, agents etc.), who will participate in Performance on behalf of the provider.

6. Warranty, insurance

6.1 The provider is liable for ensuring that all Performance from the provider is delivered according to the specifications of the Performance in the corresponding Agreement. The Performance must be free of defects, in the corresponding quantity, quality and grade and fully usable for the purpose for which it was purchased. The Performance must be delivered whilst exercising professional care and with a proactive approach. The Performance must comply with legal regulations effective in the Czech Republic or in another location where the Performance is to be provided or used according to the Agreement. The provider is obliged to ensure that all of its Performance is free of legal defects.

6.2 Unless agreed otherwise in the Agreement, the provider provides a quality warranty of 24 months on the Performance. The warranty period starts from the moment of Acceptance of the Performance as a whole, respectively Acceptance of the last separately handed over part thereof. Until Acceptance of the Performance as a whole, the warranty applies only to the parts of the Performance accepted as at the given time. However, it is understood that the customer has reported potential found defects in time, regardless of the moment of their identification, if they were reported at any time during the warranty period.

6.3 If a defect in the Performance is found after Acceptance of the Performance during the warranty period, the provider is obliged to remove the defect in the Performance or deliver substitute Performance that is free of defects, at its own expense, at latest within 10 business days from reporting of the defect by the customer, unless agreed otherwise. This does not affect the customer's rights from defective Performance, which are set out in these business terms, agreed in the Agreement or arise from the relevant legal regulations.

6.4 Defects in the Performance that prevent Acceptance of the Performance are not warranty defects, unless the customer accepted the Performance even with these defects; in this case, the defects listed in the acceptance protocol or otherwise reported during Acceptance are considered to be reported warranty defects from the moment of Acceptance of the Performance. Defects in the Performance that do not prevent Acceptance of the Performance and were listed in the acceptance protocol or otherwise reported during Acceptance are also considered to be reported warranty defects from the moment of Acceptance,.

6.5 In cases when it follows from the nature of the Performance, purpose of using the Performance or relevant legal regulations, the provider is responsible for obtaining potential necessary certificates for the Performance. The customer may request the submission of copies of these certificates as a part of the Performance, within the price for the Performance.

6.6 In cases where the Performance consists of the delivery of movable items, the provider undertakes that it will be capable of delivering spare parts for the Performance for minimally 5 years from Acceptance of the Performance. The warranty period on delivered spare parts is 24 months from delivery of the spare part.

6.7 The provider is obliged at its own expense to effectively protect the customer from third-party claims and compensate the customer in full if a third party successfully applies a claim arising from a legal defect in the provided Performance. If the third-party claim arising in connection to the Provider's fulfilment, regardless of its justification, lead to a temporary or permanent court-imposed ban or limitation in use of the Performance or part thereof, the provider is obliged to ensure substitute performance immediately and minimise the impact of this situation, at its own expense and without any impact on the price for Performance agreed according to the Agreement, whereas the customer's claims to compensation of damages will not be affected.

6.8 If the provider's obligation to maintain a specific insurance policy for risks related to the Performance is stipulated in the Agreement, the provider undertakes to maintain effective insurance in this scope, and for this purpose will fulfil the obligations arising for it from the insurance contract, in particular the payment of premiums and due fulfilment of its reporting obligation, throughout the entire duration of the Agreement. The provider will submit to the customer without undue delay, but at latest within 10 business days from the customer's request, an insurance certificate or copy of the insurance contract in the necessary scope, as evidence of having fulfilled the provider's obligation.

6.9 If the provider does not conclude insurance according to the Agreement, does not maintain its effectiveness or does not submit to the customer the insurance contract and document or confirmation according to the previous clause, the customer is authorised to conclude and maintain insurance in its own name at any time to cover the risks related to provision of the Performance, and to pay any premium that is adequate for such purposes and the value of which is usual on the market for the given risks, to the account of the provider. The customer is authorised to offset such amounts paid on behalf of the provider against any monetary receivables of the provider towards the customer, which are due or become due, or to recover these amounts as the provider's outstanding debt.

7. Subject, deadline, form and place of fulfilment of the Agreement, delivery conditions

7.1 The provider is obliged to provide the Performance according to the relevant Agreement.

7.2 The deadline, form and specific place of fulfilment are generally determined in the Agreement; if not stipulated in the Agreement, the place of performance is the customer's registered office; however, the provider is obliged to notify the potential delivery of goods or items within the performed work to the customer's registered office at least 5 business days in advance.

7.3 If the subject of Performance under the Agreement is the delivery of goods, delivery will be governed by the DDP delivery conditions according to Incoterms 2010.

8. Acceptance of Performance

8.1 The obligation to provide Performance is considered fulfilled if the Performance is duly provided and handed over by the provider and taken over by the customer.

8.2 Handover and takeover of Performance are carried out through Acceptance according to the procedure defined in the Agreement.

8.3 If the Performance corresponds to the agreed specifications and conditions set out in Art. 6.1 above, the customer will accept the Performance and indicate "Accepted" as the result of Acceptance in the acceptance protocol.

8.4 If defects in the Performance that do not prevent its Acceptance are found during Acceptance, the customer will accept the Performance and indicate in the acceptance protocol that the Performance is accepted with the reservation of the found defects; it will also indicate which defects were found in the accepted Performance or refer to a document containing a specification of these defects. The customer proceeds likewise if, at its own discretion, it accepts Performance in which defects were identified that prevent Acceptance of the Performance.

8.5 Regarding Performance that was accepted without reservations or with reservations, it is conclusively presumed that it was handed over by the provider to the customer and taken over by the customer from the provider on the date indicated in the acceptance

protocol. If physical takeover of the accepted Performance did not take place on this day, the customer will do so at latest within 5 business days, whereas the provider will provide all the necessary cooperation for this purpose. Unless agreed otherwise in the Agreement, the provider is obliged to eliminate the defects listed by the customer as reservations during Acceptance at latest within 10 business days from the day of Acceptance, indicated in the acceptance protocol.

8.6 If the fulfilment which was the subject of Acceptance does not correspond to the agreed specifications, contains defects and/or IT Security/Security defects that prevent Acceptance, the customer is not obliged to accept the Performance. If the customer refuses Acceptance of such Performance, it will indicate in the acceptance protocol that the Performance is not accepted, and is simultaneously obliged to indicate which defects in the Performance prevent Acceptance, or is obliged to refer to a document containing a specification of these defects. Acceptance of the refused Performance must be repeated without undue delay, assuming that the provider has removed the defects that prevented Acceptance. This does not affect the customer's other rights from defective Performance and/or from the provider's delay, which are listed in these business terms, agreed in the Agreement or arising from the relevant legal regulations.

The provider's Performance which is submitted for Acceptance with defects that prevent Acceptance is not considered proper, and the provider's obligation to deliver the Performance duly and punctually is not fulfilled by submitting such Performance.

8.7 Acceptance of documents

a) If the subject of Performance is the elaboration of a document, the customer is authorised to raise any comments regarding discrepancies between the submitted draft and the specifications of the Performance within the framework of its Acceptance.

b) The provider is obliged to deal with the customer's comments without undue delay and submit a new version of the document to the customer for approval, supplemented with a description of how the individual comments were handled. This procedure is repeated until all of the customer's comments have been dealt with.

c) Commenting of the document and processing of conditions does not affect the agreed deadline of Performance. The parties will record the individual versions of the document, comments that the customer had to them, and the manner of their handling in the acceptance protocol; they may also provide a reference to the respective documents describing the course of Acceptance in the acceptance protocol.

d) If the customer has no comments, or only has comments that do not prevent Acceptance, the document is accepted.

e) This procedure applies also to the Acceptance of source codes and/or approval of documents which are not directly the subject of Performance, but are to be created according to the Agreement, e.g. for elaborating detailed specifications of the Performance or elaborating the acceptance test specification.

8.8 Acceptance of the Performance by the customer in itself does not prove that the Performance was provided duly and does not preclude that the Performance may contain obvious or hidden defects. Defects in the Performance found or reported after Acceptance have the consequences described in Art. 6.3 above.

8.9 Acceptance of the Performance takes place exclusively by signing the relevant acceptance protocol or similar document by the designated person acting on behalf of the customer. Unless the Agreement explicitly stipulates otherwise, Acceptance of the Performance does not take place without fulfilling the aforementioned conditions, not even in consequence of the customer's delay, commencement of use of the Performance by the customer or in consequence of any other legal conduct (including inactivity) of the customer.

8.10 If the Performance includes documentation of the Performance and the Performance is modified within the Acceptance process, the provider is also obliged to deliver an updated version of the documentation at latest within 10 business days from Acceptance of the Performance.

9. Price, payment conditions

9.1 The price for Performance is stipulated in the respective Agreement.

9.2 If the provider is a VAT payer, it is obliged always to indicate the price for Performance without VAT, the VAT rate in the amount currently stipulated by law, and the price of Performance including VAT in all of its invoices and tax documents, offers or other materials related to the Agreement.

9.3 The price for Performance excluding VAT is stipulated as the fixed and highest permissible amount paid excluding VAT by the customer for the Performance, and as such includes all of the provider's costs related to the Performance, as well as any taxes and fees (apart from VAT), all risks (currency, inflation, etc.), customs duty, insurance, transport or storage costs, etc.

9.4 The provider is entitled to payment of the price for Performance after Acceptance of the Performance. The provider is not authorised to request an advance for the Performance or a reasonable part of the remuneration according to Section 2611 of the Civil Code, unless the parties agree otherwise in the Agreement. In the case of Performance divided into parts with partial payments, the price for Performance is paid after Acceptance of the respective part, to which the partial payment is bound. The provision of Section 2610(2) of the Civil Code is hereby precluded.

9.5 The Customer prefers electronic invoicing in ISDOC format. If the implementation of this format would be disproportionately costly for the Supplier, the PDF format is acceptable. Details of electronic invoicing, including format and transmission requirements, are set out in the Electronic Invoicing Agreement which forms an integral part of each Contract. The completed Agreement shall be sent by the Supplier to the following email address: fakturapdf@csas.cz.

9.6 Unless otherwise specified in the contract, invoices are due 30 calendar days from the date of delivery to the Customer.

9.7 All accounting documents must correspond to the valid and effective accounting and tax regulations of the Czech Republic, must contain the respective Agreement number and potentially the customer's SAP order (the structure of the invoiced items must correspond to the structure of the order). If the order is not confirmed by a written order, the name of the specific employee who placed the order must be indicated on the invoice and will also include an attached copy of the acceptance protocol or other protocol required by the Agreement, as well as the provider's account published by the tax administrator in a manner allowing remote access. Amounts paid by the customer to the provider will be paid via wire transfer exclusively to this account.

9.8 If the accounting document does not meet all of the aforementioned requirements, the customer will return such document within its maturity period to the provider, who will correct it and return it to the customer. If it is an accounting document based on which the customer is to pay any monetary amount, a new maturity period for this amount starts from the moment of delivery of a corrected document.

9.9 If the provider is given the status of an unreliable payer by decision of the tax administrator in the course of taxable fulfilment according to the provisions of the VAT Act, the customer is authorised to pay VAT from the provided fulfilment directly to the tax administrator instead of the provider, and subsequently pay the provider the agreed price for provided Performance reduced by this paid tax. The contractual parties consider this procedure to constitute the fulfilment of the customer's obligation to pay the agreed price, respectively part thereof.

9.10 If the Performance is subject to tax collected by deduction, the customer deducts the corresponding tax and pays it to the relevant financial bureau. The value of this tax will be stipulated based on confirmation of the tax domicile and declaration of the foreign entity for application of the respective agreement to limit double taxation, which forms an annex to the Agreement. For every such tax, the customer will submit to the provider a confirmation of the deduction and payment of this tax from the financial bureau. The provider is obliged immediately to submit updated confirmations and declarations concerning changes of the data in these documents. Furthermore, the provider is obliged to submit to the customer confirmation of its tax domicile always at the start of every new calendar year (at latest by 30th January of the given year) throughout the effective term of the Agreement. The provider is familiar and agrees without objections that if it fails to submit the confirmation of tax domicile or Declaration of a foreign entity, or does not submit it on time, the tax collected by deduction will be subject to the corresponding rate for this tax according to the legislation of the Czech Republic.

10. Contractual penalties and other sanctions

10.1 In the event of the provider's delay in providing the Performance or part thereof, or in removing defects within the agreed deadline, the customer is entitled to a contractual penalty in the amount of 0.5% of the total price for Performance according to the Agreement for every even started day of delay.

10.2 In the event of violation of any of the provider's obligations according to Art. 3.3 and 3.5, the customer is entitled to a contractual penalty in the amount of CZK 100,000 for any individual violation. This does not apply if these terms stipulate a special contractual penalty for any of the said cases.

10.3 In the event of a breach of any of the provider's obligations set out in Annex A and/or Annex B, the customer shall be entitled to a contractual penalty of CZK 2.5 million for any single breach of any obligation. If these conditions or the Agreement provide for a separate contractual penalty for any of these cases, only one of them, namely the special contractual penalty, shall apply.

10.4 In the event of violation of the obligation to protect Confidential Information or the nondisclosure obligation regarding Confidential Information according to the Agreement by a contractual party, the other contractual party is entitled to a contractual penalty from the other contractual party in the amount of CZK 1,000,000 for every individual case of violation.

10.5 Interest on arrears in payment of a rightfully issued invoice will be paid in the lawful amount.

10.6 The contractual penalties according to the Agreement are due within 30 days from delivery of a written request for their payment to the contractual party that is obliged to pay.

10.7 Discrepantly from Section 2050 of the Civil Code, the contractual parties have agreed that the arrangement of any contractual penalty will not affect the right to compensation of damages arising from violation of the obligation to which the contractual penalty pertains, and the claim to compensation of damages may be applied independently of the contractual penalty and in full extent. This does not apply if the Agreement explicitly stipulates otherwise.

11. Compensation of property and non-property losses

11.1 The relevant provisions of the Civil Code apply to the compensation of property losses (damages) and immaterial losses. Property losses are compensated in money, unless the parties agree otherwise in a specific case. The contractual parties declare that if damage to the customer's reputation or commercial name or other non-property loss occurs through violation of the provider's obligations, the provider will also pay the customer adequate satisfaction.

11.2 The customer is not obliged to undertake prevention exceeding standard care and caution, unless it is called on within the cooperation agreed according to the Agreement to exercise a higher degree or specific type of prevention.

11.3 The provider undertakes to compensate the customer for damages incurred through violation of the law, regardless of the provider's fault. During the provision of Performance, the provider is perceived as an entity liable for its own operation activity.

11.4 The provider is liable for the justified claims of third parties raised against the customer in connection to the Performance provided by the provider to the customer, and undertakes to compensate the customer for all damages arising therefrom.

12. Rights to copyrighted works and intellectual property

12.1 In relation the copyrighted work created for the customer based on the Agreement, i.e. based on the customer's specific requirements and/or assignment, the provider undertakes to have, at the latest at the time of handover such copyrighted work to the customer, the right to exercise all economic copyrights to such copyrighted work and the consent of the author(s) of such copyrighted work to assign all of this economic copyrights to the costumer. At the time of handover of the copyrighted work to the customer for Acceptance, the provider shall assign to the customer the right to exercise all of economic copyrights regarding such copyrighted work. In relation the all other copyrighted works, i.e. created not for the customer based on the Agreement, that are the subject of the Agreement or related to the Performance, the provider undertakes to have, at the latest at the time of handover such copyrighted work to the customer, the right to exercise all economic copyrights to such copyrighted work to the extent necessary to fulfill the purpose of the Agreement, At the time of handover of the copyrighted work to the customer for Acceptance, the provider grants the customer with exclusive rights to exercise all economic copyrights to such copyrighted work (license) to the extent necessary to fulfill the purpose of the Agreement, in particular the right to use the copyrighted work in any manner that comes into consideration, including the right to modify and change the copyrighted work. Within the granted license, it is stipulated that part of the customer´s right to modify and change the copyrighted work is as well the authorisation to exercise this right through a third party. Within the granted license, it is stipulated that the customer is authorised to use the copyrighted work and introduce it to the market without the need to indicate the authorship of the author(s), provider or any other party cooperating with the provider. The license is granted for the entire duration of the economic copyrights, without territorial or quantity limitations in the scope of use of the copyrighted work. By granting the license the provider confers the customer the right to sublicense the copyrighted work for third party and the right to assign the license to a third party in whole or in part. The provider hereby grants the customer express consent to such assignment and expressly waives his right to be notified of the assignment by the customer, for each individual case of such assignment. The copyrighted work according to this Art. 12.1 includes the complete documentation for the copyrighted work including the complete source code and all reference materials. The provider is obliged to hand this documentation over to the customer when commencing

Acceptance of the copyrighted work. The provisions of this clause apply also to the part of the Performance potentially delivered by a subcontractor, whereas if the provider does not have the right to exercise economic copyrights within the meaning of this Art. 12.1, in this case the provider is obliged to ensure the granting of all aforementioned rights to the copyrighted work (licenses) by the subcontractor directly to the customer.

12.2 All licenses to the copyrighted works provided within the Performance are provided without consideration, unless the value of remuneration is stipulated in the Agreement. The provider is fully liable to the customer for due settlement of the remuneration vis-à-vis the authors of all copyrighted works, which are used as part of the Performance.

13. Special provisions on IT deliveries

Without prejudice to other provisions of these business terms, the following special provisions shall apply for IT deliveries, which shall prevail in the case of contradiction between these special provisions for the IT deliveries and other provisions of these business terms.

13.1 Software development

a) If the subject of Performance is the software development by the provider for the customer, then the source code and/or executable artifacts creation and maintenance are performed directly in the designated Source code repository of the customer so that the Customer has direct control over the actual process of creating the source code and/or executable artifacts and their history; in this case, the customer is obligated to ensure appropriate access to the given Source code repository for the provider so that the provider can perform the required creation and maintenance of source code and/or executable artifacts in the Source code repository

b) If, for objective reasons (e.g. security restrictions, distance, etc.), it is not possible for the provider to create and maintain source codes and/or executable artifacts directly in the customer's Source code repositories, then the necessary minimum must be ensured and adhered, when the master software development branch is maintained in the customer's Source code repository and changes in the source code and/or executable artifacts are added to this main branch (merged) using Pull-request mechanism initiated by the provider, through:

(i) a secure integration circuit established between the Source code repositories of the customer and the provider or;

(ii) using import of source code from defined protected storage managed by the customer; in this case, the customer shall ensure that the provider has the necessary access to the given protected storage enabling the uploading of the source code and/or executable artifacts to the storage.

The transfer and merge of the source code and/or executable artifacts to the main development branches in the customer's Source code repositories is - regarding the effectiveness of development and its management - performed at least twice a day.

c)The provider shall deliver the generated source code and/or executable artifacts on an ongoing basis through the mechanisms specified in paragraphs (a) and (b) of this clause.

13.2 Security of the software

The source code and/or executable artifacts created by the provider must pass the standard security and quality tests proving the security, safety, and maintainability of the software being developed, at least to the following extent:

a) If the subject of Performance is the creation of source code, then at least vulnerability detection, static code analysis, documentation check, and possibly additional tests must be performed in accordance with the customer's internal software development rules, the current version of which shall be provided by the customer to the provider upon request without undue delay. If the development and maintenance of the source code are performed directly in the customer's Source code repository, see also paragraph 13.1.1 part a), safety and quality tests are performed automatically. Otherwise, the provider will ensure that the necessary security and quality tests are performed every time when the source code is handed over from the provider to the customer in accordance with the customer's requirements and policies.

Unless otherwise specified in the Agreement, the same rules apply for security and quality tests as for Acceptance under Article 13.3.

b) If the deliverable is an executable artifact, then the handed-over artifact (or artifacts) must pass the security tests prescribed by the customer's internal policies and rules for software development, at the latest during the handover of the artifact by the provider

to the customer. If the development and maintenance of the source code and the resulting artifact are performed directly in the customer's Source code repository, see also paragraph 13.1.1 paragraph part a), security and quality tests are performed automatically. Otherwise, the provider will ensure that the necessary security and quality tests are performed every time when the artifact is handed over by the provider to the customer. If the artifact is created exclusively for the customer, the source code of the artifact must be handed over as well. In the case of generic software or software that is provided in the same form to multiple customers of the supplier, this obligation is waived. This obligation under the immediately preceding sentence shall not apply in the case of COTS Software.

Unless otherwise specified in the Agreement, the same rules apply for security and quality tests as for Acceptance under Article 13.3.

13.3 Acceptance

Handover and takeover of the Performance in form of SW are carried out through Acceptance according to the procedure defined in the Agreement, in case that the Acceptance is not described in the Agreement, the customer will carry out the acceptance tests pursuant to these business terms.

The provision of Art 8.7 shall apply for the specification of acceptance tests in an appropriate manner. If the Agreement does not envisage a creation of acceptance tests, the customer is entitled to verify the lack of defects in the Performance in any reasonable manner.

The following rules for Acceptance apply unless the Agreement stipulates other rules for acceptance tests:

a) The acceptance tests are carried out by the customer with participation of the provider in accordance with the acceptance tests specification. The customer has to be informed about the start and time of the acceptance tests at latest 5 business days in advance and the provider is obliged to ensure the participation of its representative. In case of absence of the provider´s representative, the customer is not obliged to carry out acceptance testing.

b) Unless the acceptance tests specification stipulates otherwise, the result of acceptance tests is considered successful if: no Defect A-level and no more than 5 Defects of B-level and no more than 5 Defects of C-level were discovered. The categorization of defects is governed by these business terms. In case of doubts regarding the defect category, the customer makes the final decision.

c) The successful result of acceptance test does not deprive the customer of its rights stipulated in these business terms, agreed in the Agreement or arising out of relevant legal regulation in case that defects of Performance will be discovered in the future, irrespective whether these defects were discoverable within the Acceptance or not.

d) The result of individual tests shall be recorded together with the list of discovered defects in an acceptance protocol. If the result is not successful, the provider is obliged to remove the causes of such result without unreasonable delay and to repeat the tests. This procedure shall be repeated until the successful result of test is reached.

e) The acceptance testing and removal of defects that prevent to the Acceptance has no impact on the agreed term of Performance.

13.4 **Defects categorization**

Unless otherwise stipulated in the Agreement, the defect categorization is as follows:

a) Defect A-level: a defect, which entirely or substantially prevents to the use of the Performance.

b) Defect B-level: a defect which does not prevent the use of the Performance but restricts its use; this includes also workarounds of Defect A-level.

c) Defect C-level: a defect which is not a Defect A-level or a Defect B-level, this includes also workarounds of Defect B-level.

13.5 Assurance of support of COTS Software and Hosted software

Analogically to the provision of Art. 6.6, the provider is obliged to assure that the support of the producer, service provider or alternative performance of another person shall be provided in connection to the COTS Software and/or Hosted software at least for the period of 5 years from the later of the following: the date when the license or sublicense to COTS Software was granted or from the moment of its launching into operation.

The delivered COTS Software and/or the provided Hosted Software must pass the relevant security test proving the safety of the given software for the customer's environment when they are handed over by the provider to the customer.

13.6 Rights to Software

a) In relation to the COTS Software the license terms to use the copyrighted work are specified in the respective Agreement. If the license terms are not specified in the respective Agreement, the provider is obliged to get the customer provably acquainted with these license terms before the provision of the Performance, and the customer has the right to withdraw from the Agreement without any sanction if the provider fails to fulfil this obligation. Until the provider get the customer provably acquainted with the license terms to use related to the COTS Software not specified in the respective Agreement and until the customer will not express its written consent with the license terms to use related to the COTS Software not specified in the respective Agreement, the customer may not require to fulfil any obligation arising for him from the respective Agreement. The arrangement of the previous sentence does not affect the rights of the customer arising for him from the respective Agreement or the obligations of the provider stipulated therein. Unless it is agreed otherwise in the Agreement, the license terms of the COTS Software have to enable the use of the Performance, whose part is formed by the COTS Software, for the purpose followed by the Agreement and they may not (in comparison to the copyrighted work regulated by Art. 12.1.) restrict the customer´s usage right without reasonable cause.

b) The extent of the license to the custom-made Software created for the customer based on the Agreement and the obligations of the provider in relation to such Agreement is governed by Art. 12.1. Unless stipulated otherwise in the Agreement, the source code of the custom-made SW created for the customer shall be the part of such Performance, including programming/coding notes, complete documentation and data (including e.g. complete programming/coding repository records). During development and creation of the source code, notes and relevant documentation and data according to the previous sentence, the provider is obliged to comply with standards customary in the given industry, that enable clear comprehension and modification of the source code by a professional other than provider.

c) If the delivered copyrighted work is custom-made Software and/or Hosted software, the provider is obliged upon a request from the customer to conclude an agreement with the customer on maintenance of the copyrighted work, for which the customer was granted the rights under the relevant Agreement. The provider is obliged to offer a price for software maintenance under the usual conditions on the market. For the purposes of the Agreement, this obligation of the provider is considered a fundamental obligation and its violation constitutes a substantial breach of the Agreement, which represents a reason for withdrawal from the Agreement by the customer.

d) If the contractual parties do not conclude an agreement on software maintenance, or if such agreement expires, or if the provider's business activity in the area of IT is terminated, or if reasons are given for withdrawal from the Agreement, the customer is authorised to perform maintenance of the software itself or procure the maintenance of software from a third party.

13.7 Some consequences of a breach of the IT delivery Agreement

13.7.1 The customer is authorised to withdraw from the Agreement according to the provision of Art. 17.3 of the business terms, if the provider repeatedly (i.e. at least two times) in 12 consecutive calendar months breached the SLA related to the Performance.

13.7.2 In the event of violation of the obligation to hand over the source code to the copyrighted work, which is part of the Performance pursuant to Art. 13.4(b), the customer is entitled to a contractual penalty from the provider in the amount of 200% of the price of the copyrighted work according to the relevant Agreement.

13.8 Use of free and open source software for Performance

13.8.1. If a software or a part thereof that fulfils the characteristics of free software or open source software constitutes a part of Performance, the Contractor shall notify the Customer in writing and request Customer's written consent to use the free software and / or open source software. Written information about the intention to use free software and / or open source software under the preceding sentence shall always include the specific designation of the software and / or parts thereof which fulfil the features of free software and / or open source software and which constitute a part of Performance and specify the license terms governing the use of the free software and / or open source software.

14. Protection of Confidential Information

14.1 In connection to the provision of Performance, both contractual parties will exchange Confidential Information. Each contractual party is obliged to protect Confidential Information of the other party against leakage and unrightful use and undertakes not to use it for purposes other than those arising from the Agreement. The Confidential Information of one contractual party may be used by the

other contractual party exclusively to prepare and provide the Performance according to the Agreement, unless stated otherwise in the Agreement.

14.2 Unless stated otherwise, by concluding the Agreement neither contractual party grants the other contractual party the right to use its copyrighted works, trademarks or other brands for the purpose of promotion or publication or for any other purposes. The provider is not authorised to list the customer as a reference customer within the provider's activity without prior written consent from the customer.

14.3 Each contractual party is obliged to keep confidentiality regarding the Confidential Information of the other party, and to adopt adequate contractual, technical and organisational measures to protect the other party's Confidential Information.

14.4 Each contractual party undertakes that they will not duplicate the Confidential Information, which was provided to them by the other contractual party in relation to providing the Performance or during preparations to provide the Performance, in any manner, with the exception of cases when this is required in order to provide the Performance according to the Agreement, and to return it upon request at any time to the other contractual party, including all potential created copies and carriers of the Confidential Information, or to destroy it based on a request from the other contractual party, including all potential created copies and carriers of the Confidential Information.

14.5 Neither contractual party may provide the received Confidential Information in any form to third parties without written consent from the other contractual party, with the exception of the other authorised user of Confidential Information of the given contractual party. Each contractual party undertakes to ensure that its authorised users of Confidential Information will keep confidentiality regarding the Confidential Information. If the authorised user of Confidential Information violates the contractual obligation to keep confidentiality regarding the Confidential Information of the other contractual party, this will be considered a violation of the nondisclosure obligation by the said contractual party.

14.6 It is not considered a violation of the nondisclosure obligation if the contractual party is obliged to disclose the Confidential Information based on an obligation arising from legal regulations. However, the contractual party is obliged to inform the other contractual party about this in advance, if possible, unless this is disallowed by the given legal regulation, and simultaneously to limit the disclosed Confidential Information to the absolutely necessary scope subject to the disclosure obligation.

14.7 The contractual parties are obliged to inform each other of violation of the nondisclosure obligation or protection of Confidential Information without undue delay after they learn of such violation.

14.8 The nondisclosure obligation and protection of Confidential Information according to these terms, including the sanction provisions, remain effective regardless of the termination of validity or effectiveness of the Agreement, for a period of at least 10 years after its termination. In case of information protected as banking secrecy, the obligation of the provider shall last for unlimited period of time.

14.9 In case a non-disclosure agreement related to the Performance is concluded between the contractual parties (hereinafter referred to as "NDA"), in the event of contradiction between the NDA and the provisions of these business terms, the NDA shall prevail.

15. Protection of personal data

15.1 If during provision of the Performance the provider processes any personal data, in the meaning of GDPR, for the customer which is the controller according to the GDPR, the provider will become the processor of this personal data according to the GDPR for the purposes of the Agreement. When processing personal data, the contractual parties are obliged to proceed in accordance with the GDPR. In such a case, the provider undertakes, before starting of processing of personal data, to conclude a personal data processing agreement with the customer in order to meet the GDPR requirements, and in the performance of the Agreement, the personal data will be processed only in the manner specified in the relevant agreement for the processing of personal data.

15.2 The provider is obliged to get acquainted with the Principles of personal data processing of the customer. In the event that in connection with the performance of any Agreement the provider provides the customer with personal data within the meaning of GDPR, for which the provider is the administrator under GDPR, the provider is obliged to inform, without undue delay, the relevant personal data subjects about start of processing of their personal data by the customer and acquaints them with the content of the Principles of personal data processing of the customer.

16. Artificial Intelligence

16.1 If the provider uses an artificial intelligence system within the scope of performance under the Agreement, the provider undertakes to comply with the Code for the Use of Artificial Intelligence and the Extended Code for the Use of Artificial Intelligence, which form an annex to the Contract, as well as any instructions of the customer concerning the use of artificial intelligence systems, which the provider submits to the customer or makes known to the customer.

16.2 The above Codes may be reasonably amended by the customer within the meaning of Section 1752 of the Civil Code, whereby the customer shall notify the provider of such amendment at least 30 calendar days in advance via the provider's email, provided that the provider shall have the right to reject such amendment and terminate the Agreement with a notice period of 6 months, commencing on the first day of the first month following the month in which the notice is received and ending on the last day of the last month of its duration. During the notice period, the provider's rights and obligations shall be governed by the previous Code in force and now superseded. During the notice period, the provider shall, inter alia, comply with the requirements set out in Annex A II. Digital and Operational Resilience, specifically the conditions governing the termination of the Agreement and the handover of the provision of the Performance to a new provider.

16.3 The provider shall act in such a way that the use of the AI system does not breach the Agreement and does not damage the interests or reputation of the customer. The provider shall only use AI systems for purposes that comply with the Law and this Agreement.

16.4 The provider shall comply with the principle of transparency and if the performance to be delivered or provided to the customer under the Agreement is created or co-created by artificial intelligence systems or if such performance includes artificial intelligence systems, the provider shall always inform the customer in writing in advance, including information on whether the provider is a provider or user of an artificial intelligence system or tool, the particular artificial intelligence system involved, the nature of its operation, the conditions of its use and any risks.

16.5 In the event that the provider is to grant a licence or sub-licence to the customer for the subject of performance under the Agreement, or is to assign the exercise of copyright to the customer, the provider shall ensure that the customer is authorised to do so with respect to the involvement of an artificial intelligence system or the use of an artificial intelligence tool.

16.6 The provider shall comply with the rules of personal data protection in the sense of the GDPR as well as the rules of data protection and cyber security when engaging artificial intelligence systems or using artificial intelligence tools.

16.7 The provider will engage and use ethical, technically robust and safe artificial intelligence systems that promote diversity, equity and prevent discrimination.

16.8 The provider shall only use AI systems that respect the copyright and intellectual property of third parties. In connection with the use of AI systems, the provider shall guarantee human supervision by trained persons throughout the period of use.

16.9 The provider shall be liable to the customer as if it had provided the performance created or co-created by the AI system itself and undertakes to fully indemnify the customer for breach of the obligations set out in this provision of the Agreement.

17. Cooperation of the contractual parties, management of provision of Performance

17.1 The contractual parties are obliged to inform each other of all fundamental circumstances that could have an impact on the provision of Performance, e.g. about ownership or other changes on the part of the provider and all other relevant circumstances that are important for fulfilment of the obligations from the Agreement. Important changes concerning contact data including e-mails, changes in the commercial name, registered office address, bank account number, etc. or circumstances that could have a negative impact on the provider’s ability to duly provide the Performance must be reported by the provider to the customer in writing immediately.

17.2 Each contractual party will appoint responsible representatives for contractual and technical matters.

17.3 The customer’s responsible representative is authorised to control the quality of the Performance and adherence to the conditions of Performance according to the Agreement, but is not authorised to alter the Agreement in any manner on their own.

17.4 During provision of Performance, the responsible representatives of the contractual parties are responsible, among other, for mutual communication between employees, cooperating persons and other responsible representatives of the contractual parties, for the specification of potential defects, for the definition and expression of requests and for Acceptance of the Performance.

17.5 In the course of implementation of each Agreement, the contractual parties undertake to not change their responsible representative without serious reasons. The contractual party changing its responsible representative undertakes to inform the other contractual party immediately in writing about the intent to change its responsible representative.

17.6 Any information, notices and correspondence that are to be disclosed by one contractual party to the other contractual party will be considered duly delivered if they are delivered in person to the other contractual party's responsible representative, and this person confirms takeover with their signature and/or if they were sent via registered mail to the address of the contractual party set out in the Agreement.

17.7 The provider shall notify the Customer with sufficient advance about any changes in data processing, the provision of ICT functions and services provided by the Provider (especially the transition to a cloud solution, change of a cloud service provider, change of the location of data processing or storage compared to the location agreed in Contract) and further about changes that may result in reduced security or stability of the service provided, e.g. reduction in quality of IT security, change of operating system, change in access rights settings, significant decrease in HW performance, change in contingency plans (e.g. geographical change of back-up solution), loss of the originally declared certification.

18. Termination of the Agreement and consequences of terminating the Agreement

18.1 It is possible to withdraw from the Agreement under the conditions stipulated by the relevant legal regulations, these business terms or the relevant Agreement. Withdrawal from the Agreement does not affect the validity or effectiveness of other contracts, unless the Agreement stipulates otherwise.

18.2 Withdrawal is effective from the date of delivery of written notice of withdrawal to the other contractual party. In the case of the customer, withdrawal is executed without undue delay, if delivered to the provider within 3 months from the moment when the customer learned of the reason for withdrawal.

18.3 The customer is authorised to withdraw from the Agreement, without any limitation of its rights to withdrawal according to legal regulations, in particular if:

a) the provider delays in fulfilling its obligations from the Agreement, despite a written warning from the customer and provision of an additional deadline of at least 7 days from delivery of the warning to the provider;

b) the provider delays in removing defects in the Performance by a period more than two times the deadline stipulated by the Agreement or these business terms to remove defects, despite a written warning from the customer and provision of an additional deadline of at least 1/2 of the basic deadline;

c) there are deficiencies regarding the management and security of the customer's data or information by the provider;

d) constraints are identified that may significantly alter the performance of the outsourced function;

e) there have been significant changes that may materially affect the provision of the provider 's services;

f) required by a remedial measure or other decision imposed on the customer by the state supervisory authority.

18.4 The provider is entitled to withdraw from the Agreement particularly if the customer delays in paying the price for duly provided Performance for more than 30 days, despite a written warning from the provider and provision of an additional deadline of at least 14 days from delivery of the warning to the customer.

18.5 The termination of effectiveness of any Agreement does not affect the validity and effectiveness of the provisions of the Agreement (including the provisions of these business terms), which given their nature are to remain intact even after expiry of such Agreement, in particular those concerning:

a) the provision of user rights or rights to execute the customer's copyright to the copyrighted work or subject of industrial property after acceptance of the relevant Performance or part thereof, if such Performance remains in the customer's use even after expiry of the Agreement;

b) warranties on the quality of Performance and claims from the provider's liability for defects in the Performance;

c) protection of Confidential Information;

d) contractual penalties, interest on arrears or compensation of damages;

e) choice of the law, venue and other aspects of solving disputes between the contractual parties.

18.6 If a reason for withdrawal exists, the customer is authorised to withdraw from the Agreement in full scope, even if the provider has already provided partial fulfilment from the Agreement or if the Agreement bound the debtor to perform uninterrupted or repeated activity or provide gradual partial Performance.

18.7 The provider takes into account that if the Performance constitutes outsourcing in the meaning of the regulations that the customer is obliged to follow, the provider undertakes to adhere to the rules set out in Annex A to these business terms. The text of Annex A shall always take precedence in case of conflict with the text of these General Business Terms of Cooperation.

18.8 The customer is authorised to amend Annex A unilaterally in the event of changes in legal regulations, so that Annex A complies with the change in legal regulations. Such change of Annex A shall be notified by the customer to the provider immediately after its change.

19. Audit

19.1 The customer shall be empowered to audit the accuracy of Performance and compliance of Performance with legal and regulatory requirements related to the Performance.

19.2 The customer shall send the provider a written notice of intent to audit no later than 14 days before the intended audit. In the case of an audit requested by a competent supervisory authority (in particular the CNB), the notice of intent to audit may be sent within a shorter period of time.

19.3 The provider shall provide all necessary assistance to carry out the audit.

19.4 The customer may entrust another entity to carry out the audit. The customer undertakes that the entity commissioned by the customer to carry out the audit is not an entity in a competitive position vis-à-vis the provider.

19.5 The audit should not exceed the necessary period of time.

19.6 The customer or its empowered person or company will not have access to information concerning the provider's other customers, the provider's costs for providing services or the provider's internal costs or personal data, which are the subject of legislative or any other regulatory protection, as well as copies of internal inspections and audits (with the exception of those required by legal regulations). This does not apply for audits conducted at the request of or directly by the CNB or according to its explicit instructions or requests or to an audit of such Performance that is considered banking outsourcing or third party ICT service provision under DORA.

20. Governing law and solving disputes

20.1 The Agreement is concluded under and the obligations of the parties from the Agreement are governed by the legal code of the Czech Republic.

20.2 All disputes between the contractual parties arising from the obligations established by the Agreement or in relation to them will be resolved by negotiation of the parties, which will exert maximal efforts to reach an amicable solution. If the contractual parties fail to reach an amicable solution to such dispute through mutual negotiations, the given dispute will be resolved with final validity by the general courts of the Czech Republic. The parties agree on local jurisdiction of the court based on the customer's registered office.

21. Final provisions

21.1 Neither of the contractual parties is liable for damages, if it was temporarily or permanently prevented from fulfilling the obligations from the Agreement by an extraordinary unforeseeable or insurmountable obstacle that arose independently of its will. An obstacle arising from the personal or internal situations of the contractual parties or only after the contractual party was in delay in fulfilling the agreed obligation, or an obstacle that the part was obliged to overcome under the Agreement, does not relieve it of its obligation to compensate damages. Delays by subcontractors or the existence of the aforementioned obstacle on the part of the subcontractor does not relieve the provider or liability for damage incurred in this connection.

21.2 The provider is not authorised to transfer any of its rights or obligations from the Agreement to a third party without prior written consent from the customer.

21.3 The individual provisions of the Agreement and these business terms are severable in the sense that the invalidity, nullity or unenforceability of any of them will not cause the invalidity, nullity or unenforceability of the Agreement or business terms as a whole. The parties undertake, without undue delay, to replace by agreement such provisions of these business terms of the Agreement, which are contrary to legal regulations or are null or unenforceable according to the relevant legal regulations.

21.4 The rights and obligations not explicitly regulated in the Agreement are governed by the provisions of these business terms and the provision of the relevant legal regulations of the Czech Republic. In the event of contradiction between the provisions of the business terms and Agreement, the provisions of the Agreement always take precedence.

21.5 The concluded Agreement may be altered or supplemented only by written numbered amendments signed by both contractual parties, unless explicitly agreed otherwise. The names and data of the responsible representatives, contact persons and contact data of the contractual parties, including the invoicing address, may be altered by unilateral written notice sent to the other contractual party.

21.6 The following documents form an integral part of the business terms:

Annex A – I. Banking Outsourcing and II. Digital and operational resilience

Annex B – Resolution and Resilience

Annex C - Codes of conduct for the use of Artificial Intelligence

ANNEX A
BANKING OUTSOURCING AND DIGITAL OPERATIONAL RESILIENCE

I. Banking outsourcing

1. Provider takes into account, that rendering of services to the customer might be qualified as a banking outsourcing according to the Decree No. 163/2014 Coll., on the performance of the activity of banks, credit unions and investment firms ("the Decree") and EBA Guidelines on outsourcing arrangements („EBA Guidelines").
2. For this purpose the provider undertakes to accept rules set down by the Decree that might be elaborated in detail in this Annex or in any agreement meeting the requirements for the rendering of outsourcing concluded between the provider and the customer.
3. Person performing screening, inspection or audit is obligated to adhere to all provider´s security measures, with which will the customer be provably made familiar with.
4. Provider undertakes to cooperate and enable the customer (eventually the Czech national bank [„CNB"]) for the purpose of meeting the requirement set down by the Decree especially the following:

a) The provider check before and during the rendering of Performance – including in particular a check of credibility, entrepreneurial license or other license to exert given activity, professional qualification and experience, financial stability and qualification to assure Performance.

b) Regular inspections of the provider – including in particular:

- verification whether the Performance is permanently rendered in compliance with all applicable law regulations, commercial terms and Agreement,
- verification whether the provider remains trustworthy and legally, financially, professionally and technically qualified to render the Performance,
- verification whether the provider regularly verifies functionality and sufficiency of his mechanisms of internal control mechanisms and risk management including the risk management of occurrence of extraordinary events, which might have significant negative effect on due rendering of Performance. The customer undertakes to take into account in reasonable measure written suggestions about risks from the provider regarding the Performance, and to accept suggested measures to minimize them, assuming that this doesn't transfer duties of the provider to prevent risks on the customer in unreasonable extend,.
- verification whether the protection of bank secrecy and the customer´s clients´ personal data is secured permanently and sufficiently,
- verification whether there are violations of customer´s internal principles and procedures while rendering the Performance,
- verification whether provider´s internal control mechanisms secure timely recognition of incidental faults of the Performance, implementation of remedial measures, overall functionality and effectiveness of the Performance,
- evaluation of Performance´s compliance with the Decree
- verification whether the provider implemented and maintains at least such management and control principles and mechanisms which in comparison with similar rules of the customer provide at least a comparable level of quality and reliability.

The provider undertakes within the regular inspection to provide cooperation and enable access to data and other information regarding the Performance, including the access to primary information and consequential data, to verify the correctness of processing of primary information, if such processing is a part of the Performance.

c) Inspections of IT security aspects, including in particular the undertaking of the provider to

- provide the customer with documents (in form allowing its permanent storage) containing description:
  - of security strategy (including main principles to ensure the confidentiality, integrity, classification and availability od data),
  - of relevant internal regulations, e.g. security policy, description of security organization including the divisions of powers and responsibilities,
  - of solutions of security incident, incl. the obligation to clarify security incidents without undue delay, and related documents from the IS security area, backup, versioning of pertinent regulations (security policy), proof of publication of changes, auditing and archiving of security incidents at least 5 years after resolving security incident,
  - of personnel policy, including the method for employees screening and ensuring confidentiality, user management, staff training, carried out of reviewing and evaluating the safety of IS, etc. purchase, exchange, cancelling HW / SW including safe disposal of data, etc.,
- provide the customer with the description of specific architecture solution of the rendered Performance, including settings of security parameters in individual components and units
- establish reporting, including communication channels, communication matrix, deadlines etc. on security incidents, planned changes in architecture, communication.

d) Inspections of Physical security aspects, including the undertaking of the provider to

- render the Performance in compliance with the generally recognized standards (e.g. ISO, EN , PCI, DSS, etc.) listed in the Agreement. The provider shall inform the customer about any and all changes in his certification or about any new certification, including its scope and duration.
- provide the customer with a list of his assets (buildings, systems and equipment) relevant to the rendering of Performance and keeping this list up to date. If the assets (buildings, systems and equipment) do not meet the agreed standards and requirements of the customer, the provider must identify discrepancies and both parties must agree to resolve them,
- enable and support the customer in independent verification of the safety of the rendered Performance, including regular and accidental safety inspection of assets (buildings, systems and equipment) relevant to the rendered Performance,
- inform the customer in advance of any scheduled change in the security level of the rendered Performance. If the change is unscheduled the provider informs the customer about change immediately after identifying such changes,
- keep records of safety-related facts / events that may affect the security of rendered Performance to the customer. The records must apparently state what, where and when the event took place, what was the impact of the event and what measures were taken in response to this incident. In case that the event will threaten the safety of the Performance, the provider shall immediately inform the customer. The records must be kept in a way that prevents any subsequent modification. The records must be kept throughout the duration of the contract and at least another 5 years after termination of the contractual relationship.
- enable the customer to review records relating to the safety of the rendered Performance to the customer,
- hand over the entire list of the subcontractors used in the outsourcing of the rendered Performance (HW, SW equipment or support having access to data) to the customer. If changing the aforesaid list, the contractor must provide the customer with a up to date list of subcontractors,
- enable the customer to review data and information relating to subcontractors (similarly the representatives acting on their behalf) in the event of chain outsourcing and the fact that cooperation with them is not in conflict with prudential rules of the customer (legislation, directly applicable legislation of the European Union, etc.). The contractor undertakes to negotiate in contracts with subcontractors the possibility of immediate termination of cooperation with the subcontractors, if the prudential rules of the customer require so,
- prove, that his subcontractors apply at least the same security requirements as the contractor and that their compliance with these requirements is regularly inspected and maintained.

e) Audit performed by the customer and CNB and inspection of CNB – including

1. an audit of financial statement ;
2. an audit of the governance including the reports on performed inspections ;
3. eventually the accessing of reports on performed inspections carried out under a) and b);

The provider shall annually forward to the customer its annual balance sheet (compiled in compliance with Czech Accounting Standards) certified by the auditor previously agreed by the customer together with the corresponding auditor's report for the past financial year, as soon as he will have them available but no later than 180 days after the end of the reporting period. Default in aforesaid obligation constitutes a material breach of provider´s contractual obligations and the customer is entitled to withdraw from the contract with the provider;

5. Provider agrees to allow checks, inspections or audits carried out in order to meet the requirements of the Decree, (including monitoring the objective correctness of the provided outsourced activities) by employees of the customer, CNB, or a third party appointed or authorized by the customer, even at the registered office of the provider or other places of the Performance (even if they are abroad.
6. Provider agrees to notify the customer in advance of any changes that adversely affects or could adversely affect rendering of the Performance (e.g. ownership, organization, or asset structure, financial liabilities, risks, change in legislation) and all relevant data and other information relating to activities carried out under agreement.
7. The provider shall notify the customer with sufficient advance about changes in data processing (especially the transition to a cloud solution, change of a cloud service provider) and further about changes that may result in reduced security or stability of the service provided, e.g. reduction in quality of IT security, change of operating system, change in access rights settings, significant decrease in HW performance, change in contingency plans (e.g. geographical change of back-up solution), loss of the originally declared certification. In the event that the provision of services to the customer is considered a banking outsourcing within the meaning of Article 1 of this Annex, this provision replaces the provision of Article 17.7 of the General Business Terms and Conditions of Cooperation in the Area of Procurement of the Financial Group of Česká spořitelna and / or other provisions of similar meaning and purpose.
8. Provider shall establish at least such risk governance procedures and control mechanisms, which the customer would use in accordance with its guidelines for governance, if the customer would assure the Performance by himself. Upon

customer´s request the provider will allow the customer access to the documents containing the required procedures and control mechanisms. The provider is obliged to ensure notification of all reports of all operational risk events associated with rendering of the Performance for which the potential loss exceeds the limit of EUR 1000 via e-mail sent to oprisk@csas.cz. Reports shall in particular include the following:

- Place and date of the event occurrence
- Brief description of the event
- A contact person who is informed about the even
- Claim amount (if unknown at the time of notification, then its qualified assessment)

9. Provider shall perform an annual risk assessment, containing a description of the risks in activities that are rendered to the customer, including an evaluation of their potential impact. The customer has the right to request output information from the risk assessment or eventually participate in it. If the provider has no standard risk classification system, the provider may ask the customer for cooperation on risk assessment activities related to the rendering of Performance for the customer. The Customer will provide cooperation and will recommend his standards, which will be without undue delay implemented by the provider. The provider further undertakes to provide the customer with a processed risk analysis (depending on the offered supply of Performance);

10. Provider undertakes to prepare a business continuity plan, i.e. documentation for the case of threats to the availability of supply of the Performance due to extraordinary events, and this documentation, respectively its resume in accordance with internal regulations and confidentiality undertakings shall be made available by the provider to the customer within 3 months after conclusion of the Agreement. The customer undertakes to use the aforesaid information exclusively for his internal use and for processing of extraordinary procedures in connection with the subject of the Agreement. The customer shall arrange with the provider a minimum scope of renewed supply of Performance, that might be accepted by the customer as the renew of the Performance in partial scope;

11. Provider declares that he will continuously develop and improve measures to ensure the minimization the risk of interceptions of the Performance supply and that he has at his disposal sufficient backup capacities for renewal of Performance supply. The provider agrees with the presence of a provider´s representative while testing of business continuity plan and other documentation prepared by the provider to ensure continuity of the Agreement´s subject.

12. Provider undertakes to notify the customer in advance of the necessity of ensuring the rendering of Performance, whether wholly or partly by another entity (hereinafter the „outsourcing chain") and will ask a prior consent of the customer with the usage of such entity. The agreement concluded between the provider and aforesaid further entity shall conform to the principles and rules laid down in this Annex. The provider shall ensure and provide all the necessary and required cooperation and cooperation of another entity in the event that the customer or the CNB is authorized to carry out the aforementioned control activities also at the other entity.

13. If a breach of contractual obligations by the provider, or eventually other entity in the outsourcing chain is a consequence of imposition of penalties by the Czech National Bank on the customer, then the customer is entitled to demand pro rata payment of such penalties by the provider according to his culpability (including negligence). The compensation of penalties imposed by the CNB on the customer, does not limit the customer´s claim for compensations against the provider of all provable damages resulting from breach of the contractual obligation by the provider to which the CNB sanctions applied.

14. Unless otherwise stated in the Agreement, the customer is entitled to withdraw from the Agreement in the event of a serious breach of provider´s obligations listed in the provisions of this Annex or in cases in the cases referred to in Article 98 of the EBA Guidelines, in particular:

    a. where the provider of the outsourced functions is in a breach of applicable law, regulations or contractual provisions;

    b. where impediments capable of altering the performance of the outsourced function are identified;

    c. where there are material changes affecting the outsourcing arrangement or the service provider (e.g. sub-outsourcing or changes of sub-contractors);

    d. where there are weaknesses regarding the management and security of confidential, personal or otherwise sensitive data or information; and

    e. where instructions are given by the institution’s or payment institution’s competent authority, e.g. in the case that the competent authority is, caused by the outsourcing arrangement, no longer in a position to effectively supervise the institution or payment institution.

    The customer by himself is entitled to assess the seriousness of the breach and either provide the provider with additional reasonable remedy period, or to withdraw from the Agreement in question with effect since the time of delivery of the withdrawal. The customer may also withdraw from the Agreement if so required by remedial measures by the CNB.

15. Provider is required to take into account written recommendations from the customer concerning the risks associated with rendered Performance and take measures to minimize them, the customer undertakes to use the information and audit findings solely for his internal use and communication between the customer and the provider.

16. In the event of termination of rendering of the Performance the provider is obliged to provide full cooperation to the customer with transferring of performance back to the customer or to a third entity appointed by the customer in order to ensure continuity of activities even after the termination of the Agreement. The aforesaid cooperation also includes the obligation to transfer all data and information to the customer related to the Performance in a format specified by

the customer, transfer of all relevant documents and further steps leading towards the acquisition of rendering of the Performance by himself (or third entity).

17. Unless stated otherwise in the Contract, all data provided to the provider shall constitute the property of the customer, who may at any time request their return. This applies in particular to, but is not limited to, insolvency or imminent insolvency of the provider.

18. Unless stated otherwise in the Contract, provider shall store all data on the territory of the Member States of the European Union.

II. Digital and operational resilience

1. The provider acknowledges that the Performance for the customer may be deemed to be the provision of third party ICT services supporting essential or critical functions under Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector ("**DORA Regulation**").

2. For this case, the provider undertakes to accept the rules set out in the DORA Regulation, which may be elaborated in more detail in this Annex (or any other Annex to the Agreement) or in any contract fulfilling the prerequisites for the provision of third-party ICT services concluded between the provider and the customer.

3. Unless these business, including the Annexes, or the Agreement of which these General Business Terms of Cooperation ("**Contract Documents**") are a part, expressly provide for certain DORA Regulation requirements (in particular requirements pursuant to Article 30 of the DORA Regulation), the provider undertakes to accept and fulfil the DORA Regulation requirements with respect to the customer without reservation.

4. If any requirement of the Contract Documents is found to be in conflict with the requirements of DORA Regulation (in particular under Article 30 of DORA Regulation), the requirement of the Contract Documents shall apply to the extent that it does not conflict with the requirements of DORA Regulation. To the extent that there are conflicting requirements, the DORA requirement shall apply.

5. ICT functions and services provided by the provider or other subcontractor may only be provided from within the European Union, unless otherwise agreed in the Agreement. Unless expressly stated in the Contract Documents, the provider undertakes to inform the customer, at the latest prior to the signing of the Agreement, of the locations, including regions and countries, from where the contracted or provided ICT functions and services are provided and where the relevant data are processed, including where they are stored, including such locations in relation to subcontractors.

6. If part of the Performance is provided by a subcontractor, the provider shall be liable to the customer for the performance of the Performance by the subcontractor as if it were performed by the provider itself.

7. The provider undertakes to act with professional care in providing the Performance and to perform its obligations agreed in the Agreement and these business terms in a proper and timely manner.

8. For the purpose of complying with the requirements of DORA Regulation, the provider agrees to :

    a) Regularly update and revise the description of all ICT functions and services specified in the Agreement, including all material information about the services provided and their functionality, including an accurate assessment of qualitative and quantitative performance targets for the levels of services provided, so as to enable the customer to monitor the provision of such services and the achievement of such targets efficiently and to take corrective action;

    b) the provider undertakes to inform the customer of any changes to these ICT functions and services, including the location from which the Performance is to be provided and where all data and information is to be processed and stored, and any necessary and intended changes must be communicated in writing to the customer well in advance, at least 60 days before the intended change, and include a detailed description:

        - proposed changes,
        - reason for its introduction,
        - the expected impact on the services provided (quality, link to other relevant assets of the customer),
        - the expected impact on the price of services (performance);

    c) any changes to ICT functions and services must be subsequently approved by both parties in accordance with the Agreement. If the Agreement does not contain provisions for the approval of such changes (change procedure), changes to ICT functions and services may only be made by an amendment to the Agreement. The customer shall have the right to reject the proposed changes, in particular if it considers that they could adversely affect the quality and/or availability of the services provided and/or the information security of its assets;

    d) if the agreed service levels are not met, the provider shall immediately, but no later than within 3 calendar days, take appropriate measures to remedy the situation and minimise the impact on the customer's operations, and shall inform the customer of this fact without delay. At the same time, the

provider shall submit to the customer a corrective action plan containing measures to remedy the situation. The corrective measures shall be implemented in accordance with the corrective action plan, subject to approval by the customer.

9. The provider undertakes to participate in ICT security awareness and digital operational resilience training programmes developed by the customer or a third party authorised by the customer (the "**Training**"). The provider undertakes that participation in the Training shall include all employees and officers of the provider and managers involved in the provision of the Performance, including any subcontractors. If requested by the customer, the provider shall provide the customer with assistance, including information and know-how, in the preparation of the Training, including participation in the development of the content of the Training to a level of complexity commensurate with the provision of the Performance.

10. The provider shall take all appropriate technical and organisational measures, tools and ICT policies to prevent and minimise the risk of a breach of data availability, confidentiality, integrity and trustworthiness in accordance with the requirements of the customer's regulatory framework as a financial entity and the requirements of established best practice in the information security industry. In addition, the provider expressly undertakes to:

    a) provide regular training in cyber hygiene and safe user practices for its employees involved in the Performance and regular verification of the skills trained;

    b) ensure periodic vetting of staff involved in the delivery of benefits. The screening will be carried out in accordance with legislation, in particular in the field of labour law and privacy protection;

    c) ensure the use of a user and administrator identity management and authentication tool that provides identity verification prior to user and administrator activities, manages the number of failed login attempts, ensures authentication credentials are resistant to unauthorized theft and misuse, and user authentication. The authentication mechanism is based on multi-factor authentication with at least two types of factors;

    d) ensure regular checking of access permissions;

    e) ensure the use of robust encryption protocols to secure all data related to the Performance both "in rest" and "in transition";

    f) ensure that regular vulnerability scans are performed on systems used directly or indirectly to provide the Performance. Vulnerabilities classified as severe and critical shall be addressed by the provider as soon as a verified remedy (patch) is available. In the event of any vulnerability found in systems directly used or developed for the customer, the provider shall inform the customer immediately upon discovery of the vulnerability. The notification to the customer shall include a proposal for remediation of the identified vulnerability;

    g) ensure that penetration tests are performed by an independent third party at least once per calendar year. The test shall cover the environments used by the provider to provide the Performance. The provider agrees to provide the customer with a report of the penetration tests performed within one (1) week of receipt of the report;

    h) ensure the maintenance of policies and procedures for monitoring, detecting, documenting and responding to actual and reasonably anticipated security incidents, including establishing procedures for reporting such incidents involving the Performance provided directly or indirectly to the customer and the relevant supervisory authority in accordance with the cybersecurity regulations affecting the provider (in particular, reporting to the National Cyber and Information Security Authority and the Office of Personal Protection and law enforcement authorities);

    i) ensure compliance with the requirements of established best practice in the software development industry, the so-called "Secure Software Development Life Cycle", including at least the definition of security requirements for the developed software and security testing, static code analysis, automated security testing of code, etc;

    j) ensure that the third parties directly and indirectly involved in the provision of the Performance are regularly audited, in particular with regard to whether the third party is able to comply with requirements relating to ensuring the confidentiality, availability, integrity and reliability of data in general, which are at least at the same level of protection as the requirements imposed on the provider by the Contract Documents. The provider undertakes to provide evidence of regular vetting of third parties directly and indirectly involved in the provision of the Performance upon request of the customer.

11. The provider undertakes to report any incident or reasonable suspicion of an incident directly or indirectly related to the provision of the Performance. Provider shall report any incident or reasonably suspected incident promptly, but no later than eighteen (18) hours after provider becomes aware that an incident has occurred or may occur, to ithelpdesk@csas.cz . Provider shall disclose in the notification, to the best of its current knowledge:

    a) the nature of the incident, unauthorised disclosure or processing of data and information;

    b) the nature of the data and information concerned;

    c) the nature of the entity that caused the incident that unlawfully accessed or processed the data and information in question;

d) the steps the provider has taken and plans to take to mitigate the harmful effect and prevent similar events from occurring in the future.

12. If either party determines that the content of the incident notification is insufficient to determine the scope of the incident, both parties shall cooperate in the investigation of the incident and shall provide timely access to relevant security and operational records upon request to determine the impact on the provision of Performance and any liability that may result from the incident.

13. Except to the extent caused by the acts or omissions of the customer, the provider shall be responsible for all costs, internal and external, associated with any breach or reasonably suspected breach and the costs resulting therefrom, including the investigation of the data breach, legal and accounting fees and expenses associated with the customer's investigation of and response to such incident and the provision of notice to all persons affected by the incident, government regulatory authorities, if applicable, and the recovery of customer data, if applicable.

14. The provider shall provide the customer, promptly upon the customer's request, with all assistance and assistance in resolving an incident related to the Performance and/or the customer's assets affected by or on which the Performance caused the incident; if the provider is not liable for the costs pursuant to the preceding paragraph13 and the Agreement does not provide for an amount to cover the costs of such assistance and assistance, the provider shall provide it free of charge without any claim for reimbursement.

15. In the event that the Agreement does not expressly state that the creation and implementation of an exit strategy (or part thereof, if there is one, which applies to performance under other contracts and from other providers) for the handover of the provision of the Performance by the provider to the customer and/or to a new provider (hereinafter referred to as the "**Exit Strategy**") is part of the Performance, then the provider undertakes to provide all necessary assistance to the customer for the creation and implementation of the Exit Strategy without delay at the customer's request. Such cooperation shall include, in particular:

    a) providing the necessary information, documentation and data required to ensure a smooth handover of the Performance to the customer and/or the new provider and the development and implementation of the Exit Strategy;

    b) enabling the customer to access relevant systems and documents to the extent necessary to develop and implement the Exit Strategy and to effect a seamless transition of the Performance;

    c) transferring to the customer a complete knowledge of the Performance so that the customer has sufficient knowledge of the Performance to be able to provide the Performance itself or through a new provider and to be able to develop and implement an Exit Strategy;

    d) the necessary involvement of the provider's professional staff, with sufficient knowledge of the Performance and the technologies used, in the development and implementation of the Exit Strategy.

    This obligation shall apply to the development of the Exit Strategy and its implementation and, thereafter, to any need to update the Exit Strategy due to changes in the Performance and/or assets requiring such Exit Strategy to be updated. The obligations in relation to the implementation of the Exit Strategy in the actual transition of the Replacement Service are set out in**Fehler! Verweisquelle konnte nicht gefunden werden.** below.

16. The provider undertakes to ensure that all data processed within the Performance can be recovered, returned and made available in a structured and machine-readable format at any time in accordance with the customer's instructions. This data must be complete, containing the entire database of the Performance provided, including links and maintaining the authenticity and correctness of the data contained, all so that importing the submitted file will result in a complete recovery that will be eligible for deployment in live operation in the relevant environment. The provider undertakes to ensure that all data processed in the context of the Performance can be restored, returned and made available at any time in the required quality, in particular in cases of insolvency, crisis resolution, interruption of the provider's activities or termination of the Agreement for any reason, and to release them to the customer immediately upon the customer's request.

17. In cases of crisis resolution and/or interruption of the provider's activities, the provider shall in particular:

    a) immediately inform the customer of the planned measures and timeframe for ensuring re-access and restoration of the processed data to the required state;

    b) provide the customer with access to the processed data and ensure its recovery within the agreed timeframe; and

    c) provide the customer or a third party designated by the customer with reasonable assistance and assistance in retrieving content from the production environment, including assistance in understanding the structure and format of the database export file and the data being processed, including linkages, and in getting the database operational in a live environment after recovery.

18. In the event of termination of the Agreement, the provider shall:

    a) for a period of one hundred and eighty (180) days from the termination of the Agreement, continue to provide the customer with access to the processed data;

    b) within three (3) days of the expiration of the time period set out in a), submit to the customer all data processed within the Performance in a structured and machine-readable format as instructed by the customer. Such data shall be complete, containing the entire database of the Agreement, including

links and maintaining the authenticity and accuracy of the data contained, all so that the import of the submitted file will result in a complete recovery that will be eligible for deployment in live operation in the relevant environment.

c) provide the customer or a third party designated by the customer with reasonable assistance and assistance in retrieving content from the production environment, including assistance in understanding the structure and format of the database export file and the data being processed, including linkages, and in getting the functional database up and running after handover of the services.

19. The provider undertakes to implement, maintain and annually test business continuity plans and disaster recovery plans, including pandemic plans, in relation to the Perofrmance of the services.

20. The provider shall cooperate fully and provide all assistance to the regulatory authorities and authorities competent to resolve the customer's crisis, including persons appointed by them.

21. Contractual penalties:

    a. In the event that the provider fails to comply with the obligations under Annex A, Part I, Paragraph 12, i.e. fails to obtain the prior approval of the customer for the use of a subcontractor, the provider undertakes to pay a contractual penalty of CZK 20,000 for each individual case of violation.

    b. In the event that the provider fails to comply with the obligations pursuant to Annex A, Part II, Paragraph 8(b), i.e. fails to properly inform the customer of all changes to the functions and services of the ICT within the meaning of Annex A, Part II, Paragraph 8(b), the provider undertakes to pay a contractual penalty in the amount of CZK 20,000 for each individual case of breach.

    c. In the event that the provider fails to comply with the obligations under Annex A, Part II, paragraph 8(d), i.e.

        - fails to take timely and appropriate measures to remedy and minimise the impact on the customer's operations, or
        - fails to inform the customer in time about the measures according to the previous point, or
        - fails to submit a properly prepared corrective action plan to the customer in a timely manner,

        the provider undertakes to pay a contractual penalty of CZK 20,000 for each individual case of breach.

    d. In the event that the provider fails to comply with the obligations under Annex A, Part II, Paragraph 11, i.e. fails to inform the customer in time of a security incident or a reasonable suspicion of an incident, the provider undertakes to pay a contractual penalty of CZK 5,000 for each hour of delay.

    e. In the event that the provider fails to comply with the obligation under Annex A, Part II, Paragraph 14, i.e. fails to provide timely and prompt assistance and assistance in the event of a cyber security incident, the provider undertakes to pay a contractual penalty of CZK 10,000 for each day of delay.

    f. In the event that the provider fails to comply with the obligations under Annex A, Part II, Paragraph 18 (b), i.e. fails to submit the processed data and databases in a structured, machine-readable format in a timely or proper manner, the provider undertakes to pay a contractual penalty of CZK 10,000 for each day of delay.

ANNEX B
RESOLUTION AND RESILIENCE

1. The provider takes into account that the customer is a bank and as such he has to comply with the resolution legislation in the financial market introduced by the Directive 2014/59/EU of the European Parliament and of the Council of 15 May 2014 establishing a framework for the recovery and resolution of credit institutions and investment firms (BRRD) and the national legislation implementing it, primarily the law No. 374/2015 Sb., zákon o ozdravných postupech a řešení krize na finančním trhu.

2. For the purposes of this Annex, the following terms shall have the following meaning:

   "Erste Group" means a group of commercial corporations directly or indirectly controlled by Erste Group Bank AG, registered office: Am Belvedere 1, A-1100 Vienna, Austria, including this company. In this case, control refers to the holding of an ownership interest of more than 50% in the given company or holding of more than half of the voting rights, directly or indirectly.

   "**IZ**" means law No. 182/2006 Sb., o úpadku a způsobech jeho řešení (insolvenční zákon), which is the law by which the BRRD was transposed into national law in the Czech Republic, in its respective current form.

   "**ZOPŘK**" means law No. 374/2015 Sb., zákon o ozdravných postupech a řešení krize na finančním trhu, which is the law by which the BRRD was transposed into national law in the Czech Republic, in its respective current form.

   "**BRRD**" means the Directive 2014/59/EU of the European Parliament and of the Council of 15 May 2014 establishing a framework for the recovery and resolution of credit institutions and investment firms, as subsequently amended.

   "**CNB**" stands for "Czech National Bank" ("Orgán příslušný k řešení krize") that acts, *inter alia*, as national resolution authority in accordance with the ZOPŘK.

   "**SRMR**" means the Regulation (EU) No 806/2014 of the European Parliament and of the Council of 15 July 2014 establishing uniform rules and a uniform procedure for the resolution of credit institutions and certain investment firms in the framework of a Single Resolution Mechanism and a Single Resolution Fund.

   "**Resolution Action**" means (i) with regard to the customer: (a) any decision of the Resolution Authority to put the customer under resolution, and/or (b) any measure undertaken or initiated by the Resolution Authority with regard to the customer, in each case in accordance with the SRMR, the BRRD, IZ, ZOPŘK or in accordance with any other applicable law implementing the BRRD or any other applicable law regulating resolution of credit institutions and investment firms; and (ii) with regard to an Erste Group Member other than the customer: (a) any decision of the respective competent resolution authority of such Erste Group Member to put the respective Erste Group Member under resolution, and/or (b) any measure undertaken or initiated by the respective competent resolution authority of such Erste Group Member with regard to such Erste Group Member, in each case in accordance with the SRMR, the BRRD or in accordance with any applicable law implementing the BRRD or any other applicable law regulating resolution of credit institutions and investment firms. For the avoidance of doubt, the term "Resolution Action" as included herein also includes any measures potentially taken by the Resolution Authority or by the Erste Group member as part of or in relation to a business reorganisation or business restructuring plan following a bail-in event.

   "**Resolution Authority**" or "**Resolution Authorities**" means (i) with regard to the customer, the CNB, and (ii) with regard to an Erste Group Member other than the customer, the respective resolution authority(ies) of such respective Erste Group Member.

   "**SRB**" stands for "Single Resolution Board" and was established in accordance with the SRMR as the European Banking Union's resolution authority.

3. The customer and any other relevant Erste Group Members, being European credit institutions, are subject to the regulations of the SRMR, the BRRD and the respective national transposing laws such as IZ and ZOPŘK. The provider recognises the mandatory applicability of such regulations and the powers of the Resolution Authorities as resolution authorities of the customer and such other relevant Erste Group Members in a resolution scenario. The provider undertakes to cooperate fully (e.g. to provide the necessary information and documents to allow access, etc.) with the competent supervisory authorities and with the authorities competent to resolve the crisis of the financial entity, including the persons appointed by them (in Czech Republic e.g. NÚKIB or CNB).

4. The provider shall not be entitled to terminate, suspend or modify the Agreement solely because the customer and/or any other relevant Erste Group Member become(s) subject to Resolution Actions, or actions having a similar effect,

being taken or initiated by the Resolution Authority(ies). For the avoidance of doubt, this shall not operate as a waiver of other termination rights as set out in the Agreement.

5. Notwithstanding anything to the contrary in the Agreement, the provider herewith consents to the full or partial assignment and/or transfer of any rights and/or obligations of the customer and/or of another relevant Erste Group Member under the Agreement to another legal entity upon the direction of the Resolution Authority(ies) in case such assignment and/or transfer is required by the Resolution Authority(ies) as part of or as a consequence of a Resolution Action.

6. In the event the customer and/or another relevant Erste Group Member ceases to be an Erste Group Member as a result of a Resolution Action (hereinafter referred to as “Divested Erste Group Member”), any rights given to such Divested Erste Group Member under the Agreement shall remain unaffected for a period of one year after the divestment. For the avoidance of doubt, an Erste Group Member shall be deemed “Divested” when it no longer meets the definition of Erste Group Member under the Agreement.

7. The provider undertakes to notify the customer in advance of the necessity of ensuring the rendering of Performance, whether wholly or partly by another entity (hereinafter the „outsourcing chain") and will ask a prior consent of the customer with the usage of such entity. The agreement concluded between the provider and aforesaid further entity shall conform to the principles and rules laid down in this Annex. The provider shall ensure and provide all the necessary and required cooperation and cooperation of another entity in the event that the customer or the CNB is authorized to carry out the aforementioned control activities also at the other entity.

Aneex C - Codes of conduct for the use of Artificial Intelligence

Code of conduct for the use of Artificial Intelligence

PREAMBLE

Artificial intelligence is fundamentally changing the way we interact with information technology. It's a tool that helps us to solve tasks more creatively, more efficiently and ultimately in a smarter way. However, we are still responsible for the outcomes of its use.

Artificial intelligence tools have been with us for many years, but thanks to tools like ChatGPT, they have recently experienced a major evolution. Their use in everyday work such as preparing emails or producing creative texts and graphics, integrating them into internal processes and improving client services in the form of virtual assistants or product personalisation is a great opportunity, but also a big commitment.

We want to be a part of this breakthrough and a leader in the field of artificial intelligence in the banking sector, at the same time we are aware of our responsibilities towards our environment and therefore we follow this Code of conduct when utilizing artificial intelligence in Česká spořitelna, a.s. ("**ČS**").

WHAT WE MEAN BY ARTIFICIAL INTELLIGENCE

We consider artificial intelligence to be an artificially created machine system that can - more or less independently - deduce and generate outputs such as answers, recommendations or content based on input data. AI-based systems can thus communicate, provide advise and produce texts, images and videos with an impact on the outside world. Artificial intelligence is closely associated with machine learning and processing of large amounts of data, and its key characteristics are the ability to adapt and deduce the most likely responses to given inputs.

The most attention is currently being drawn to the tools of so-called generative artificial intelligence (according to the European Regulation on Artificial Intelligence, this is a "general purpose AI system"), which are tools that create content in the form of texts, images, audio or video and, thanks to the ability to produce texts can imitate human communication. Examples of generative artificial intelligence (general purpose AI system) tools are ChatGPT, Google Bard, Microsoft 365 Copilot or GitHub Copilot for mainly text-based communication, or Midjourney and DALL-E for image creation. This Code of conduct applies to all artificial intelligence tools or any other tools that use artificial intelligence in any way.

PRINCIPLES AND TENETS

I. ACCOUNTABILITY AND COMPLIANCE WITH LEGISLATION

1. We use and develop artificial intelligence tools with the acceptance of full responsibility at the level of ČS top management and promote a responsible and ethical approach to the use of artificial intelligence.
2. We comply with all applicable laws and regulations when using and creating artificial intelligence tools, in particular specific rules regarding artificial intelligence itself, banking sector regulations, data protection and intellectual property legislation.
3. The use of artificial intelligence is rigorously managed on the basis of a risk assessment in accordance with ČS internal regulations.
4. We only use artificial intelligence tools that have been thoroughly assessed and have been internally approved, and only for approved purposes. We use these tools provided by ČS to perform our work-related tasks. This also includes trying and testing these tools, learning about their principles, and gaining experience with artificial intelligence and machine learning.
5. We are continuously educating ourselves in the field of artificial intelligence and strengthening our awareness of the benefits and risks. We also promote education and awareness-raising among our partners and the public.

As an employee or external collaborator of ČS, I abide by the following rules:

a) For my work tasks, I do not use commonly available artificial intelligence tools (whether they are freely available or commercially available), but only tools approved by ČS for this purpose.

- *For my work I do not use artificial intelligence tools available on the web (e.g. ChatGPT available on openai.com), but only a special version of ChatGPT for ČS, available on the Chatbot OpenAI (cs.cz) or in the Teams application.*
- *Suggestions for new use-cases of approved artificial intelligence tools for specific purposes, products or activities within ČS (hereinafter referred to as "**use-cases**") can be submitted via the Teams application by uploading a post to CSAS Artificial Intelligence | Obecné | Microsoft Teams.*

– *The selected use-cases and their conditions, which will be created using artificial intelligence tools for specific purposes or activities in ČS, shall be approved in accordance with the rules set out in the internal regulation on the Use of Artificial Intelligence in Česká spořitelna.*

– *A list of artificial intelligence tools approved for use in ČS, as well as an overview of approved use-cases, is available on AI Working group (sharepoint.com).*

b) If I want to use artificial intelligence tools in my work, I keep up-to-date with current information and familiarise myself with the educational materials provided by ČS for this purpose and specifically brought to my attention, so that I am aware of any risks associated with the use of artificial intelligence. I shall also complete any mandatory training courses brought to my attention by ČS at the appropriate times.

– *I can find current mandatory training courses and educational materials on the use of artificial intelligence in ČS on AI EduHub (sharepoint.com).*

c) If I use an artificial intelligence tool in the performance of my work, I maintain responsibility for the results of that work and use it with that understanding.

– *While the output of artificial intelligence may sound confident, it may not be true. Artificial intelligence can "hallucinate" or completely "fabricate", and therefore it is essential to properly check each artificial intelligence output for both its content and form before using it.*

II. TRANSPARENCY AND TRUST

6. We use artificial intelligence with transparency in order to strengthen client trust in our services and improve the client experience and the work environment for our colleagues.

7. Our employees, clients and colleagues always know that they are interacting with artificial intelligence, if that is the case. We also provide clients and colleagues with information about the limitations of artificial intelligence in a particular case and their rights related to the use of artificial intelligence, where relevant.

As an employee or external collaborator of ČS, I abide by the following rule:

a) If I use approved generative artificial intelligence (general purpose AI system) tools as inspiration or assistance in preparing communications, documents or materials that I subsequently review or edit myself, I do not have to inform clients about the use of artificial intelligence.

III. HUMAN INTERVENTION AND SUPERVISION

8. We use artificial intelligence as a tool that serves people, respects human dignity and personal autonomy, and operates in a way that allows human control and supervision.

As an employee or external collaborator of ČS, I abide by the following rules:

a) I am aware that even if I use an artificial intelligence tool, my actions and outputs of my work may have implications for humans, and I approach the use of these tools with that in mind.

b) I only use an artificial intelligence tool if I have familiarised myself with how it works, how it is operated and what the consequences of its use may be, so that I can avoid the negative impacts of its use on humans.

c) If I use artificial intelligence tools in my work, I strive to use them effectively and efficiently.

IV. PRIVACY, CYBERSECURITY AND DATA PROTECTION

9. When using artificial intelligence, we take the proper care to protect the personal data and privacy of our clients, colleagues and other persons and respect banking secrecy, as well as safeguard our confidential information, know-how and trade secrets.

10. We use artificial intelligence in a manner that does not compromise the proper delivery of our services to our clients and does not compromise the security of our systems.

11. When using and creating artificial intelligence tools, we only use data and inputs for which we have the right to use them in this way, both from the point of view of personal data protection, intellectual property right and other data rights.

As an employee or external collaborator of ČS, I abide by the following rules:

a) I do not enter any data concerning clients, colleagues or other persons or any confidential information of ČS into artificial intelligence tools unless this use of the tool has been approved by ČS.

b) If I enter data or other inputs into the artificial intelligence tool, I have verified that ČS can use the data in this way.

– *Personal data protection rules may restrict the use of some data for training of artificial intelligence or output processing.*

– *Some inputs such as texts, images or videos from the Internet may be subject to third-party intellectual property rights. Just as I cannot use them in my normal work output, I cannot provide them as input to artificial intelligence tool, unless I have properly secured the rights to them.*

c) Artificial intelligence outputs are the property of ČS and I may use them only for the performance of my work tasks at ČS. When using the outputs of artificial intelligence, I shall also comply with other duties set out in the ČS Work Rules regarding ČS property.

d) I do not grant or warrant any rights (e.g., copyright, or other intellectual property rights) to the output of artificial intelligence, that I transmit or provide to a third party (i.e., a party other than ČS and its employees).

e) I am aware that artificial intelligence is usually based on third party software and tools that can be misused for cyber or other attacks, therefore I use artificial intelligence tools in accordance with IT security rules.

V. DIVERSITY AND FAIR ACCESS

12. We promote diversity and fairness. Therefore, we use and create artificial intelligence tools in a way that takes into account the various actors in society, promotes equity and cultural diversity, while avoiding bias, discrimination and unfair prejudice.

13. We make every effort to ensure that the use of artificial intelligence does not discriminate, does not promote stereotypes, does not take into account prejudices and other undesirable types of bias. In particular, we are committed to avoiding discrimination against groups and individuals on the basis of race, origin, gender, religion, sexual orientation or political opinion.

14. To this end, we ensure the quality of the data used for training of artificial intelligence. Where we provide this data ourselves, we regularly test, review and adjust it to minimise the risks of bias or discrimination.

As an employee or external collaborator of ČS, I abide by the following rules:

a) When I use an artificial intelligence tool for an activity that may affect an individual or a group of people, I make sure that the results are fair to all groups and are not affected by bias, and I try to control and verify these aspects as much as possible.

b) When I provide data to artificial intelligence tools, I ensure that they are continuously tested, checked and adjusted to minimise the risk of bias or discrimination based on race, origin, gender, religion, sexual orientation or political opinion in particular.

Extended Code of conduct for the use of Artificial Intelligence

A. INTRODUCTORY PROVISIONS

1. This Extended code of conduct for the use of Artificial Intelligence (hereinafter referred to as "**Extended Code**") is intended for:

   a) employees of Česká spořitelna, a.s. (hereinafter referred to as "**ČS**") who are involved in the approval of:

      i) artificial intelligence tools for their use in ČS;

      ii) specific use cases for the use of approved artificial intelligence tools for specific purposes, products or activities of ČS (hereinafter referred to as "**use-case**");

   b) employees of ČS involved in the technical implementation and administration of specific artificial intelligence tools approved for their use in ČS;

   c) employees of ČS involved in the implementation of specific approved use-cases (including employees who subsequently become the owner or administrator of the technical solution or internal process within the implemented use-case);

   d) employees of ČS who, as part of their job description, procure an approved artificial intelligence tool;

   e) employees of ČS who, on its behalf, provide its business partners with outputs generated by artificial intelligence tools on a contractual basis;

   f) employees of ČS who, using artificial intelligence tools, produce outputs in the form of texts, images and audiovisual materials that are intended for the general public or for which increased visibility is expected;

   g) employees of ČS who test, develop or implement evaluation, communication or other models using artificial intelligence tools;

   h) employees of ČS who are managers in relation to the employees referred to in letters (a) to (g) above;

   i) external collaborators and contractors of ČS involved in the activities referred to in letters (a) to (g) above;

   (hereinafter referred to as "**Responsible Employees**").

2. Unless a specific clause of this Extended Code assigns responsibility to a particular group of Responsible Employees listed above, the obligations set out in this Extended Code shall apply to all Responsible Employees.

3. The measures in this Extended Code are based on the Code of Conduct for the Use of Artificial Intelligence. Selected principles and tenets to which ČS and its employees and external collaborators have committed under the Code of Conduct for the Use of Artificial Intelligence, have been developed into specific obligations for Responsible Employees in this Extended Code. What is meant by artificial intelligence is described in the Code of Conduct for the Use of Artificial Intelligence. The obligations set out in the Code of Conduct for the Use of Artificial Intelligence remain unaffected.

B. PRINCIPLES AND TENETS

B.1 Accountability and compliance with legislation

4. Only artificial intelligence tools that guarantee **compliance with applicable legislation, in particular sectoral banking regulation, financial services regulation and data protection regulation (in particular personal data)** within the intended use-cases and the relevant agreed licence terms, may be developed, purchased and implemented. As part of the evaluation of use-cases, it is necessary to take into account not only the desired uses, but also the possible misuses that can be reasonably foreseen.

5. The Responsible Employees in charge of the technical implementation and administration of the approved artificial intelligence tools shall comply with the **instructions, technical documentation and terms of use of the purchased artificial intelligence tool** and shall monitor their continuous updates, which they shall record in the technical documentation of the artificial intelligence tool according to point 6 below.

6. The Responsible Employees in charge of the technical implementation and administration of the approved artificial intelligence tools are required to maintain **written technical documentation** on the artificial intelligence tools and to record in particular:

   a) the name of the artificial intelligence tool and the identification data of its provider;

   b) a description of its intended use in ČS;

   c) information on whether ČS develops the artificial intelligence tool itself, or is only a user of an artificial intelligence tool developed by a third party, or whether it is a combination of the two previous options, i.e. ČS further develops and trains the artificial intelligence tool developed by the third party;

   d) the process of developing, purchasing, implementing and using an artificial intelligence tool;

   e) in the case of the purchase of an artificial intelligence tool the following:

      - the reasons for choosing a particular artificial intelligence tool;

      - the applicable terms of the contract, terms of use and their continuous updating;

   f) a records of the process of ongoing evaluation of the role of ČS in relation to the specific approved artificial intelligence tool, with evaluation to be carried out at least once every 12 months, or after any significant intervention in the artificial intelligence tool;

   g) the nature of the input data and the process of its continuous testing;

   h) the licence or other similar legal rights to the output of the artificial intelligence tool.

7. In the case of artificial intelligence tools that are expected to interact with clients within the intended use-cases, it is necessary to take technical measures **to reduce the risk that the outputs of these tools will be interpreted as investment advice** pursuant to Act No. 256/2004 Coll., **insurance intermediation** pursuant to Act No. 170/2018 Coll., **consumer credit intermediation** pursuant to Act No. 257/2016 Coll., and other activities that are only authorised to be provided by persons with appropriate training as defined by law. Exceptions are cases where the artificial intelligence tool is intended for this activity and the use for this activity has been evaluated in the approval of the specific use-case. An analysis of compliance with regulatory requirements must be carried out at the latest before the artificial intelligence tool is put into operation within a specific use-case and the conclusions of this analysis must be taken into account when implementing the artificial intelligence tool.

B.2 Transparency and trust

8. In the case of artificial intelligence tools that are expected (within the scope of the intended use-cases) to interact with clients, employees (beyond the scope of their work tasks) or other natural persons as data subjects within the meaning of the GDPR, it is necessary to develop the terms of use of the artificial intelligence tool and to transparently inform data subjects about the purpose, time, scope and manner of processing their personal data.

B.3 Human intervention and supervision

9. Only properly **trained and qualified employees or external collaborators** are involved in the development and implementation of artificial intelligence tools.

10. The intended operation of the artificial intelligence tools as recorded in the technical documentation maintained in accordance with point 6 above, shall be continuously **reviewed and evaluated**. This control shall be ensured by

the Responsible Employees in charge of the technical implementation and administration of the artificial intelligence tools at least once every 12 months and, in addition, after any substantial intervention in the artificial intelligence tool.

11. The Responsible Employees involved in the production of outputs that are intended for the general public or are expected to be highly visible shall ensure that such outputs produced using artificial intelligence tools are subject to increased human review and human intervention in the sense of editing, corrections or additions prior to their use. A written record of this review and any corrections shall be made and kept on file by the Responsible Employee.

12. In the event that the artificial intelligence system will, within the intended use-case make fully **automated decisions about clients' rights or make automated decisions that have legal effects for clients or significantly affect clients** (e.g. decision on the provision of the mortgage loan), the Responsible Employees in charge of the implementation of the specific use-case (or those who are the owner or administrator of the internal process within the implemented use-case) are obliged to ensure that the rules set out in Article 22 of Regulation 2016/679 (GDPR) are taken into account, i.e. in particular appropriate measures are taken in the form of the **right to human intervention**, the right to express the opinion of the client concerned and the right to challenge the decision taken in this automated manner. Within the framework of these rules, the client (data subject) has the right not to be subject to any decision based solely on automated processing, including profiling, which has legal effects concerning him or her or similarly significantly affects him or her, to which exceptions are allowed only where such automated decision is necessary for the conclusion or performance of a contract between the controller and the data subject or is permitted by the European Union Law or the law of the member state of the European Union or is based on the consent of the client (data subject). For further information and compliance with the necessary requirements, please contact the 6900_01 – team GDPR (e-mail: GDPR@CSAS.CZ) or the relevant Data Protection Officer of ČS.

B.4 Privacy, cybersecurity and data rights

Personal data

13. When developing, implementing and using artificial intelligence tools within the intended use-cases, **solutions that work only with impersonal data of a static nature** (e.g. preferences of individual client groups) or with data in pseudonymised form are **preferred**.

14. If the development, implementation and use of artificial intelligence tools are to use personal data, **the rules for the processing of personal data and special categories of personal data** under Regulation 2016/679 (GDPR) must be complied with, and in particular the following rules:

    a) the processing of personal data must be based on an appropriate legal basis;

    b) the principle of transparency as set out in point 8 above must be complied with;

    c) measures must be taken to enable data subjects to exercise their rights under the GDPR;

    d) in the case of automated individual decision-making, including profiling pursuant to Article 22 of the GDPR, the procedure set out in point 12 above must be followed;

    e) appropriate technical and organisational measures must be in place to ensure the secure processing of personal data in accordance with Article 32 of the GDPR;

    f) a data protection impact assessment in accordance with Article 35 of the GDPR, must be carried out in light of the specific circumstances, whereby the use of an artificial intelligence tool will generally pose a high risk in the processing of personal data for which a data protection impact assessment is necessary.

    In order to comply with the rules mentioned above, close cooperation between the Responsible Employees and the GDPR team or the relevant Data Protection Officer of ČS must be ensured, and the rules for working with personal data, which are set out in the internal regulations: Personal Data Protection and Banking Secrecy (csin.cz), must be respected.

15. If a particular artificial intelligence tool offers the **possibility of increased data privacy and data protection**, the Responsible Employees in charge of the technical implementation and administration of the approved artificial intelligence tools shall ensure that this option is **used in** the development, implementation and use of the artificial intelligence tool, unless there is a **legitimate reason** to the contrary, which shall be recorded in the technical **documentation** as set out in point 6 above.

16. In the development, implementation and use of generative artificial intelligence (according to the European regulation on artificial intelligence, this is a "general purpose AI system") tools, solutions are preferred in which the inputs and generated outputs are located **in an environment dedicated only to ČS** and neither the input nor the output data **are used back to train or improve the language model of the provider of the artificial intelligence tool**. The actual training or enhancement of the language model within ČS is possible if permitted within the corresponding standard ČS acceptance process.

Intellectual property rights

17. Only generative artificial intelligence (general purpose AI system) tools can be used to produce content (e.g. source codes or marketing materials) provided outside of ČS, that:

    a) grant corresponding copyright, author's rights or other similar usage rights to the output of the artificial intelligence tool to ČS; or

    b) in the contracts, contractual terms or terms of use of the artificial intelligence tool shall include an obligation of the provider of the tool **to indemnify ČS in the event that the use of the output of the artificial intelligence tool causes ČS harm, in particular** through **claims by third parties for infringement of copyright and intellectual property rights**.

18. The Responsible Employees in charge of the technical implementation and administration of approved artificial intelligence tools or in charge of the implementation of a specific use-case (including those who are the owner or administrator of an internal process within the implemented use-case) shall ensure that artificial intelligence tools developed or modified by ČS are **trained on data whose use for training and within the outputs of the tool does not constitute an infringement of the copyright and intellectual property rights of third parties**.

19. The outputs of generative artificial intelligence (general purpose AI system) tools in the form of texts, images or audiovisual materials may be provided to the business partners of ČS only if:

    a) these partners are also provided with **information that the artificial intelligence tool produced or was involved in the creation of the output**; and

    b) the output **is not provided with a license or a statement that the copyright and intellectual property rights in the output have been cleared**.