PSS PRVÁ STAVEBNÁ SPORITEĽŇA

Attachment to the Order

Incorporation of rights and obligations arising from EU regulation on digital operational resilience of the financial sector (Regulation (EU) 2022/2554 and other related regulations)

1. This attachment is an integral part of any Order whose subject matter is ICT Services relevant to Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience of the financial sector, as amended (hereinafter referred to as the "**DORA Regulation**") and other related regulations, in particular Commission Delegated Regulation (EU) 2024/1773 of 13 March 2024 and Commission Delegated Regulation (EU) 2025/532 of 24 March 2025 (hereinafter referred to as "**ICT Services**").
2. The Provider declares that he has read this document, which forms part of the Order, and undertakes to comply with and fulfill the obligations arising from this document.
3. The Provider undertakes to identify and assess all relevant risks in connection with this Order, including the possibility that the contractual arrangement between the Provider and the Customer in relation to ICT Services supporting critical or important functions under this Order may contribute to increasing the risk of ICT concentration at the entity level pursuant to Article 29 of the DORA Regulation.
4. The Customer is entitled, on the basis of a risk-based approach, to determine in advance the frequency of audits and inspections at the Provider's premises, as well as the areas in which the audit or inspection is to be carried out, in compliance with generally accepted auditing standards in accordance with any instructions from supervisory authorities on the use and integration of these auditing standards.
5. The Customer is entitled to continuously monitor the performance of the Provider. The Customer has, in particular:
   a) the right to access, inspect, and audit the Provider; in case of ICT Services supporting critical or important functions, also the unlimited right to access, inspection and audit by the Customer or an authorized third party and the competent authority, and the right to make and take copies of relevant documentation on site if they are crucial to the Provider's activities, whereby the effective exercise of these rights shall not be prevented or restricted by other contractual arrangements or policies; this corresponds to the right of the Customer and his representatives to access all locations where ICT Services are provided or secured;
   b) in case of ICT Services supporting critical or important functions, the right to agree on alternative security levels approved by the Customer if the rights of other clients are affected;
   c) the right, in case of contracts with high technical complexity, to verify if the Provider's auditors, whether external or internal, or an association of auditors, have the appropriate skills and knowledge to carry out the relevant audits and assessments effectively;
   d) the right to carry out an audit or inspection, as a rule, once per calendar year; the Customer shall notify the Provider of the performance of an audit or inspection on site in advance, at least 7 working days before it is carried out;
   e) the Customer shall carry out inspections and audits in accordance with the principle of proportionality, in accordance with the Provider's security rules and without disrupting the Provider's activities beyond the usual extent;
   f) the Customer shall prepare a record of the inspection and audit carried out by him, containing the identified findings and deficiencies; the Customer shall inform the Provider of the identified findings and deficiencies without undue delay, requesting a proposed deadline for resolving the identified deficiencies and findings; the Provider shall be obliged to regularly inform the Customer about the solution and resolution of the identified deficiencies and findings.
6. The Provider is obliged to:
   a) accept audit and control by the Customer, cooperate fully during on-site inspections and audits carried out by the competent authorities, the main supervisory authority, the Customer or an authorized third party, and is obliged to provide assistance and cooperation and access to the required documentation;
   b) provide detailed information on the scope, procedures to be followed and frequency of such inspections and audits.
7. The Provider undertakes to identify and assess any conflict of interest that may arise from the performance of this Order.
8. If the subject of performance under this Order is the provision of ICT Services supporting critical or important functions, the Provider declares that he has processes, procedures, and measures in place in accordance with the requirements of the most current and stringent international information security standards.
9. The Provider undertakes to inform the Customer of the place of performance under this Order. The Provider acknowledges that any change in the place of performance of the subject matter of this Order by the Provider is subject to the written consent of the Customer.

10. The Provider undertakes to inform the Customer of the place of processing and storage of personal data and other than personal data.
11. The Provider is obliged to ensure access, recovery, return of personal data and other than personal data processed by the Provider in an easily accessible format in case of insolvency, crisis resolution, termination of the Provider's business operations or in case of termination of the Contract according to the instructions of the Customer.
12. The Provider is entitled, with the prior consent of the Customer and after mutual agreement on the terms of sub-delivery, to provide ICT Services supporting critical or important functions or their significant parts through a sub-provider, whose identification details shall be communicated by the Provider to the Customer sufficiently in advance of the commencement of performance under this Order, as well as at any time during the term of the Contract, if requested by the Customer, and at the same time with each change concerning the sub-provider.
13. The Provider undertakes to inform the Customer in writing without delay of any changes to the facts stated above in this document, and the Provider is entitled to implement these changes only after obtaining the prior written consent of the Customer. The Provider is also obliged to inform the Customer without undue delay of any security events or incidents that could have a negative impact on the Provider's ability to provide the services to the Customer with the subject of performance under this Order in the quality, quantity, deadlines, and budget that were agreed upon.
14. The Provider agrees to comply with the description of the level of services to be provided, including updates and revisions, as set out in the Order.
15. The Provider is obliged to provide assistance to the Customer at no additional cost in case of an ICT incident related to the subject of performance caused, brought about or aggravated by the Provider's activities. In other cases, a cost-sharing agreement between the Provider and the Customer is possible.
16. The Provider is obliged to co-operate with the competent authorities and the Customer's crisis management authorities, including their designated persons.
17. The Provider is obliged to participate in the Customer's ICT Security Awareness and Information Awareness Program and Digital Operational Resilience Training in accordance with Article 13(6) of the DORA Regulation.
18. If the subject matter of performance under this Order is the provision of ICT Services supporting critical or important functions or their significant parts, the Provider is also obliged to:
    a) immediately, but no later than 24 hours after becoming aware of any development that could have a material impact on the Provider's ability to effectively provide the subject of performance in accordance with the obligations set out in this Order, inform the Customer of such development, including the specific impact on the SLA;
    b) to implement and test contingency plans and is required to have ICT security measures, tools, and policies in place that provide an adequate level of security for the provision of services that are the subject of performance under this Order by the Customer in accordance with its regulatory framework; upon request by the Customer, the Provider is obliged to make the results of such testing available to the Customer;
    c) participate in the Customer's penetration testing based on a specific threat in case that the Customer is obliged to perform such testing and cooperate fully with it as specified in Articles 26 and 27 of the DORA Regulation.
19. ICT Services supporting critical or important functions or their significant parts provided by the Provider are subject to independent review and are included in the Customer's audit.
20. In case of provision of ICT Services through a sub-provider, the Provider is fully responsible for their provision by the sub-provider to the full extent as if he had provided them himself.
21. In case of provision of ICT Services that effectively support critical or important functions or their significant parts, the disruption of which would reduce the security or continuity of provision of ICT Services through a sub-provider, the Provider is also obliged to fulfill the following obligations:
    a) monitor all ICT Services provided through a sub-provider to ensure the continuous fulfillment of all its contractual obligations towards the Customer;
    b) monitor and report to the Customer on sub-providers providing ICT Services;
    c) assess all risks associated with the place of provision of ICT Services by current or potential sub-providers providing ICT Services and its parent company and the place from which the ICT Service is provided;
    d) specify in a written contract with sub-providers providing ICT Services the obligations of sub-providers to monitor and report to the Provider;
    e) ensure the continuity of ICT Services throughout the sub-provider chain in case that a sub-provider fails to fulfill his contractual obligations, and include requirements for business continuity plans within the meaning of Article 30 (3) (c) of the DORA Regulation and defines the levels of ICT Services that sub-providers must comply with in connection with these plans;

f) specify in the written contract with the sub-provider providing ICT Services the ICT security standards and, where applicable, any additional security requirements that sub-providers must comply with in accordance with Article 30 (3) (c) of the DORA Regulation;
g) oblige the sub-provider to provide the Customer and the relevant competent authorities and crisis resolution authorities with the same rights of access, inspection and audit as set out in Article 30 (3) (e) of the DORA Regulation, as provided to the Customer and the relevant competent authorities and crisis resolution authorities by the Provider;
h) inform the Customer of any intended significant changes to contracts with sub-providers in accordance with Article 5 of the Commission Delegated Regulation (EU) 2025/532.

22. If personal data is processed by a sub-provider/sub-providers, the Provider is obliged to identify the place of processing and the appropriate safeguards taken to the Customer. The provision of this point shall not apply if the place of processing and the appropriate safeguards are agreed in a separate contract on the processing of personal data concluded between the contracting parties in connection with this Order.
23. The Customer is entitled to monitor the ICT Services supporting critical or important functions in accordance with Article 30 (3) (a) of the DORA Regulation, and to monitor the ICT risk that may arise in connection with the use of ICT Services provided by sub-providers providing ICT Services supporting critical or important functions or their significant parts.
24. The Customer is entitled to assess whether and how a potentially long or complex chain of sub-providers providing ICT Services supporting critical or important functions or their significant parts may affect their ability to fully monitor contractual functions and the ability of the competent authority to effectively supervise the Customer.
25. The Customer is entitled to request from the Provider information on the contractual documentation concluded between the Provider and all his sub-providers providing ICT Services supporting critical or important functions or their significant parts, the disruption of which would reduce the security and continuity of the services provided, as well as information on the relevant performance indicators in accordance with Article 30 (3) (e) of the DORA Regulation and Article 8 (2) of the Commission Delegated Regulation (EU) 2024/1773.
26. In case of intended significant changes to contracts with sub-providers relating to ICT Services supporting critical or important functions or their significant parts, the Provider is obliged to inform the Customer of the risks to which he is or could be exposed, as well as whether such changes could affect the Provider's ability to fulfill his obligations under the Contract as specified in Article 5 of Commission Delegated Regulation (EU) 2025/532, as well as with regard to Article 1 of Commission Delegated Regulation (EU) 2025/532, within a sufficient period of time, but not less than 7 working days, necessary for the Customer to assess the impacts and risks of such changes.
27. The Provider is entitled to make intended significant changes in the provision of ICT Services supporting critical or important functions or their significant parts, including a change of sub-provider providing ICT Services supporting critical or important functions or their significant parts, always only on the basis of their approval by the Customer or if the Customer does not raise any objections to these changes within the period provided by the Provider.
28. If, based on a risk assessment, the Customer finds out that the planned sub-delivery or changes in the sub-delivery by the Provider exceed the Customer's risk tolerance, the Customer has the right, before the expiry of the period for comments provided to him for this purpose by the Provider, to:
    a) inform the Provider about the results of the risk assessment and
    b) raise objections to changes and request modification of the proposed changes to the sub-deliveries prior to their implementation.
29. The Customer is entitled to terminate the Contract by giving three months' notice, which shall commence on the first day of the calendar month following the month in which the notice was delivered to the Provider, for the following reasons:
    a) significant breach by the Provider of the relevant laws, other regulations or contractual terms and conditions;
    b) circumstances identified during the monitoring of the Provider's risks which are considered capable of changing the performance of the functions provided based on this Order, including significant changes affecting the Provider's arrangement or situation;
    c) the demonstrated weaknesses of the Provider relating to his overall management of ICT risk, and in particular how it ensures the availability, authenticity, integrity and confidentiality of data, whether personal or otherwise sensitive data or other than personal data;
    d) if the competent authority can no longer effectively supervise the Provider due to conditions or circumstances related to this Order;
    e) failure to resolve identified deficiencies by the Provider in connection with Article I, Clause 5 Letter f) of this document.

f) if the Provider makes significant changes to contracts with sub-providers providing ICT Services supporting critical or important functions or their significant parts, despite objections and requests for adjustments to the changes by the Customer;
g) if the Provider makes significant changes to contracts with sub-providers providing ICT Services supporting critical or important functions or their significant parts before the expiry of the period granted by the Provider to the Customer without the Customer's consent;
h) if the Provider concludes a contract with a sub-provider for the provision of ICT Services supporting critical or important functions or their significant parts, which are not expressly permitted as the subject of sub-delivery in the Contract with the Customer;
i) if the Provider refuses to provide the Customer with, or provides the Customer with false, incomplete, or misleading information regarding sub-providers and contracts concluded with sub-providers providing ICT Services supporting critical or important functions or their significant parts, which the Customer is obliged to ascertain in accordance with the applicable regulation concerning the digital operational resilience of the financial sector and related legislation following on from the regulation in question, regardless of whether such conduct by the Provider was intentional or negligent.

30. The Customer is also entitled to terminate the Contract by giving 3 months' notice, if so determined by the competent authorities, which shall commence on the first day of the calendar month following the month in which the notice was delivered to the Provider, if so decided by the competent authorities or the Customer's crisis management authorities.