

# OBLIGATIONS ARISING FROM THE DORA REGULATION

**REQUIREMENTS FOR THIRD-PARTY PROVIDERS**

**AND RELATED ACTIVITIES CARRIED OUT ON THE PART OF  
FINANCIAL INSTITUTION IN THE POSITION OF CUSTOMER  
(hereinafter referred to as „ČSOB“)**




# INTRODUCTION TO THE DORA RULES FOR ICT SERVICES

- **What is DORA:** Regulation (EU) 2022/2554 of the European Parliament and of the Council on digital operational resilience for the financial sector, which aims to ensure that financial institutions are better prepared for digital threats and can effectively manage ICT risks.
- **Objective of the rules:** To protect critical and important functions of financial institutions from outages and security incidents associated with ICT services provided by third parties. DORA emphasises prevention, resilience and the ability to respond quickly.
- **Key areas:**
  - **Risk management:** Implementation of procedures for the identification, assessment and management of risks associated with ICT services.
  - **Security measures:** Ensuring the protection of data and ICT systems against attacks and vulnerabilities.
  - **Control of sub-providers:** The review and supervision of providers delivering ICT services, including the management of the sub-provider chain.
  - **Response to incidents:** Setting up procedures to respond quickly and effectively to security incidents.
- **Implementation in the ČSOB environment:**
  - Contract amendments for ICT service providers
  - Register of information



# ACTIVITIES ON THE PART OF ČSOB

- **Management of risks related to ICT service providers:**
    - ČSOB must ensure regular assessment of risks related to ICT service providers and must adapt measures based on changes in their risk profiles.
    - It must ensure that providers actively contribute to effective ICT risk management and that their processes are documented and compliant with DORA requirements.
  - **Monitoring of and compliance with contracts:**
    - ČSOB shall monitor the performance of providers and ensure that they follow the established SLAs (ideally at least annually) and security measures.
    - ČSOB has the right to conduct regular audits and inspections to verify compliance with contractual and regulatory requirements.
- 

# SECURITY AND INCIDENT RESPONSE REQUIREMENTS

## Measures:

- Security – ICT service providers must ensure the protection of ČSOB data by encryption, regular backups and implementation of security measures to protect the data against unauthorised access.
- Providers must have service continuity plans in place and conduct regular tests of these plans to ensure that they are functional and effective.


## Response to incidents:

- Providers must promptly report any critical security incidents and vulnerabilities that may affect the services they deliver.
- Providers must work with ČSOB to identify the causes of incidents, remedy the situation and implement measures to prevent future incidents.





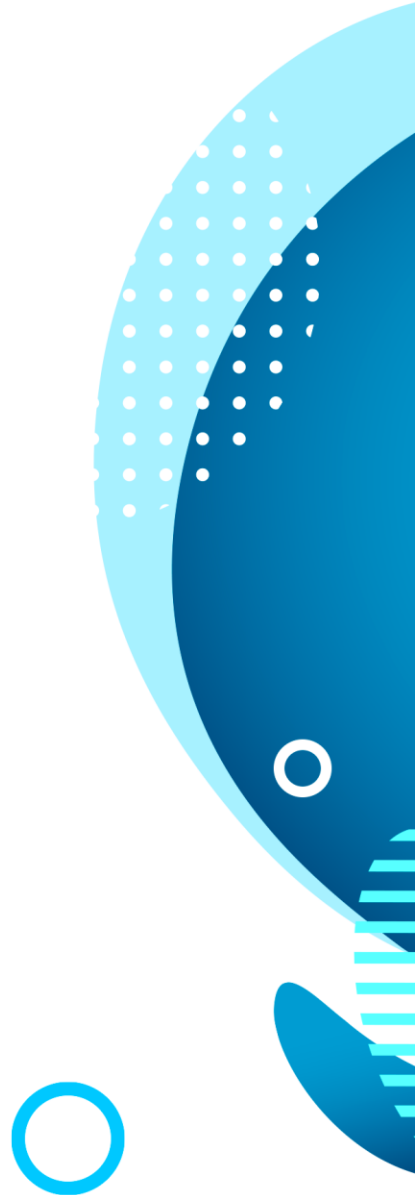
# CONTROL OF SUB-PROVIDERS

- **Approval of sub-providers:**
    - Providers may use sub-providers only with the prior written consent of ČSOB. Each sub-provider must be assessed in terms of risks, in particular with regard to sub-providers in a different geographical location and their impact on security and the continuity of services.
    - It is necessary to assess potential risks associated with the location of sub-providers and ensure that all steps have been taken to protect ČSOB data.
  - **Responsibility and audit:**
    - Providers are fully responsible for the activities of their sub-providers and must ensure that they meet the same security and SLA requirements.
    - ČSOB has the right to audit and inspect sub-providers to ensure that all standards and measures are being followed.
- 



# DATA SECURITY OBLIGATIONS

- **Data protection:** Providers must guarantee that all ČSOB data are securely protected and regularly backed up, and that the data can be transferred or deleted at ČSOB's request. They must also guarantee their removal after the end of the contract.
- **Vulnerability management:** Providers are obliged to immediately address any identified vulnerabilities in ICT systems and ensure that data remain protected in the face of new threats. They must use up-to-date technology and procedures to ensure data security.

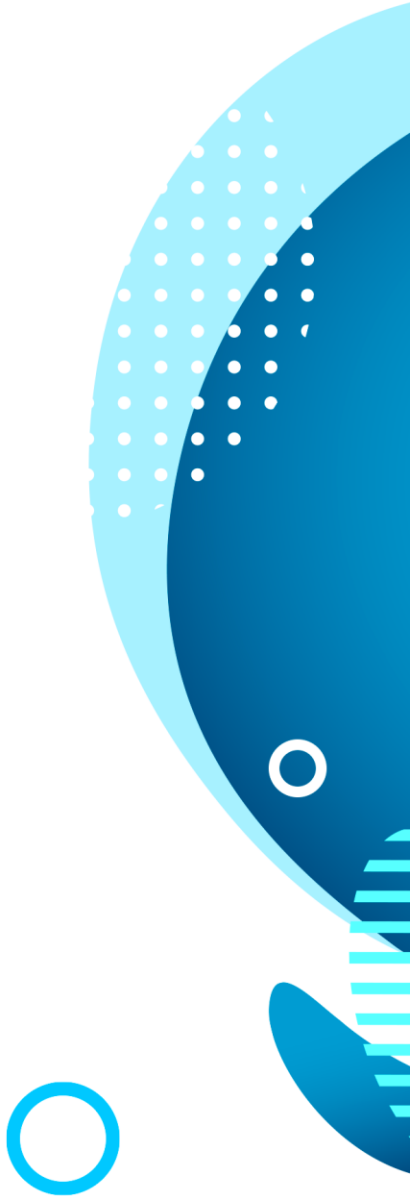



# **OBLIGATIONS RELATED TO PROVIDERS OF SERVICES SUPPORTING CRITICAL OR IMPORTANT FUNCTIONS**





# CRITICAL AND IMPORTANT FUNCTIONS

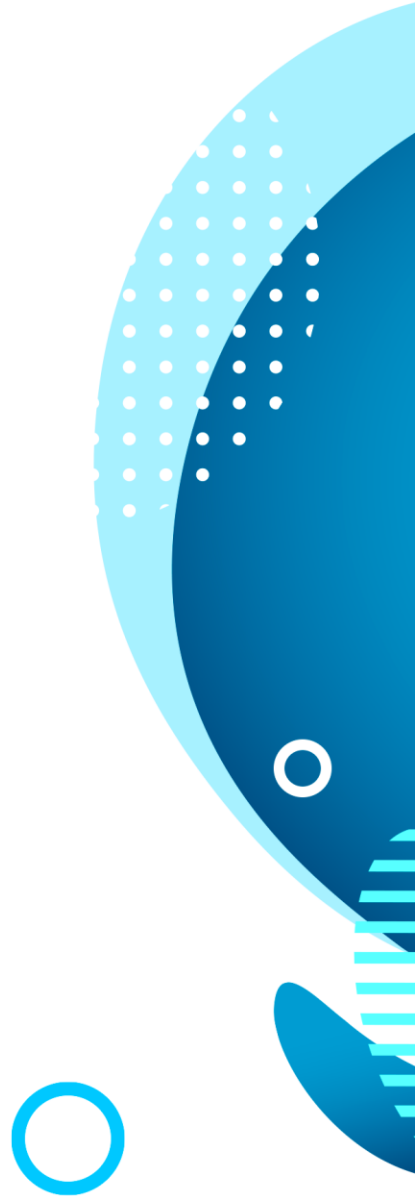
- **Critical and important function:** An activity whose interruption or failure could materially affect the stability of ČSOB or its ability to meet its key obligations. The determination thereof follows the KBC methodology.
  - During the lifetime of the function, its classification can be changed from/to critical and important according to the current impacts.
  - **ICT service supporting critical and important functions:** An ICT service that is essential for the correct and secure functioning of defined critical and important functions.
- 
- 






# OBLIGATIONS FOR CRITICAL OR IMPORTANT FUNCTIONS

- **Purpose of the DORA Amendment (specifically Section 11):** To establish specific measures to ensure that ICT services that support critical or important functions remain resilient to failures and threats. The aim is to minimise the impact on ČSOB and ensure the continuous availability of these services.
- Providers must implement strategies to ensure that, even in the event of a major disruption, operations remain stable and functional.





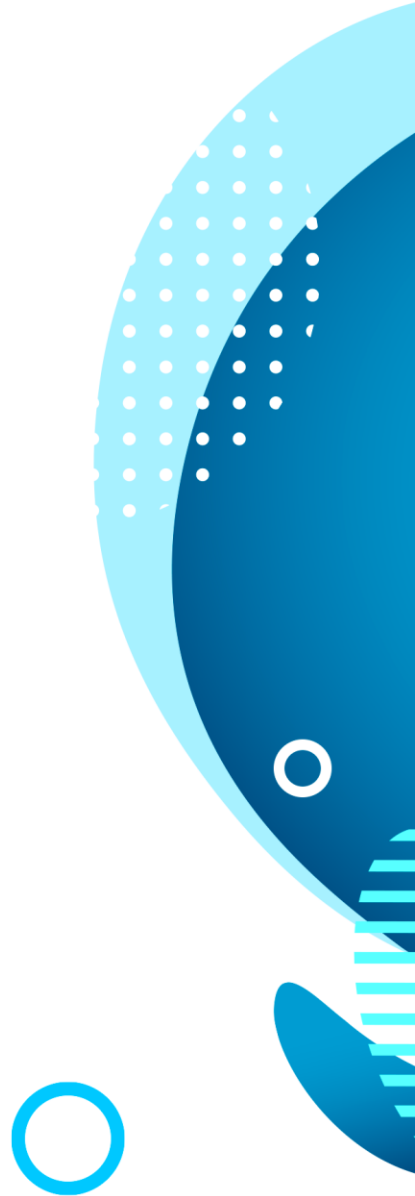
# MONITORING AND REPORTING

- **Regular updates:** The description of ICT services, including performance targets and security measures, shall be reviewed regularly. This ensures that providers, as well as ČSOB, can respond quickly to new threats and adapt to changing requirements and environments.
  - **Reporting of important events:** The provider is obliged to notify ČSOB of any event that could affect the performance of services. This includes immediate (within 24 hours) reporting of failures, cyber attacks or other incidents that may disrupt critical functions.
- 




# CONTINUITY OF OPERATION

- **Continuity plans:** The provider must establish and maintain detailed business continuity plans that include scenarios for handling crisis situations. These plans must be tested regularly to ensure their effectiveness in real incidents.
- **Security measures:** The implementation of advanced technologies and processes to secure ICT services is crucial. Measures must comply with current security standards and be adapted to the nature and severity of the identified risks.



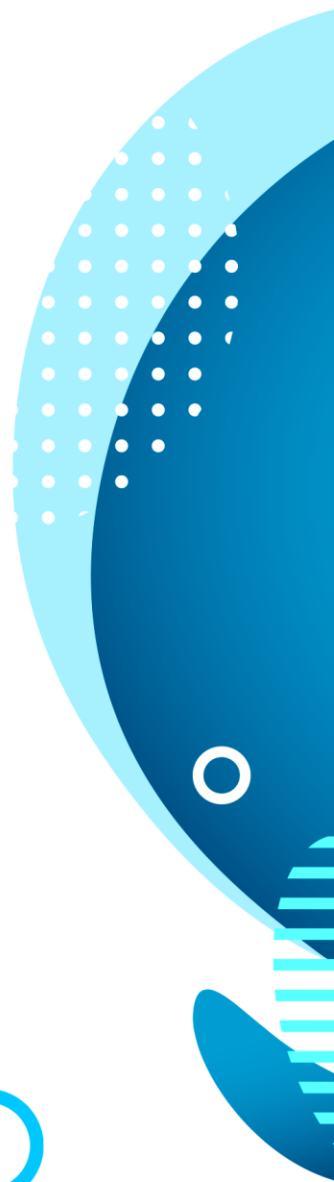



# USE OF CODE LIBRARIES AND TLPT

- **Monitoring code libraries:** The provider must have processes in place to monitor the code libraries in use (including open-source solutions) to ensure that they are up-to-date and free of known vulnerabilities. This includes regular updates and version tracking.
  - **Threat-Led Penetration Testing (TLPT):** Providers must be prepared to test the security of ICT services by simulated cyber attacks (TLPT), which are carried out by ČSOB or a third party authorised by it. These tests ensure that weaknesses in the system are identified and addressed. The results must be shared and used to improve security measures, even if the test is performed independently by the provider.
- 



# RIGHT TO AUDIT; COOPERATION


- **Right to audit:** ČSOB has the right to conduct detailed audits of ICT service providers. These audits may include a review of documentation, security measures, and systems audits. The provider must provide unrestricted access to the data and resources needed for the audit.
  - **Cooperation:** The provider is obliged to fully cooperate with ČSOB and the competent supervisory authorities. This includes providing access to information, participating in audits and inspections and sharing the results of security tests. The provider must also proactively address and remove identified vulnerabilities.
- 
- 



# **KEY TAKEAWAYS AND SUMMARY**

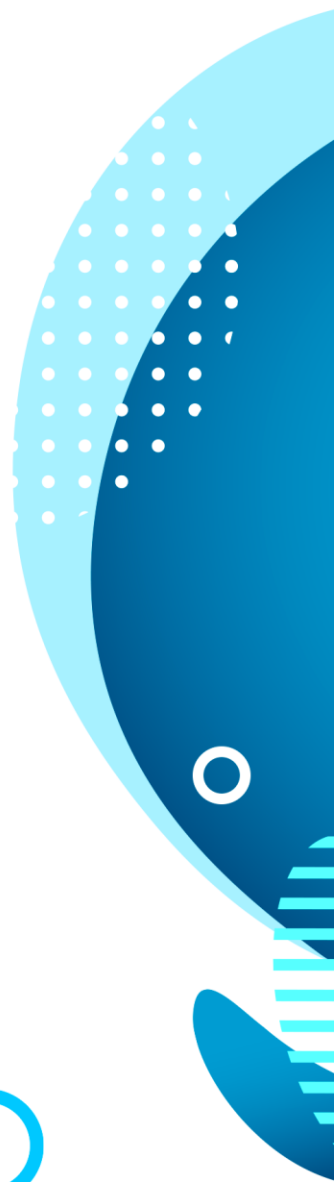




# KEY OBLIGATIONS

- **Risk management:** It is necessary to regularly assess the risks related to ICT service providers and update measures.
  - **Monitoring and auditing:** Regular SLA compliance checks and audits of compliance with contractual security requirements are required.
  - **Security measures:** Providers must implement appropriate security measures, e.g., encryption, backup and continuity management, and must report any incidents without delay.
  - **Management of sub-providers:** Before using sub-providers, providers must obtain approval from ČSOB. Sub-providers must follow the same terms and conditions as providers.
  - **Response to incidents:** Providers must cooperate to quickly identify and remedy incidents and ensure the security of ČSOB data.
  - **Continuity of operation and testing:** Providers must conduct regular tests of continuity plans, including simulation of crisis scenarios.
- 



# PROVIDERS OF SERVICES SUPPORTING CRITICAL OR IMPORTANT FUNCTIONS

- **The number of providers of** services supporting critical or important functions **is not fixed.**
  - **New providers may be identified** based on the identification of new or the reclassification of existing critical or important functions.
  - Similarly, **providers of services supporting critical or important functions may be removed** from the list as a result of a change in the classification of services supported.
- 
- 
- 



# Thank you for your attention

