MORAIS LEITÃO
GALVÃO TELES, SOARES DA SILVA
& ASSOCIADOS

LEGAL ALERT

DORA REGULATION:

NEW REGULATORY TECHNICAL STANDARDS ON ICT SUBCONTRACTING

1. Background

The European Supervisory Authorities (**ESAs**) have recently published the Final Report on the Draft Regulatory Technical Standards (**RTS**) as mandated by Article 30(5) of Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (**DORA Regulation**).

These RTS establish new requirements for financial entities concerning the subcontracting of Information and Communication Technology (**ICT**) services, particularly those supporting critical or important functions, to strengthen ICT risk management in these situations.

Aligned with DORA, the RTS strengthen the digital resilience of financial institutions across the European Union (**EU**), ensuring that risks associated with subcontracting ICT services are adequately managed and mitigated

2. Key aspects of the RTS

2.1. Assessing ICT subcontracting

Article 1 of RTS specifies the elements that financial entities should consider when determining the *(i)* size, *(ii)* risk profile, *(iii)* nature, *(iv)* scale, and *(v)* complexity of their services, activities, and operations. This includes evaluating factors such as:

- The type of ICT services supporting critical or important functions, covered by agreement between the financial entity and ICT third-party service provider and between the latter and its subcontractors;
- The location of ICT subcontractors and their parent companies;
- The length and complexity of the subcontracting chain;
- The nature of data shared with ICT subcontractors and whether the subcontracted ICT services are provided within the EU or in third countries, including where services are delivered and data processed/stored;
- The identification of the ICT subcontractors that are part of the financial entity's corporate group and whether they are registered with or supervised by a competent authority of an EU Member State or of a third country;
- The evaluation of the concentration of ICT services with a single or few subcontractors;
- The ability to switch ICT service providers and the risk of disruptions affecting critical ICT services when using subcontractors.

2.2. Implementing uniform standards for intragroup subcontracting

Article 2 of the RTS establishes that the financial groups' parent company must ensure that these standards apply equally to intragroup subcontractors, which means that entities within the same corporate group are subject to the same oversight as external providers, particularly:

- Financial entities must ensure that intragroup ICT service providers are subject to the same risk assessments and continuous monitoring as third-party service providers;
- Parent company must implement consistent subcontracting practices across all entities within the group, ensuring a cohesive approach to risk management and compliance.

2.3. Due diligence and risk assessment for critical functions

Under **Article 3** of the RTS, financial entities must decide, before engaging an ICT third-party service provider, if such provider is allowed or not to subcontract all or part of any critical functions by assessing:

- If the ICT third-party service provider has implemented a due diligence process to ascertain potential subcontractor's operational and financial abilities;
- If the ICT third-party service provider can identify, notify and inform the financial entity about all subcontractors involved and verify that the agreements with such subcontractors allow the financial entity to comply with legal obligations such as access rights for audits and inspections;
- Whether the ICT third-party service provider has adequate resources, expertise and risk management structures to oversee subcontracted services and that the financial entity has the also resources and structures to oversee both the ICT third-party service provider and its subcontractors;
- The risks related to the location of subcontractors and ICT concentration (including the risks of possible failure).

This assessment should be periodically carried out by financial entities.

2.4. Conditions for Subcontracting Critical ICT Services

According with **Article 4** of the RTS, financial entities must clearly define which ICT services supporting critical or important functions can be subcontracted and under what conditions. When admissible, the contractual agreements between the financial entity and the ICT third-party service provider must include:

- The ICT third-party service provider's responsibility for subcontracted services;
- Requirements for monitoring and reporting on subcontracted services;
- Risk assessment of subcontractor locations and data handling (including its parent company);
- Guarantee of continuity of services and compliance with established security standards;
- The financial entity's rights of access, inspection and audit for subcontracted services;
- The duty to notify in case of material changes to subcontracting arrangements; and
- The financial entity's termination rights.

Any amendments to these agreements in order to comply with DORA Regulation must be promptly implemented and documented.

2.5. Requirements related to the chain of ICT subcontractors:

Article 5 of the RTS establishes requirements for subcontracting related to the chain of the ICT third-party service providers which include:

- Identification of the entire chain of ICT subcontractors involved in providing critical or important services that should be kept up-to-date;
- The financial entity must retain overall responsibility for the ICT services provided by third-party providers meaning that the agreement must allow the monitoring of ICT risks.
- The agreement must include provisions that allow the financial entity to assess the impact of a potentially complex subcontracting chain on the ability to monitor critical functions and on the competent authorities' ability to supervise the financial entity;
- Rights for financial entity to obtain information from the ICT third-party service provider about the subcontracting agreements and relevant performance indicators.

2.6. Material changes in subcontracting of critical ICT services

Article 6 of the RTS outlines the procedures that financial entities must follow when there are material changes to the subcontracting arrangements:

- Implement a notification procedure of any material changes to subcontracting arrangements in which the notice period must be long enough for the financial entity to be able to evaluate the impact of these changes on its risk exposure and to assess whether the ICT third-party service provider can still fulfill its obligations under the agreement or not;
- The ICT third-party service provider should only proceed with the proposed changes to the subcontracting arrangements after the financial entity has either approved them or chosen not to object by the end of the notice period;
- If the financial entity's risk assessment shows that the changes exceed its risk tolerance, it must act before the notice period ends by:
    - Informing the ICT third-party service provider of the risk assessment results; and

- Objecting to the changes and requesting the necessary modifications before the changes are implemented.

2.7. Termination of the contractual agreement

Article 7 of the RTS establishes the conditions where the financial entity has the right to terminate the agreement with the ICT third-party service provider. Such situations are the cases where the ICT third-party service provider:

- Implements material changes despite the financial entity's objection and request for modifications;
- Implements material changes to subcontracting arrangements for critical or important ICT services before the notice period ends and without the financial entity's explicit approval; or
- Subcontracts an ICT service supporting a critical or important function that the contractual agreement does not explicitly allow to be subcontracted.

Next steps

These RTS, once adopted by the European Commission, will become legally binding, requiring immediate actions from financial entities to ensure compliance, such as:

- **Contractual revision:** assess all existing contracts with ICT third-party service providers to ensure they comply with the new RTS requirements, including provisions related to subcontracting and risk management.
- **Risk management frameworks:** strengthen internal processes to incorporate the RTS's demands for due diligence and continuous monitoring of ICT services subcontractors.
- **Engage with subcontractors:** communicate with all ICT services subcontractors to ensure they understand the new requirements and their roles in maintaining compliance.
- **Audit:** prepare for potential regulatory audits by reviewing and updating all relevant documentation, particularly in relation to ICT services subcontracting arrangements.

Final remarks

The introduction of these RTS under DORA represents a crucial development in the EU's efforts to enhance digital operational resilience within the financial sector.

The DORA Regulation will be fully enforceable as of 17 January 2025.

Both, financial entities as well as ICT third-party service providers must act quickly to, respectively align their subcontracting practices and to adapt to these new requirements to avoid non-compliance risks and strengthen their overall operational integrity.

For more detailed advice on how these changes may impact your organization, please contact our team.

Nicole Fortunato
Nuno Sobreira
Ashick Hussein Remetula
Márcia Tomás Pires