DORA: last batch of final draft RTS published

2 August 2024

With less than half a year until DORA becomes applicable on 17 January 2025, the remaining final draft RTS are now available and allow for further preparing implementation of the soon-to-be-standard cybersecurity legislation (cf. here for a general introduction to DORA and here for a deeper dive into the requirements on agreements between financial entities and ICT third-party service providers (**TPSPs**)).

On 17 and 26 July 2024, the Joint Committee (**JC**) of the three European Supervisory Authorities (ESAs) have published joint reports *inter alia* on the finalised drafts of the last outstanding Regulatory Technical Standards (**RTS**) under Regulation (EU) 2022/2554 (Digital Operational Resilience Act – **DORA**).

These final drafts take into consideration the feedback received by the JC during the consultation phase which ended on 4 March 2024. Authorities and corporations were invited to submit comments and responses regarding the consultation drafts of the RTS.

These joint reports include the final drafts of five RTS, which constitute important specifications of certain aspects set out by DORA:

- RTS on Reporting major ICT-related incidents and significant cyber threats;
- RTS Conditions enabling the conduct of the oversight activities;
- RTS specifying the criteria for determining the composition of the joint examination team (**JET**);
- RTS on threat-led penetration testing (**TLPT**); and
- RTS on subcontracting.

Further, the joint reports include final drafts of:

- the Implementing Technical Standard on reporting major ICT-related incidents and significant cyber threats; and
- two guidelines on (i) the estimation of aggregated costs/losses caused by major ICT-related incidents and (ii) oversight cooperation have been published, setting the supervisory authorities on the path to apply DORA's cybersecurity framework beginning 17 January 2025.

The guidelines have already been adopted by the Boards of Supervisors of the three ESAs. The final draft technical standards have been submitted to the European Commission, which will now review with the objective to adopt these legal acts in the coming months.

If you are within DORA's scope of application, you should consider whether these requirements will apply to your required ICT risk management and whether any further implementation will be required to be compliant with DORA. In particular, the publishing of the final drafts provides the opportunity to perform a gap assessment of relevant (contractual) implementations against this final draft set and update your ICT risk management based on the updated requirements.

Please see below a short overview on the contents of the final drafts of the RTS as well as a short summary on the relevant updates compared to the consultation drafts.

RTS on the reporting of major ICT-related incidents and significant cyber threats

This RTS *inter alia* specifies the content of the reports and the deadlines for major ICT-related incidents and significant cyber threats.

Compared to the draft RTS published on 8 December 2023 in the course of the consultation phase, the final draft includes several important changes, including:

- Extension of ICT incident reporting timelines (the consultation included numerous feedback about diverging NIS2 and GDPR requirements, highlighting the challenges coming from falling into the scope of a multitude of cybersecurity legislation);
- Reduction in number of fields to be reported;
- Allowing for single aggregated reporting of financial entities supervised by a single competent authority; and
- Further implementing the proportionality principle by reducing and exempting smaller financial entities from reporting requirements on weekends and public holidays.

RTS on the harmonisation of conditions enabling the conduct of the oversight activities

One of the legislative aims of DORA is to implement a pan-European cybersecurity level playing field by harmonising the conditions enabling oversight and create a new oversight framework for the oversight of critical ICT third–party service provider (CTPPs) in Europe.

This RTS specifies:

- the information to be provided by an TPSP in the application-for a voluntary request to be designated as critical;
- the content, structure and format of the information to be submitted, disclosed or reported by the ICT third-party service to the Lead Overseer, including the template for providing information on subcontracting arrangements; and
- the details of the competent authorities' assessment of the measures taken by CTPPs based on the recommendations of the Lead Overseer.

The main changes in the final draft are related to:

- the scope of the information to be provided by an TPSP in the application to be designated as critical;
- the relevant identification code; and
- the scope and content of the information to be provided by the CTPPs to the Lead Overseer including information about their subcontracting arrangements and the competent authorities' assessment of the risks addressed in the recommendations of the Lead Overseer.

RTS specifying the criteria for determining the composition of the joint examination team (JET)

This RTS specifies certain information, criteria and details to enable the ESAs and the national competent authorities to harmonise the conditions enabling the conduct of oversight, in particular to establish a pan-European oversight framework of CTPPs.

This includes:

- the information to be provided by an TPSP in the application for a voluntary request to be designated as critical;

- the information to be submitted by the TPSPs that is necessary for the Lead Overseer to carry out its duties;
- the criteria for determining the composition of the JET, their designation, tasks, and working arrangements;
- the details of the competent authorities' assessment of the measures taken by CTPPs based on the recommendations of the Lead Overseer.

The JET is composed of staff members from:

- the ESAs;
- the relevant competent authorities supervising the financial entities to which the CTTP provides ICT services;
- the national competent authority designated or established in accordance with the NIS2 Directive responsible for the supervision of an essential or important entity subject to that Directive, which has been designated as CTPP, on a voluntary basis;
- one national competent authority from the Member State where the CTPP is established, on a voluntary basis.

Feedback was limited and focused on providing clarifications on specific limited provisions.

RTS on threat-led penetration testing (TLPT)

This RTS specifies the criteria used for identifying financial entities required to perform TLPT, the requirements and standards governing the use of internal testers, the requirements in relation to scope, testing methodology and approach for each phase of the testing, results, closure and remediation stages and the type of supervisory and other relevant cooperation needed for the implementation of TLPT and for the facilitation of mutual recognition.

Following from the consultation process, several changes to the draft RTS have been made, including:

- A more transparent calculation method relating to the criteria and increasing thresholds used for selecting certain entities to perform TLPT by default;
- Clarifying processes that require extended cooperation between the involved TLPT authorities, in pooled and joint TLPTs; and
- Introducing flexibility in the requirements for both external and internal testers and threat intelligence providers.

RTS on subcontracting (published on 26 July)

The last outstanding final draft to the RTS on subcontracting has been published on 26 July 2024.

This RTS specifies the elements that a financial entity must determine and assess when subcontracting ICT services that support critical and important functions. Additionally, it defines the information that the written subcontract must cover.

The RTS in particular sets out:

- requirements when the use of subcontracted ICT services supporting critical or important functions or material parts thereof by TPSPs is permitted by financial entities and sets out the conditions applying to such subcontracting;
- the requirement for financial entities to assess the risks associated with subcontracting during the precontractual phase; this includes the due diligence process.

- requirements regarding the implementation, monitoring and management of contractual arrangement regarding the subcontracting conditions for the use of ICT services supporting critical or important functions or material parts thereof ensuring that financial entities are able to monitor the entire ICT subcontracting chain of ICT services supporting critical or important functions.

The final draft RTS considers numerous feedback received on the practically important topic. Feedback related mainly to:

- **Proportionality**: A more proportionate approach has been implemented regarding the requirements on subcontracting. Numerous feedback was given that the requirements set out in the draft RTS would be too burdensome when applied to the full chain of ICT service provision.

- **Monitoring of the subcontracting chain**: Respondents suggested that the responsibility to monitor ICT subcontractors should be the responsibility of the TPSPs and so should not be passed to the financial entity (which is not party to the contract), although the financial entity should set out in the contract that the TPSP is monitoring and exercising appropriate oversight over the subcontractor.

  However, although European legislation has made an express policy choice with DORA to enable financial entities to reap the benefits of innovative solutions by not imposing a hard limit on the number of levels in the subcontracting chain when ICT services supporting critical or important services are subcontracted by TPSPs, it still sets out that the financial entity should be able to monitor the subcontracting chain in its entirety.

  With regards to the proportionate application of this requirement, it has been clarified that financial entities are to particularly focus such monitoring on subcontractors that effectively underpin the provision of the service.

- **Imposing requirements on TPSPs**: The RTS imposes specific requirements on ICT third-party service providers, including: a responsibility of the third-party service provider for the provision of information to the financial entity, and requirements on audit and access rights. Respondents were concerned that too many rights for the financial directly would make it difficult to enter into subcontracting arrangements.

- **Termination**: Feedback was given that better ensure a balance between contractual freedom and FE's statutory right to terminate the contract with the TPSP in specific circumstances under material changes on subcontracting arrangements. Feedback was given that right to object to changes in subcontracting arrangements is not realistic, noting that many financial entities lack the necessary bargaining power. The ESAs responded that these termination rights are established by statutory law and thus cannot be abolished by way of RTS.

- **Transition period**: Respondents suggested that ESAs should consider flexibility to enable market participants sufficient time to comply with the final requirements. The ESAs commented that DORA does not foresee transitional periods and therefore the requirements under DORA will apply at its date of application (i.e., 17 January 2025).