Bird & Bird

DORA Contract Compliance: Implications of the Final RTS Subcontracting for Current and Future ICT Agreements

6 August 2024

On 17 and 26 July 2024, the European Supervisory Authorities published the second batch of the final Regulatory Technical Standards ("**RTS**") under the Digital Operational Resilience Act (Regulation (EU) 2022/2554, "**DORA**"). Our colleagues have previously provided a detailed overview of the various RTSs published in the second batch here.

In this article, we will focus specifically on one of these RTSs – the final draft of the RTS *"to specify the elements which a financial entity needs to determine and assess when subcontracting ICT services supporting critical or important functions"* ("**RTS Subcontracting**") published on 26 July 2024 and based on Article 30(5) DORA.

Similar to DORA itself, the RTS Subcontracting contains provisions that relate both to the internal governance of financial entities (e.g., risk management) and those that need to be incorporated directly into contractual agreements with ICT service providers ("**ICT Contracts**"). This article will address exclusively on the latter aspect, examining the specific requirements relating to subcontracting that must be reflected in ICT Contracts.

Contractual Requirements under DORA and the RTSs in General

The DORA text outlines approximately 25 requirements that need to be reflected in the ICT Contracts, mainly in Article 30 DORA. We use the term "approximately" because for some requirements, it is not entirely clear whether they complement other requirements or stand alone as independent requirements.

Additional requirements may be introduced through delegated acts (Article 57 DORA), such as RTSs. However, most RTS provisions focus on the internal governance of financial entities or merely reiterate existing ICT contractual requirements from DORA. This is particularly true for the RTS *"to specify the policy on ICT services supporting critical or important functions"* finalised on 17 January 2024 (in short RTS Policy), which, upon closer inspection, does not establish any truly independent requirements but rather repeats existing requirements or highlights additional contractual options – often to facilitate the incorporation into the ICT Contracts.

Specific Contractual Requirements under the RTS Subcontracting

The situation is notably different when it comes to the RTS Subcontracting. Unlike the DORA itself, which provides only a vague requirement regarding subcontracting in Article 30(2)(a) DORA ("*conditions applying to such subcontracting*"), the RTS Subcontracting introduces a significant number of independent and specific requirements that must be incorporated into ICT Contracts (due to their nature as delegated acts). The draft version of the RTS Subcontracting, dated 27 November 2023, already included approximately 15 additional requirements for ICT Contracts. However, the changes between this draft and the final text are substantial. To highlight just two significant changes:

- Article 4 RTS Subcontracting: Several amendments and additions have been made to the core requirements catalogue of the RTS – for example, a new obligation for ICT service providers to inform the financial entity about material changes in subcontracting (Article 4(1)(j)), or the explicit inclusion of a provision stating that the ICT service provider remains responsible for the delivery of ICT services, including those provided by subcontractors (Article 4(1)(a)).
- Article 5 RTS Subcontracting: Several new contractual requirements have been added compared to the previous draft version – for example, the obligation to identify and keep the entire chain of ICT subcontractors up to date (Article 5(1)(a)/(b)), or the inclusion of elements that enable the financial entity to better assess and manage the risks associated with a long or complex chain of subcontractors (Article 5(3)).

In its final version, the RTS Subcontracting now contains approximately 22 requirements to be reflected in ICT contracts, including the addition of about seven new requirements and the modification of several others, compared to the draft. This means that the requirements imposed by the RTS Subcontracting now almost double the number of requirements imposed by DORA itself (from 25 to 47).

Comparison with Existing Outsourcing Regulations

The importance of the RTS Subcontracting – and the changes introduced in its final draft – becomes even more apparent when compared to existing outsourcing regulations, such as the European Banking Authority's Guidelines on Outsourcing ("**EBA Guidelines**"). While DORA and the EBA Guidelines have different thresholds for applicability (with DORA's threshold for "ICT services" being significantly lower) and different objectives, there is a considerable overlap between the contractual requirements of the two frameworks, particularly since the EBA Guidelines also address cybersecurity and resilience to some extent.

For financial entities or ICT service providers that already have a contractual outsourcing addendum covering all requirements of the EBA Guidelines (in case of ICT service providers often titled "Financial Services Addendum"), most of the 25 contractual requirements directly stemming from DORA are likely already addressed. A detailed gap analysis usually reveals only a minimal "surplus" of requirements introduced by DORA, consisting of less than a handful of additional obligations. For example, the obligation to participate in the financial entity's ICT security programs and training as outlined in Article 30(2)(i) DORA, or the support to be provided to the financial entity during ICT incidents as outlined in Article 30(2)(f) DORA.

However, this assessment changes drastically with the publication of the final draft of the RTS Subcontracting. While the EBA Guidelines do include some subcontracting requirements (notably in paragraphs 76 to 80), the approximately 22 requirements from the RTS Subcontracting far exceed the density of these rules. As a result, what was initially a relatively manageable "surplus" of DORA requirements over the EBA Guidelines has, by the end of July, become a much more extensive set of "excess" obligations requiring attention.

Implications for Financial Entities and ICT Service Providers

At this point, few financial entities or ICT service providers have not yet engaged deeply with DORA, which is set to come into force in just six months. For many affected organisations, DORA compliance projects are already well underway – this includes not only adjustments to internal governance frameworks within financial entities but also revisions to standard contract templates for new agreements and the preparation of amendments to bring existing agreements into DORA compliance. However, with the recent publication of the final RTS Subcontracting, these ongoing projects – particularly those who already considered the former draft of the RTS Subcontracting – require a reassessment.

Each of the new RTS Subcontracting requirements must be carefully examined to determine whether it is already covered in existing (template or legacy) contracts. The devil is often in the details, as many requirements may already be addressed at a basic level, and the task now is to determine whether further adjustments are necessary. For entirely new requirements, the drafting of new clauses will be necessary. These new clauses will need to take account of specific considerations, such as strategic contractual objectives or instructions from the organisation's existing internal governance.

Possible considerations are amongst others:

- A financial entity may need to consider that a (large) ICT service provider might only offer a contractual DORA standard for all clients on a "take it or leave it" basis.
- Conversely, ICT service providers may need to be flexible in responding when financial entities insist on using their own pre-established DORA standard for its countless ICT providers.
- In negotiations, both financial entities and ICT service providers must decide how far they are able and willing to accommodate the other party.

In any case, it is crucial that both financial entities and ICT service providers approach these new requirements with a balanced perspective – and ideally, with sufficient experience in the neighbouring outsourcing regulation. The goal should be to strike a tailored compromise that balances compliance with regulatory mandates and the organisation’s own interests.