LEGAL UPDATE

DORA and subcontracting: final draft RTS published

Date: 15 August 2024

Article 30(2)(a) DORA specifically mentions subcontracting as one of the topics that need to be addressed in an ICT contract. A financial entity can choose not to allow subcontracting, but if it does, it should determine the conditions for subcontracting. As such, Article 30 DORA does not set any standard or requirement as to the content of subcontracting arrangements in an ICT contract.

However, in the context of ICT services supporting - so called - critical or important functions, DORA contains in Article 30 paragraph 5 the task for ESAs to develop draft regulatory technical standards (hereinafter "**RTS**") to specify further the elements which a financial entity needs to determine and assess when subcontracting ICT services.

On 26 July 2024, the ESAs published their final report on the draft Regulatory Technical Standards on subcontracting (hereinafter the "**Final Draft**"), after having published its first draft for these RTS on 8 December 2023 (hereinafter the "**First Draft**").

It is not the first time the ESAs specifically address subcontracting. EBA, ESMA and EIOPA have set guidelines and standards for subcontracting in outsourcing agreements (e.g. EBA Guidelines on outsourcing and cloud contracts, EIOPA Guidelines on outsourcing to cloud service providers and ESMA Guidelines on outsourcing to cloud service providers, hereinafter collectively referred to as the "**Guidelines**"). Hence, one might assume that financial entities already complying with the relevant Guidelines applying to them, would not have any issues with this DORA requirement and that the RTS on subcontracting would not require further amendments to subcontracting stipulations already observing such Guidelines.

This Legal Update answers two questions: how does the Final Draft compare to the First Draft and does the Final Draft potentially affect ICT contracts as related to subcontracting that already comply with the Guidelines?

First Draft compared to the Final Draft

The consultation period following the First Draft has led the ESAs to clarify, change and amend several points. In our view three amendments are specifically relevant for the selection of a service provider and the content of ICT contracts as to subcontracting. These are discussed in the below.

Due Diligence and risk assessment

First of all, Article 1 contains much more detail that needs to be taken into account by a financial entity when applying DORA in order to determine the risk profile of ICT services in relation to subcontracting. Article 3 then requires a due diligence and a risk assessment particularly on the use of subcontractors. One of the elements that stands out in Article 3 Final Draft is that the financial entity shall assess that the ICT service provider ensures that the contractual arrangements with the subcontractors providing ICT services supporting critical or important functions or material parts thereof, allow the financial entity to comply with its own obligations stemming from DORA and all other applicable legal and regulatory requirements (Article 3(1)(c)). The italic part is new and stretches the scope and depth of the risk assessment and due diligence requirements of both the financial entity and the service provider considerably. Whilst it is already best practice to include some of these legal or regulatory requirements in an assessment (take for example the assessment of requirements under the GDPR), imposing that all legal and regulatory requirements are met is of another level. The practicality of complying with this requirement can be expected to be challenging, both on the part of the financial entity and the service provider and will add extra burden in any tender procedure on the both of them. We assume that it may also narrow the circle of potential service providers that are actually capable and willing to comply.

Continuity of ICT Services

The First Draft introduced in Article 4(f) a strict standard to be included in ICT contracts as regards subcontracting, namely:

"(…) *that the ICT third-party service provider is required to ensure the continuous provision of the ICT services supporting critical or important functions, even in case of failure by a subcontractor to meet its service levels or any other contractual obligations*;"

As drafted - at least in a Dutch contract law context - and included in an ICT contract such clause would likely constitute a contractual guarantee. Clearly, this is a far-reaching contractual requirement that - in our view - goes beyond any standard set by DORA itself and may in addition not be technically possible. In such event continuous provision of services will not be realised, only a debate on liability. One may ask if the overall objectives of DORA are served by this requirement of the First Draft.

Fortunately, the Final Draft does not require the ensured continuous provision of the services as such. Rather, Article 4(1)(g) contains the following requirement:

"(..) *that the ICT third-party service provider is required to ensure the continuity of the ICT services supporting critical or important functions throughout the chain of subcontractors in case of failure by an ICT subcontractor to meet its contractual obligations, and that the written contractual agreement with the subcontractor providing the ICT services supporting critical or important functions or material parts thereof includes the requirements on business contingency plans as set out under Article 30(3)(c) of Regulation (EU) 2022/2554 and defines the service levels to be met by the ICT subcontractors in relation to these plans*;"

The most important changes are that the Final Draft puts focus on the continuity of the services throughout the chain of subcontractors in case there is a failure by one of them. This change requirement applies a different angle on continuity and sets a different standard that is still a strict but a less burdensome obligation. Clearly, in the Final Draft the ESAs are tying the subcontracting obligations back to Article 11 and Article 30(3)(c) DORA, which address the ICT business continuity policy, effective response to ICT related incidents and business contingency plans.

Monitoring of the chain of subcontractors

Monitoring the chain of subcontractors is more specifically addressed in Article 5 which has been changed considerably. Financial entities must maintain an ongoing understanding of the overall functioning of the subcontracting chain and ensure appropriate monitoring of its overall functioning. However, this does not mean that each link in the chain must be monitored individually, as was the case in the First Draft, where Article 4 stated that the financial entity must effectively monitor the *entire ICT-subcontracting chain*. Detailed monitoring is only required for those subcontractors that "effectively underpin" the ICT service supporting critical or important functions (Article 5(2) Final Draft).

The key question is what "effectively underpin" means. The ESAs have not clarified this concept, other than to say that this includes subcontractors whose disruption would impair the security or continuity of service provision. Apparently, there can also be a broader circle of subcontractors that underpin the services. An additional complicating factor is that subcontracting is not a defined notion in DORA. The Guidelines defined 'sub-outsourcing', thus giving financial entities some guidance as to which sort of third parties to include as subcontractor in the outsourcing of cloud contract in order to comply. In short, for the contracting practice it means that the scope of the financial entities' obligations as to monitoring the chain of subcontractors - and also of the service provider to further pass on monitoring obligations - remains difficult to demarcate in ICT contracts.

Guidelines vs Final Draft

The expectation is that this RTS would not materially deviate from the Guidelines. Indeed, the RTS address the same topics, in short, responsibility of the service provider for service provisioning despite subcontracting, monitoring and audits, (material) change of subcontracting arrangement including replacement of subcontractor, and the possibility to object and termination rights with respect to such changes.

The big difference is the level of detail added to elements that need to be taken into account when assessing subcontracting and subcontractors. In addition, the Final Draft is much more prescriptive as to the content of subcontracting provisions in ICT contracts than the Guidelines are.

There is more. If subcontracting is permitted the Final Draft takes a different approach than the Guidelines: the Guidelines require that in the agreement between the service provider and the financial entity, it is specified what may not be subcontracted. The Final Draft requires the opposite: inclusion of the critical and important functions that are eligible to be subcontracted.

Further, the Guidelines do not specifically extend due diligence obligations to subcontractors (but only with respect to the service provider). However, a proper due diligence cannot be done without taking into account the entire supply chain. So, if not already part of the obligation pursuant to the Guidelines it would certainly be a best practice. However, the Final Draft explicitly sets out detailed elements that need to be taken into account (Article 1) and also sets rules for the due diligence itself (Article 3). The due diligence requirements are far more detailed than in the First Draft and require a more in-depth analysis. Although the Final Draft does not contain a specific requirement to include the due diligence requirements of Article 3 in the contractual arrangements between the financial entity and its ICT service provider, in practice it can be expected these are likely to become contractual obligations in an ICT contract. Reason for this is that the financial entity is required to periodically reperform the risk assessment during the term of the contract (as per Article 3(2)) and it should also be taken into account if a subcontractor is proposed to be added or replaced during the term. The due diligence and risk assessment affect both existing ICT contracts but - to cater for a flow down of these requirements - also in existing subcontracts.

Also, the requirement set out in Article 4(1)(g) on continuity of services will require change of most of the existing ICT contracts covered by the Guidelines as these do not contain the same standard. A further point of attention would be monitoring the chain of subcontractors: it may be that subcontractors of the subcontractors are not covered sufficiently to meet Article 5 Final Draft because of the different scope (the defined notion of sub-outsourcing versus subcontractor (undefined)).

In sum, other than perhaps expected based on the existing requirements on subcontracting in the Guidelines, ICT contracts that already comply with the Guidelines will need to be reviewed and likely also amended on subcontracting. As often is the case in an ICT contract: the devil is in the detail.
This is a Legal Update by Robert Boekhorst.

For more information:

Robert Boekhorst
+31 30 25 95 578
robertboekhorst@vbk.nl