MEALEY'S® LITIGATION REPORT

Cyber Tech & E-Commerce

Beyond The Implementation Deadline: Bridging Legal, Technical And Contractual Complexity For Ongoing DORA Compliance

By
Fabio Coco

ADVANT Nctm
Milan, Italy

A commentary reprinted from the October 2025 issue of Mealey's Litigation Report: Cyber Tech & E-Commerce

LexisNexis®

Commentary

Beyond The Implementation Deadline: Bridging Legal, Technical And Contractual Complexity For Ongoing DORA Compliance

By
Fabio Coco

[Editor's Note: Fabio Coco is a partner at ADVANT Nctm, member firm of European law association ADVANT. Any commentary or opinions do not reflect the opinions of ADVANT Nctm or LexisNexis®, Mealey Publications™. Copyright © 2025 by Fabio Coco. Responses are welcome.]

The European Union's (EU) Digital Operational Resilience Act (DORA) entered into force on 17th January 2025, meaning that banks, payment institutions, insurance undertakings, investment firms, asset managers, alternative investment fund managers – even crypto-asset service providers and central counterparties – and other in-scope entities have now had to be DORA-compliant for a number of months. Ensuring that systems, contracts and internal procedures are compliant with DORA is being treated as a paramount priority by the vast majority of firms. Most have now progressed beyond preliminary gap analyses and mapping of ICT services to the execution of structured implementation programs.

This is not a one-off compliance task, but rather a new standard for business-as-usual. It requires a continuous and dynamic process of reviewing and enhancing internal policies, risk management frameworks, and incident response procedures as well as revision of contractual arrangements with ICT service providers.

The Regulatory Landscape

Today's financial system is highly digital and interconnected. While this creates opportunities, it also makes the entire system vulnerable to cyber threats and IT disruptions.

To address this risk, the EU created DORA, a new legal framework to make the European financial system more secure.

DORA's impact is extensive: it applies not only to all financial companies in the EU but also to their ICT service providers. This is a major change from previous regulations, which were often fragmented and left significant security gaps.

For example, the pre-existing European Banking Authority (EBA) guidelines on outsourcing cover all outsourcing agreements regardless the type of service involved, but they do not cover other kinds of service agreements that do not qualify as outsourcing. Furthermore, European Securities and Markets Authority (ESMA) and European Insurance and Occupational Pensions Authority (EIOPA) guidelines on cloud outsourcing only apply to cloud services. The existing regulation overlooked various areas of critical importance which are now covered by DORA.

While DORA is an EU regulation, its reach is global. Any financial entity or ICT provider based outside the EU that operates within EU market must also ensure its procedures, policies, and contracts comply with DORA requirements.

Barriers To Full Compliance

Firms face two primary barriers in achieving full compliance with DORA: the complexity of the technical and legal requirements, and the staggered issuance of essential regulations that may cause uncertainty and hesitation.

Firstly, a significant obstacle is the inherent link between technical operations and legal obligations. DORA mandates actions that are fundamentally technical in nature but require precise legal interpretation and implementation. For example, financial entities must classify their ICT services and establish criteria for categorizing ICT-related incidents. These criteria are intrinsically tied to the technical specifications of the services and infrastructure in use and must be accurately "translated" into legally binding and enforceable terms within contracts with ICT providers. For these reasons, the approvals process is complex because any implementation measure requires validation from both internal IT experts, who confirm technical feasibility and accuracy, and legal counsel, who ensure the amendment of contracts is compliant and robust. Clearly, this takes time and may create significant delays.

The second major barrier has been the piecemeal finalization of the DORA legal framework. While the primary Regulation was published on 27 December 2022, the corresponding Regulatory Technical Standards (RTS) and Implementing Technical Standards (ITS) were not released contemporaneously, with some of the delegated regulations being published very close to, or even after, the application date (17 January 2025). Therefore, implementing DORA has been a protracted journey where, so far, the firms, the IT consultants and, of course, the lawyers have had to operate within an evolving legal landscape, continually adapting their strategies as new regulations and Q&A guidance from the European Supervisory Authorities (ESAs) were released. As a consequence, this dynamic and uncertain framework has inevitably extended the timelines for drafting new policies and concluding complex negotiations with ICT service providers.

In practice, this renegotiation and amendment of contracts with ICT service providers has been the single most difficult and delicate challenge in implementing DORA.

While ICT service providers are not directly subject to DORA themselves, the regulation imposes stringent requirements that financial entities must pass on to them contractually. From the provider's perspective, these new terms often represent significant new operational burdens and potential liabilities. This creates a challenging negotiation dynamic where providers may be resistant to accepting the new, more onerous obligations.

The negotiations are particularly intense due to several highly intrusive provisions mandated by DORA.

For instance, requisites regarding unrestricted rights of access, inspection and audit place the onus on the provider to manage the potential operational disruptions this may cause and protect the privacy of their clients.

Exit strategies must also be built into contracts, with ICT service providers required to manage the transition period if the financial entity is to migrate to another ICT service provider. This is unlikely to be commercially convenient.

Additionally, firms will need provisions to govern the relationship between ICT service providers and their sub-contractors. The provider will be responsible for amending existing sub-contractor agreements – a task that will be challenging if subcontractors are reluctant to accept new terms.

Most DORA-mandated contract clauses need to be carefully tailored, both legally and technically, to the specific service being provided. This may hamper the systematic use of standardized, "one-size-fits-all" templates and requires in-depth, case-by-case drafting. Negotiations on contracts regarding ICT services supporting critical or important functions, which are regulated – among others – by the Delegated Regulation (EU) 2024/1773, are even more complex due to the more stringent requirements.

Furthermore, financial entities must ensure these DORA-compliant contracts also align with a broader ecosystem of existing regulations and this adds another layer of complexity to the compliance exercise.

Moving Beyond The Initial Implementation Phase

Looking ahead, the initial implementation challenges are set to evolve into more permanent, and potentially more complex, operational issues.

For instance, new contracts due to be signed will have to be immediately compliant with DORA, meaning

the due diligence and negotiation process with both existing and new ICT service providers will have to take into account all the new requirements set forth by DORA.

Firms will also need to factor in the costs associated with the implementation of DORA in the long term. DORA compliance is not a one-time capital expenditure but rather a significant and ongoing operational expense. Currently, during negotiations, some providers require additional fees to compensate them for the additional liabilities and obligations they have absorbed under DORA-compliant contracts. Moving forwards, we will likely see more complex interactions with ICT service providers, as they will be prepared to challenge the applicability of the most burdensome provisions, such as those regarding the service level agreements, key performance indicators, ICT incident classification and reporting or termination rights and exit plans.

Furthermore, as we move beyond the initial implementation phase, the posture of the authorities will shift from guidance to active supervision and enforcement. In this respect, any identified shortcomings will carry a greater risk of formal sanctions, financial penalties, and significant reputational damage.

Practical Strategies For Ensuring Ongoing DORA Compliance

To overcome the challenges of implementing DORA, financial entities can – and should – establish a multidisciplinary DORA implementation team, comprising legal experts and IT consultants, that are able to handle new problems effectively, understanding and navigating the new complexities that arise from the regulation's specific requirements.

The team should also be equipped to engage in detailed negotiations with ICT service providers, focusing on a clear plan of priorities to ensure compliance with DORA requirements.

This structured approach may prevent future compliance issues and will provide a clear framework for accountability, minimizing operational and legal risks. ■

MEALEY'S LITIGATION REPORT: CYBER TECH & E-COMMERCE
edited by Sheri Melnick
The Report is produced monthly by

1600 John F. Kennedy Blvd., Suite 1655, Philadelphia, PA 19103, USA
Telephone: 1-800-MEALEYS (1-800-632-5397)
Email: mealeyinfo@lexisnexis.com
Web site: lexisnexis.com/mealeys
ISSN 1535-718X