What is the Digital Operational Resilience Act (DORA)? Final Council of the European Union Compromise Texts of the DORA Directive and the DORA Regulation

FINANCIAL INSTITUTIONS, PAYMENT SERVICE PROVIDERS, BANKING

Sep 13, 2022
On 23 June 2022, the Council of the European Union published the consolidated version of the DORA Directive.

The text explains that PSD2 rules on information and communications technology (ICT) security controls and mitigation elements for the authorisation to perform payment services should be changed to align with the DORA Regulation. Also, the PSD2 incident reporting rules should cease to apply for financial entities regulated under PSD2 and subject to DORA, as the DORA rules will apply instead to all operational and security incidents and whether these are payment-related or not.

Other changes to the PSD2 include that:

A payment institution (PI) shall, when applying for authorisation, submit to the competent authorities of the home Member State the procedures and arrangements DORA puts in place for the use of ICT services;
The outsourcing of important operational functions, including ICT systems, to agents, branches or other entities must not be undertaken in a way which weakens the quality of the PI's internal control and the ability of the competent authorities to monitor and retrace the PI's compliance with all of the PSD2 obligations;
As for the management of operational and security risks, Member States must ensure that payment service providers (PSPs) establish a framework with appropriate mitigation measures and control mechanisms. Moreover, PSPs must establish and maintain effective incident management procedures, including for the detection and classification of major operational and security incidents.
On 23 June 2022, the Council also published the consolidated version of the DORA Regulation.

The aim of the DORA Regulation is to introduce more stringent requirements on ICT risk management and ICT-related incident reporting than the ones previously agreed in May 2022 in the revised Network Information Security Directive (NIS2). Hence, the DORA Regulation constitutes lex specialis to NIS2.

Under the DORA Regulation, credit institutions, e-money institutions (EMIs), payment institutions (PIs) and account information service providers (AISPs) should report all operational or security

payment-related incidents previously reported under PSD2, whether such incidents are ICT-related or not.

Scope of the DORA Regulation

The DORA Regulation applies to PIs, AISPs, EMIs, crypto-asset providers as authorised under the Regulation on Markets in Crypto-assets (MiCA) and issuers of asset-referenced tokens, as well as to a wide range of ICT third-party service providers, including providers of cloud computing services, software, data analytics services, and providers of data centres services.

As for payment systems and the provision of payment processing activities, the DORA Regulation explains that the potential systemic cyber risk associated with the use of ICT infrastructures should be addressed at EU level and that the Commission (EC) should swiftly consider the need to enlarge the scope of the DORA Regulation. The Commission must submit, as part of the PSD2 review, a report to the Council and the European Parliament no later than 6 months after the date of entry into force.

Based on this review report, and after consulting the European Banking Authority (EBA), European Securities and Markets Authority (ESMA), European Insurance and Occupational Pensions Authority (EIOPA), European Central Bank (ECB) and the European Systemic Risk Board (ESRB), the Commission may submit, if appropriate and as part of PSD3, a proposal to ensure that all operators of payment systems and entities involved in payment-processing activities are subject to an appropriate oversight, while taking into account existing central bank oversight.

In the meantime, as payment systems and payment processing activities are critical for the functioning of European financial markets, until a harmonised regime and supervision of operators of payment systems and processing entities are put in place at EU level, Member States may draw inspiration from the requirements in the DORA Regulation when applying rules to operators of payment systems and processing entities supervised under their own jurisdictions.

The DORA Regulation imposes, among others:

The identification all ICT-supported business functions, roles and responsibilities and their roles and dependencies with ICT risk;
Protection and prevention measures, as well as detection mechanisms;
ICT Business Continuity Policies;
Backup policies, restoration and recovery methods;
Communication plans enabling a responsible disclosure of major ICT-related incidents or vulnerabilities to clients and counterparts, as well as to the public, as appropriate;
Further harmonisation of ICT risk management tools, methods, processes and policies.It is also foreseen thatthe European Supervisory Authorities (ESAs) will develop Regulatory Technical Standards (RTS) about the specification of such elements;
An ICT-related incident management process;
A classification of ICT-related incidents and cyber threats;
The reporting of major ICT-related incidents and voluntary notification of significant cyber threats;
The testing of ICT tools and systems;
Key principles for the management of ICT third party risk, such as adopting and regularly reviewing a strategy on ICT third-party risk, taking into account the multi-vendor strategy in the provision on ICT risk management framework, if applicable. Moreover, financial entities must identify alternative solutions and develop transition plans enabling them to remove the contracted functions and the relevant data from the ICT third-party service provider and securely and integrally

transfer them to alternative providers or reincorporate them in-house, in case this becomes necessary;
Pre-contractual assessment of ICT concentration risk in relation to ICT services supporting critical or important functions;
Key contractual provisions which cover, among others, the locations, namely the regions or countries, where the contracted or subcontracted functions and ICT services are to be provided and where data is to be processed, including the storage location, and the requirement for the ICT third-party service provider to notify in advance the financial entity if it envisages changing such locations;
The designation of critical ICT third-party service providers: the ESAs must designate the ICT third-party service providers that are critical for financial entities and appoint as Lead Overseer for each critical ICT third-party service provider the ESA that is responsible. The ICT third-party service provider must, as a consequence, notify the financial entities to which they provide services of their designation as critical ICT third-party service providers.
The provisional indicative European Parliament Plenary sitting date for the final approval of the DORA Directive and the DORA Regulation is currently scheduled for 9 November 2022. The current text is not to be modified further.

Monica is founder and managing director of Trust EU Affairs and can be reached at monacom@trusteuaffairs.com

Monica Monaco
Founder & Managing Director, Trust EU Affairs

Based in Brussels for the past 18 years, Monica is the founder and managing director of TrustEuAffairs. She is a member of the Society of European Affairs Professionals (SEAP) since 2004, and served as a member of the SEAP Board from 2012 to 2015. Monica is a member of the Europol Virtual Currencies Taskforce and also a member of the European Commission Payment Systems Market Expert Group (PSMEG). Monica has been Senior Manager for EU Regulatory Affairs in the Legal Department of Visa Europe for more than ten years, responsible for relations with the European Commission, Parliament and Council, as well as with various national regulators. Before joining Visa Europe she worked as a consultant for both Andersen, Deloitte & Touche and the OECD in Paris, as well as the Council of Europe in Strasbourg, dealing with a variety of financial services matters. Monica can be reached at: monacom@trusteuaffairs.com