Seqlense

La réglementation DORA (Digital Operational Resilience Act) est devenue pleinement applicable et exécutoire le 17 janvier 2025

Cécile Henry
General Manager, CLR & Co-Founder

DORA - 17 Janvier 2025

Le Digital Operational Resilience Act (DORA) est une réglementation clé de l'Union européenne visant à renforcer la cybersécurité et la résilience opérationnelle des institutions financières et de leurs fournisseurs de services tiers. En tant qu'entités financières de droit européen, les Crypto-Asset Service Providers (CASP) sont également concernés par cette réglementation. Avec MiCA (Markets in Crypto-Assets Regulation), DORA est l'autre cadre réglementaire européen clé qui impacte les CASP. Alors que MiCA se concentre sur les aspects réglementaires et financiers des marchés de crypto-actifs, DORA est liée à la cybersécurité et à la résilience opérationnelle des institutions financières, y compris les CASP.

Rappel du calendrier

Le calendrier de la réglementation Dora est le suivant :
- 24 septembre 2020 : Proposition de DORA par la Commission européenne dans le cadre du Paquet Finance Numérique dans le but d'améliorer la résilience aux cybermenaces dans le secteur financier.
- 10 mai 2022 : Accord provisoire entre le Parlement européen et le Conseil.
- 27 décembre 2022 : Publication au Journal officiel de l'UE.
- 16 janvier 2023 : Entrée en vigueur de Dora
- 17 janvier 2024 : Première vague de normes politiques.
- 17 juillet 2024 : Deuxième vague de normes politiques et acte délégué.
- 17 janvier 2025 : Entrée en vigueur du DORA

Éléments clés

DORA vise à établir un cadre harmonisé pour les entités financières afin de garantir leur résilience numérique. Ce règlement s'applique, entre autres, aux banques, aux compagnies d'assurance, aux CASP, aux établissements de paiement, aux entreprises d'investissement et aux fournisseurs de TIC critiques.

DORA comprend cinq piliers principaux qui sont :

1. La gestion des risques liés aux TIC avec
-> La mise en œuvre d'un cadre solide de gestion des risques liés aux TIC ;
-> L'identification, la classification et l'atténuation continues des menaces liées aux TIC et la détection rapide des anomalies ;
-> Une gouvernance appropriée impliquant des rôles et des responsabilités clairs.

2. La gestion, la classification et le signalement des incidents liés aux TIC, avec
-> un rapport normalisé sur les incidents majeurs liés aux TIC à l'intention des régulateurs ;
-> une classification harmonisée des cybermenaces afin de garantir l'efficacité du signalement des cyberincidents dans l'ensemble de l'UE.

Seqlense

La réglementation DORA (Digital Operational Resilience Act) est devenue pleinement applicable et exécutoire le 17 janvier 2025

Cécile Henry
General Manager, CLR & Co-Founder

DORA - 17 Janvier 2025

3. Test de résilience opérationnelle numérique avec
-> des tests réguliers des systèmes et contrôles TIC, y compris des tests de pénétration et des exercices de red-teaming (tests d'intrusion) ;
-> des tests avancés pour les entités financières importantes, avec des tests de pénétration basés sur la menace (TLPT) au moins tous les trois ans pour les institutions critiques.

4. Gestion des risques liés aux TIC par des tiers, avec
-> un cadre de surveillance pour les fournisseurs tiers de TIC, y compris les fournisseurs de services cloud ;
-> la gestion des risques associés aux fournisseurs tiers de TIC.

5. Partage de l'information avec :
-> des dispositions pour le partage des informations sur les cybermenaces entre les entités financières :
-> des dispositions pour le partage d'informations sur les cybermenaces entre les entités financières.

En date du 16 janvier 2025, l'AMF a également annoncé l'application des orientations révisées élaborées par les autorités européennes de supervision dans le cadre de la réglementation DORA **:** https://www.amf-france.org/fr/actualites-publications/actualites/resilience-operationnelle-lamf-applique-les-orientations-revisees-de-lesma-sur-la-cooperation-de#:~:text=Le%20r%C3%A8glement%20DORA%20(2022%2F2554,de%20la%20communication%20(TIC).

Sources :
https://www.europarl.europa.eu/RegData/etudes/ATAG/2022/738197/EPRS_ATA(2022)738197_FR.pdf
https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng

Seqlense

Digital Operational Resilience Act (DORA) became fully applicable and enforceable on 17 January 2025

Cécile Henry
General Manager, CLR & Co-Founder

DORA - 17 Janvier 2025

The Digital Operational Resilience Act (DORA) is a key regulation in the European Union aiming to strengthen the cyber security and operational resilience of financial institutions and their third-party service providers. As financial entities under European law, Crypto-Asset Service Providers (CASPs) are also concerned by this regulation. With MiCA (Markets in Crypto-Assets Regulation), DORA is the other key European regulatory framework that impacts CASPs. While MiCA focuses an the regulatory and financial aspects of crypto-asset markets, DORA is related to cybersecurity and operational resilience for financial institutions, including CASPs.

Reminder of the timeline

The timeline of Dora regulation is as follows:
- 24 September 2020: Proposal of DORA by the European Commission as part of the Digital Finance Package with the aim to improve the resilience to cyber threats in the financial sector.
- 10 May 2022: Provisional agreement between European Parliament and Council.
- 27 December 2022: Publication in the Official Journal of the EU.
- 16 January 2023: Entry into force of Dora
- 17 January 2024: First wave of policy standards.
- 17 July 2024: Second wave of policy standards and Delegated Act.
- 17 January 2025: Entry into application of DORA

Key elements

DORA aims to establish a harmonised framework for financial entities in order to ensure their digital resilience. This regulation applies, among others, to banks, insurance companies, CASPs, payment institutions, investment firms, and critical ICT providers.

DORA encompasses five main pillars which are:

1. ICT risk management with:
the implementation of a robust ICT risk management framework;
-> a continuous identification, classification and mitigation of ICT threats and prompt detection of anomalies;
-> an appropriate governance involving clear roles and responsibilities.

2. ICT incident management, classification and reporting with:
-> standardised reporting of major ICT-related incidents to regulators;
-> harmonised classification of cyber threats in order to ensure effective cyber incident reporting across the EU.

3. Digital operational resilience testing with:
-> regular testing of ICT systems and controls, including penetration testing and red team exercises;
-> advanced testing for significant financial entities, with Threat-Led Penetration Testing (TLPT) at least every three years for critical institutions.

Seqlense

Digital Operational Resilience Act (DORA) became fully applicable and enforceable on 17 January 2025

Cécile Henry
General Manager, CLR & Co-Founder

DORA - 17 Janvier 2025

4. ICT third-party risk management with:
-> oversight framework for ICT third-party providers, including cloud service providers;
-> management of risk associated with ICT third-party providers.

5. Information sharing with:
-> arrangements for sharing cyber threat information among financial entities.

Sources :
https://www.europarl.europa.eu/RegData/etudes/ATAG/2022/738197/EPRS_ATA(2022)738197_FR.pdf
https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng