SOPHOS

Guide Sophos sur la loi DORA (Digital Operational Resilience Act) concernant la résilience opérationnelle numérique

Un livre blanc Sophos. Avril 2024

À propos de la loi DORA

Le règlement sur la résilience opérationnelle numérique du secteur financier (règlement 2022/2554 de l'Union européenne) (« DORA » ou le « règlement ») est un règlement de l'Union européenne visant à garantir la résilience numérique des entités financières[1] au sein de l'UE contre les incidents et les perturbations opérationnelles liés aux technologies de l'information et de la communication (TIC). La Commission européenne a finalisé le règlement DORA le 16 janvier 2023. Les exigences de ce règlement entreront en vigueur et s'appliqueront à partir du 17 janvier 2025.

Champ d'application de la loi DORA

La loi DORA s'applique à toutes les « entités du secteur financier » de l'UE, y compris les banques, les sociétés d'investissement, les établissements de crédit, les compagnies d'assurance, les plateformes de financement participatif, ainsi qu'aux tiers importants offrant aux institutions financières des services liés aux TIC, telles que les éditeurs de logiciels, les fournisseurs de services hébergés dans le cloud et les datacenters, les fournisseurs de services d'analyse de données, et bien d'autres encore. L'article 2 du règlement (UE) 2022/2554 identifie les entités suivantes visées par la loi[2].

LISTE DES ENTITÉS FINANCIÈRES VISÉES PAR LE RÈGLEMENT :

- Établissements de crédit
- Institutions de paiement
- Prestataires de services d'information sur les comptes
- Établissements de monnaie électronique
- Sociétés d'investissement
- Fournisseurs de services de crypto-actifs et émetteurs de jetons se référant à un ou des actifs
- Dépositaires centraux de titres
- Contreparties centrales
- Plateformes de négociation
- Référentiels commerciaux
- Sociétés de gestion
- Gestionnaires de fonds d'investissement alternatifs
- Prestataires de services de communication de données
- Entreprises d'assurance et de réassurance
- Intermédiaires d'assurance, intermédiaires de réassurance et intermédiaires d'assurance à titre accessoire
- Institutions de retraite professionnelle
- Agences de notation
- Administrateurs d'indices de référence d'importance critique
- Prestataires de services de financement participatif
- Référentiels de titrisation
- Prestataires tiers de services TIC

Pourquoi le règlement DORA ?

Le règlement DORA « prend acte du fait que les incidents liés aux TIC et le manque de résilience opérationnelle sont susceptibles de compromettre la solidité de l'ensemble du système financier, même s'il existe un capital "adéquat" pour les catégories de risques traditionnelles »[3]. Le cadre réglementaire DORA fixe des exigences relatives à la sécurité des réseaux et des systèmes d'information des entités du secteur financier afin d'améliorer la cybersécurité dans l'ensemble du secteur financier de l'Union européenne. Ces exigences aident les entités financières à réduire l'impact potentiel des menaces numériques sur la continuité de leurs activités, leur responsabilité juridique, les pertes financières et la dégradation de leur réputation.

Exigences de la loi DORA

Afin d'atteindre un niveau commun élevé de résilience opérationnelle numérique, le présent règlement définit des exigences uniformes concernant la sécurité des réseaux et des systèmes d'information qui soutiennent les processus opérationnels des entités financières[4], comme suit :

1. **Gestion des risques liés aux TIC (ICT Risk Management)** : les entités financières doivent disposer d'un cadre de gestion des risques liés aux TIC solide, complet et bien documenté, faisant partie de leur système global de gestion des risques, qui leur permet de répondre aux risques liés aux TIC de manière rapide, efficace et complète, et de garantir un niveau élevé de résilience opérationnelle numérique[5].
2. **Processus de gestion des incidents liés aux TIC (ICT-Related Incident Management Process)** : les entités financières doivent enregistrer tous les incidents liés aux TIC et les cybermenaces importantes. Les entités financières doivent mettre en place des procédures et des processus appropriés pour assurer une surveillance, un traitement et un suivi cohérents et intégrés des incidents liés aux TIC, afin de garantir que les causes profondes sont identifiées, documentées et traitées en vue d'éviter que de tels incidents ne se reproduisent[6].
3. **Test de résilience opérationnelle numérique (Digital Operational Resilience Testing)** : pour garantir que les entités financières soient prêtes à faire face aux incidents liés aux TIC, la loi DORA définit des normes communes en mettant l'accent sur les tests de résilience à mener par ces entités, « telles que l'évaluation et l'analyse des vulnérabilités, les analyses open source, l'évaluation de la sécurité

des réseaux, l'analyse des lacunes, l'examen de la sécurité physique, des questionnaires et des solutions logicielles d'analyse, l'examen du code source lorsqu'une telle opération est possible, des tests basés sur des scénarios, des tests de compatibilité, des tests de performances, des tests de bout en bout et des tests de pénétration »[7].

4. **Gestion des risques liés aux TIC tierces (TPRM : Third-Party Risk Management) :** reconnaissant l'importance croissante des fournisseurs de services TIC tiers, la loi DORA exige que les entités financières « gèrent le risque lié aux tiers en matière de TIC en tant que composante intégrante du risque TIC au niveau du framework global de gestion des risques TIC »[8] par le biais d'accords contractuels tels que l'accessibilité, la disponibilité, l'intégrité, la sécurité, et la protection des données personnelles ; des droits de résiliation clairs ; entre autres.

5. **Partage d'informations et de renseignements (Information and Intelligence Sharing)** : dans le but de renforcer la capacité collective des institutions financières à identifier et à combattre les risques liés aux TIC, la loi DORA les encourage à « échanger entre elles des informations et des renseignements sur les cybermenaces, notamment des indicateurs de compromission, des tactiques, des techniques et des procédures, des alertes de cybersécurité et des outils de configuration, dans la mesure où ce partage d'informations et de renseignements :

   A. vise à améliorer la résilience opérationnelle numérique des entités financières, notamment en sensibilisant aux cybermenaces, en limitant ou en empêchant la capacité des cybermenaces à se propager, en soutenant les capacités de défense, les techniques de détection des menaces, les stratégies de mitigation ou les différentes étapes de réponse et de rétablissement après une attaque ;

   B. se déroule au sein de communautés composées d'entités financières de confiance ;

   C. est mise en œuvre au moyen de dispositifs d'échange d'informations qui protègent le caractère potentiellement sensible des informations partagées et qui sont régis par des règles de conduite dans le plein respect du secret des affaires (business confidentiality), de la protection des données personnelles conformément au règlement (UE) 2016/679 et aux lignes directrices sur les politiques en matière de concurrence. »[9]

6. **Cadre de surveillance des fournisseurs tiers de TIC critiques (Oversight Framework of Critical ICT Third-Party Providers)** : le comité mixte (Joint Committee), conformément à l'Article 57(1) des Réglementations (EU) No 1093/2010, (EU) No 1094/2010 et (EU) No 1095/2010, établit le forum de surveillance (Oversight Forum) en tant que sous-comité chargé de soutenir les travaux du comité mixte (Joint Committee) et du superviseur principal (Lead Overseer) cité par l'Article 31(1), point b), dans le domaine du risque tiers lié aux TIC au niveau de l'ensemble des secteurs financiers. Le forum de surveillance (Oversight Forum) prépare les projets de positions communes et les projets de loi communs du comité mixte (Joint Committee) dans ce domaine.

Le forum de surveillance (Oversight Forum) discute régulièrement des évolutions pertinentes en matière de risques et de vulnérabilités liés aux TIC et promeut une approche cohérente dans la surveillance des risques liés aux tiers en matière de TIC au niveau de l'Union.[10].

DORA et NIS 2

Les réglementations DORA et NIS 2 sont deux éléments essentiels de la législation européenne en matière de cybersécurité. La directive NIS 2 (Directive (UE) 2022/2555) est une loi législative qui vise à atteindre un niveau commun élevé de cybersécurité dans l'ensemble de l'Union européenne.[11]

La relation entre DORA et NIS 2 est la suivante : NIS 2 vise à améliorer la cybersécurité et à protéger les infrastructures critiques dans l'UE, tandis que DORA répond à la dépendance croissante du secteur financier au sein de l'UE à l'égard des technologies numériques et vise à garantir que le système financier reste fonctionnel même en cas de cyberattaque.

Il est important de souligner que NIS 2 est une directive européenne. D'ici le 17 octobre 2024, les États membres doivent adopter et publier les mesures nécessaires pour se conformer à la directive NIS 2[11]. La loi DORA est un règlement européen[12] qui sera applicable en l'état dans tous les pays de l'UE à partir du 17 janvier 2025.

L'article 1(2) de la loi DORA prévoit que, concernant les entités financières couvertes par la directive NIS 2 et ses règles de transposition nationales correspondantes, la réglementation DORA sera considérée comme une loi juridique de l'Union spécifique au secteur et répondant aux exigences de l'article 4 de la directive NIS 2[12]. DORA agit en tant que « *lex specialis* » par rapport à NIS 2[13,14] pour le secteur financier, un

principe qui stipule qu'une loi spécifique prévaut sur une loi générale. Ainsi, pour les entités financières couvertes par DORA, ce texte prévaut sur NIS 2. Toutefois, un tel cas de figure ne signifie pas que les obligations NIS 2 ne soient plus applicables aux entités concernées par les deux textes.

Sanctions en cas de non-respect de la loi DORA

Les sanctions potentielles associées à la loi DORA peuvent être importantes et, contrairement au RGPD et/ou NIS 2, inciter l'entreprise à s'y conformer en lui imposant des amendes sur une base journalière. Les organisations jugées non conformes par l'organisme de contrôle compétent peuvent se retrouver soumises à une sanction récurrente représentant 1 % du chiffre d'affaires global quotidien moyen de l'année précédente, pendant une durée maximale de six mois, jusqu'à ce qu'elles soient conformes. L'organe de contrôle peut également émettre des mises en demeure, des avis de résiliation, des sanctions pécuniaires supplémentaires et des avis publics.[15].

Calendrier de déploiement de la loi DORA

La loi DORA a été proposée pour la première fois par la Commission européenne en septembre 2020. Elle est entrée en vigueur le 16 janvier 2023. Les entités financières et les fournisseurs de services TIC tiers ont jusqu'au 17 janvier 2025 pour préparer la loi DORA et sa mise en œuvre. Le premier lot de normes techniques en matière de réglementation (RTS : Regulatory Technical Standards), et de normes techniques en matière de mise en œuvre (ITS : Implementing Technical Standards) a été publié le 17 janvier 2024. Le deuxième lot de ces normes est en cours de consultation.

1. L'accent mis sur les « entités financières » plutôt que sur les « institutions financières » démontre l'approche adoptée par l'UE pour aborder la résilience opérationnelle numérique du secteur financier de manière globale, en reconnaissant la nature interconnectée et numérique des systèmes financiers actuels. Cette approche garantit que le cadre réglementaire peut s'adapter au paysage changeant des services financiers, où les frontières traditionnelles entre les différents types d'activités financières sont devenues de plus en plus floues.
2. À l'inverse, l'article 2 paragraphe 3 identifie également les entités auxquelles DORA ne s'applique pas, notamment les gestionnaires de fonds d'investissement alternatifs, les entreprises d'assurance et de réassurance, les institutions de retraite professionnelle qui gèrent des régimes de retraite, les personnes morales exemptées par d'autres lois de l'UE, les organismes d'assurance et de réassurance et les intermédiaires d'assurance secondaire, ainsi que les offices de chèques postaux.
3. https://www.digital-operational-resilience-act.com/#:~:text=DORA%20sets%20uniform%20requirements%20for,platforms%20or%20data%20analytics%20services.
4. https://www.digital-operational-resilience-act.com/Article_1.html
5. https://www.digital-operational-resilience-act.com/Article_6.html
6. https://www.digital-operational-resilience-act.com/Article_17.html
7. https://www.digital-operational-resilience-act.com/Article_25.html
8. https://www.digital-operational-resilience-act.com/Article_28.html
9. https://www.digital-operational-resilience-act.com/Article_45.html
10. https://www.digital-operational-resilience-act.com/Article_32.html
11. https://www.nis-2-directive.com/
12. https://www.digital-operational-resilience-act.com/
13. https://www.dora-info.eu/dora/recital-16/
14. https://www.ebf.eu/wp-content/uploads/2021/06/EBF-key-messages-on-NIS2-proposal.pdf
15. https://www.orrick.com/en/Insights/2023/01/5-Things-You-Need-to-Know-About-DORA

Ce document ne constitue pas un avis juridique et ne reflète pas les opinions de Sophos ou de ses employés. Les entreprises doivent consulter leur propre avocat pour obtenir des conseils juridiques sur les lois et réglementations.

© Copyright 2024. Sophos Ltd. Tous droits réservés.
Immatriculée en Angleterre et au Pays de Galles N° 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, Royaume-Uni.
Sophos est la marque déposée de Sophos Ltd. Tous les autres noms de produits et de sociétés mentionnés sont des marques ou des marques déposées appartenant à leurs propriétaires respectifs.

2024-04-09 (WP-MP)

SOPHOS