Note juridique sur le règlement DORA

RÈGLEMENT (UE) 2022/2554 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) no 1060/2009, (UE) no 648/2012, (UE) no 600/2014, (UE) no 909/2014 et (UE) 2016/1011 :

L'OBJET DU REGLEMENT	LES ORGANISMES CONCERNES	LES MESURES A METTRE EN PLACE
Améliorer la résilience opérationnelle numérique des acteurs des services financiers face aux risques grandissants liés à la digitalisation des entreprises et à l'augmentation de la cybercriminalité.	• Les établissements de crédit ; • Les établissements de paiement, y compris les établissements de paiement exemptés en vertu de la directive (UE) 2015/2366 ; • Les prestataires de services d'information sur les comptes ; • Les établissements de monnaie électronique, y compris les établissements de monnaie électronique exemptés en vertu de la directive 2009/110/CE ; • Les entreprises d'investissement ; • Les prestataires de services sur crypto-actifs agréés en vertu du règlement du Parlement européen et du Conseil sur les marchés de crypto-actifs, et modifiant les règlements (UE) no 1093/2010 et (UE) no 1095/2010 et les directives 2013/36/UE et (UE) 2019/1937 (ci-après dénommé « règlement sur les marchés de crypto-actifs ») et les émetteurs de jetons se référant à un ou des actifs ; • Les dépositaires centraux de titres ; • Les contreparties centrales ; • Les plates-formes de négociation ; • Les référentiels centraux ; • Les gestionnaires de fonds d'investissement alternatifs ; • Les sociétés de gestion ; • Les prestataires de services de communication de données ; • Les entreprises d'assurance et de réassurance ; • **Les intermédiaires d'assurance, les intermédiaires de réassurance et les intermédiaires d'assurance à titre accessoire ;** • Les institutions de retraite professionnelle ; • Les agences de notation de crédit ; • Les administrateurs d'indices de référence d'importance critique ;	• Gouvernance du risque informatique ; • Formation à la résilience opérationnelle numérique (article 12 règlement DORA) ; • Analyse du système informatique ; • Gestion des risques informatiques ; • Conduite de tests de résilience ; • Encadrement des risques liés aux prestataires SI (article 28 du règlement DORA) ; • Mécanismes d'échange d'information sur les risques (article 13 règlement DORA).

Document créé le 17 juin 2024, modifié le 10 septembre 2024

	• Les prestataires de services de financement participatif ; • Les référentiels des titrisations ; • Les prestataires tiers de services TIC. **LES CAS D'EXEMPTIONS :** • Les gestionnaires de fonds d'investissement alternatifs visés à l'article 3, paragraphe 2, de la directive 2011/61/UE ; • Les entreprises d'assurance et de réassurance visées à l'article 4 de la directive 2009/138/CE ; • Les institutions de retraite professionnelle qui gèrent des régimes de retraite qui, ensemble, ne comptent pas plus de quinze affiliés au total ; • Les personnes physiques ou morales exemptées en vertu des articles 2 et 3 de la directive 2014/65/UE ; • **Les intermédiaires d'assurance, intermédiaires de réassurance et intermédiaires d'assurance à titre accessoire qui sont des <u>microentreprises ou des petites ou moyennes entreprises</u> ;** • Les offices des chèques postaux visés à l'article 2, paragraphe 5, point 3), de la directive 2013/36/UE.	

La directive européenne et le règlement DORA (pour « Digital Operational Resilience Act ») ont pour objectif d'améliorer la résilience opérationnelle numérique des acteurs des services financiers face aux risques grandissants liés à la digitalisation des entreprises et à l'augmentation de la cybercriminalité.

Cette notion de résilience doit se comprendre comme la capacité pour une entreprise de la communauté européenne de pouvoir **<u>faire face à un risque d'attaque ou de panne sur son système informatique</u>** et sera pleinement applicable à l'ensemble des Etats Membres à partir du <u>17 janvier 2025</u>.

La directive DORA est issue du projet de règlement sur la résilience opérationnelle numérique adopté le 10 novembre 2022 par le Parlement européen. La directive ainsi que son règlement sont entrés en vigueur le 16 janvier 2023.

L'objectif de la directive DORA est d'harmoniser et de simplifier les réglementations et les outils pour permettre de diminuer la multiplicité de réglementations actuellement en vigueur à travers l'UE. Cela permettra notamment de diminuer les risques TIC (Technologies de l'Information et de la Communication) en cybersécurité.

Les organismes concernés par DORA sont définis à l'article 2 de ladite directive :

- Les établissements de crédit ;

- Les établissements de paiement, y compris les établissements de paiement exemptés en vertu de la directive (UE) 2015/2366 ;
- Les prestataires de services d'information sur les comptes ;
- Les établissements de monnaie électronique, y compris les établissements de monnaie électronique exemptés en vertu de la directive 2009/110/CE ;
- Les entreprises d'investissement ;
- Les prestataires de services sur crypto-actifs agréés en vertu du règlement du Parlement européen et du Conseil sur les marchés de crypto-actifs, et modifiant les règlements (UE) no 1093/2010 et (UE) no 1095/2010 et les directives 2013/36/UE et (UE) 2019/1937 (ci-après dénommé « règlement sur les marchés de crypto-actifs ») et les émetteurs de jetons se référant à un ou des actifs ;
- Les dépositaires centraux de titres ;
- Les contreparties centrales ;
- Les plates-formes de négociation ;
- Les référentiels centraux ;
- Les gestionnaires de fonds d'investissement alternatifs ;
- Les sociétés de gestion ;
- Les prestataires de services de communication de données ;
- Les entreprises d'assurance et de réassurance ;
- **Les intermédiaires d'assurance, les intermédiaires de réassurance et les intermédiaires d'assurance à titre accessoire** ;
- Les institutions de retraite professionnelle ;
- Les agences de notation de crédit ;
- Les administrateurs d'indices de référence d'importance critique ;
- Les prestataires de services de financement participatif ;
- Les référentiels des titrisations ;
- Les prestataires tiers de services TIC.

Il est prévu dans ce même article des **cas d'exemption** pour lesquels le règlement DORA ne va pas s'appliquer :

- Les gestionnaires de fonds d'investissement alternatifs visés à l'article 3, paragraphe 2, de la directive 2011/61/UE ;
- Les entreprises d'assurance et de réassurance visées à l'article 4 de la directive 2009/138/CE ;
- Les institutions de retraite professionnelle qui gèrent des régimes de retraite qui, ensemble, ne comptent pas plus de quinze affiliés au total ;
- Les personnes physiques ou morales exemptées en vertu des articles 2 et 3 de la directive 2014/65/UE ;
- **Les intermédiaires d'assurance, intermédiaires de réassurance et intermédiaires d'assurance à titre accessoire qui sont des microentreprises ou des petites ou moyennes entreprises ;**
- Les offices des chèques postaux visés à l'article 2, paragraphe 5, point 3), de la directive 2013/36/UE.

Document créé le 17 juin 2024, modifié le 10 septembre 2024

La Commission européenne dans sa recommandation du 6 mai 2003, entrée en vigueur le 1er janvier 2005 et reprise en droit français dans l'article 3 du décret n° 2008-1354 du 18 décembre 2008 relatif aux « critères permettant de déterminer la catégorie d'appartenance d'une entreprise pour les besoins de l'analyse statistique et économique » notamment, donne la définition des micro, petites et moyennes entreprises :

- **Microentreprise : elle emploie moins de 10 personnes et son chiffre d'affaires annuel (montant d'argent perçu à une période donnée) ou son bilan (état des actifs et des passifs de la société) n'excède pas 2 millions d'euros ;**
- **petite entreprise : elle emploie moins de 50 personnes et son chiffre d'affaires ou son bilan n'excède pas 10 millions d'euros ;**
- **moyenne entreprise : elle emploie moins de 250 personnes et son chiffre d'affaires n'excède pas 50 millions d'euros ou son bilan n'excède pas 43 millions d'euros.**

Par conséquent, toutes les entreprises rentrant dans cette définition ne sont pas concernées par le règlement DORA.

Pour se mettre en conformité avant janvier 2025 les organismes cités précédemment devront mettre en place 7 mesures :

- Gouvernance du risque informatique ;
- Formation à la résilience opérationnelle numérique (article 12 règlement DORA) ;
- Analyse du système informatique ;
- Gestion des risques informatiques ;
- Conduite de tests de résilience ;
- Encadrement des risques liés aux prestataires SI (article 28 du règlement DORA) ;
- Mécanismes d'échange d'information sur les risques (article 13 règlement DORA).

Le non-respect des obligations issues du règlement DORA permet au pays de l'UE d'appliquer des sanctions pénales spécifiques aux règles de résilience opérationnelle numérique, avec instauration d'une responsabilité elle aussi spécifique, pour les dirigeants (art. 52 du règlement DORA).

Ces sanctions pourront être appliquées par les « autorités compétentes » de chaque pays européens (en France : AMF, ACPR Banque de France, …), lesquelles disposeront de véritables pouvoirs d'enquête (inspection dans les locaux informatiques, injonction visant à faire cesser l'infraction à la réglementation DORA, astreintes journalières, ...), (art 46 du règlement DORA).

Dans la continuité de la Directive et du Règlement DORA, trois (3) règlements délégués ont vu le jour afin de les compléter. Il s'agit entre autres :

Du **Règlement délégué (UE) 2024/1772** en ce qui concerne les normes techniques réglementaires spécifiant les critères de classification des incidents liés aux TIC et des cybermenaces, établissant des seuils de matérialité et spécifiant les détails des rapports sur les incidents majeurs.
Il fixe les critères de classifications autant sur les clients, les contreparties financières que les transactions.
Premièrement, le règlement détermine comment identifier :

- Les atteintes à la réputation
- La durée et les interruptions de service
- La répartition géographique
- Les pertes de données
- La criticité des services touchés
- Les conséquences économiques

Il évoque ensuite la problématique des incidents majeurs et des seuils d'importance significatifs. Avec cela on va avoir la définition de l'incident majeur et ses conditions de détermination. Aussi les seuils d'importance significatifs pour la détermination d'un incident majeur.

Enfin il termine sur le point des cybermenaces importantes. Puis il détermine les seuils d'importance significative élevés pour la détermination des cybermenaces importantes, en listant les conditions.

Du **Règlement délégué (UE) 2024/1773** en ce qui concerne les normes techniques réglementaires spécifiant le contenu détaillé de la politique relative aux arrangements contractuels pour l'utilisation de services TIC à l'appui de fonctions essentielles, ou importantes fournis par des prestataires de services TIC tiers.
Ce dernier vient imposer à toute entité assujettie la mise en place d'un profil de risque. Il précise que la politique relative à l'utilisation de services TIC soutenant des fonctions critiques ou importantes qui sont fournis par des prestataires tiers de services TIC, tient compte de la taille et du profil de risque global de l'entité financière, ainsi que de la nature, de l'échelle et des facteurs d'augmentation ou de diminution de la complexité de ses services, activités et opérations.

Il précise ensuite l'application au niveau des groupes. En effet, l'entreprise mère devra se charger de fournir les états financiers consolidés ou sous-consolidés pour le groupe. De plus cette dernière veillera à ce que la politique soit mise en œuvre de manière cohérente dans toutes les entités financières faisant partie du groupe, et à ce qu'elle soit adaptée à l'application effective du présent règlement à tous les niveaux pertinents du groupe.

De plus, le règlement nous livre le détail du dispositif de gouvernance, avec à la tête l'organe de contrôle de l'entité chargé de mettre en place la politique et de l'actualiser annuellement

Document créé le 17 juin 2024, modifié le 10 septembre 2024

En outre, nous avons les principales phases du cycle de vie pour l'adoption et l'utilisation d'accords contractuel. Ainsi la politique précise les exigences, notamment les règles, les responsabilités et les processus à respecter à chacune des phases principales du cycle de vie d'un accord contractuel.

La politique va exiger que les besoins métiers de l'entité financière soient définis avant la conclusion de tout accord contractuel. Cela au niveau de l'entité financière. Et elle listera les risques à prendre en compte.

Par ailleurs ladite politique définira également un processus approprié et proportionné de sélection et d'évaluation des prestataires tiers potentiels de services TIC, en tenant compte de leur appartenance ou non au groupe, et exige qu'avant de conclure un accord contractuel. Pour ce faire l'entité financière devra effectuer des diligences raisonnables aux fins de vérifications auprès du prestataire tiers de services TIC. Ces dernières sont listées de manières exhaustives dans le règlement.

Pour finir, au sujet des accords contractuels, le règlement établit le cadre de sa mise en place avec les clauses à y insérer, le suivi à effectuer, et les conditions de résiliation de ces derniers.

Du **Règlement délégué (UE) 2024/1774** en ce qui concerne les normes techniques réglementaires spécifiant les outils, les méthodes, les processus et les politiques de gestion du risque cybernétique et le cadre simplifié pour la gestion du risque cybernétique. Ce dernier met en place les éléments généraux des politiques, procédures, protocoles et outils de sécurité des TIC. Ensuite il détaille la Gestion du risque lié aux TIC, la mise en place de Politique de gestion des actifs de TIC. Et au sujet de la Sécurité des opérations de TIC : on va avoir la mise en place Politiques et procédures pour les opérations de TIC.