Le numérique - Le Règlement sur la résilience opérationnelle numérique du secteur financier (Règlement DORA)

Pourquoi est-ce important pour les intermédiaires ?

Le Règlement sur la résilience opérationnelle numérique du secteur financier (Règlement DORA) fait partie de la stratégie en matière de finance numérique de la Commission qui a été publiée en septembre 2020. L'objectif premier du Règlement DORA est de renforcer la sécurité informatique des entités financières. Il vise à établir un cadre global de résilience opérationnelle numérique dans les secteurs européens de la banque, de l'assurance et de l'investisseur, en exigeant des entités financières relevant de son champ d'application qu'elles se conforment à des exigences en matière de sécurité numérique et de notification afin d'atténuer leurs risques liés aux technologies de l'information et de la communication (TIC).

Le Règlement DORA est entré en vigueur, ainsi que ses mesures de niveau 2, le 17 janvier 2025. **Les intermédiaires d'assurance qui sont des micro-entreprises et des PME sont exclus du champ d'application du Règlement DORA et de ses mesures de niveau 2.** Les "entreprises d'investissement opt-out" qui relèvent de la MiFID II sont également exemptées du Règlement DORA. Les grands intermédiaires d'assurance (plus de 250 personnes, un chiffre d'affaires annuel supérieur à 50 millions d'euros et/ou un bilan annuel supérieur à 43 millions d'euros) entrent, par contre, dans le champ d'application du Règlement DORA. Dans certains cas, les intermédiaires, s'ils sont considérés par les assureurs comme des prestataires tiers de TIC ou dans le cadre de délégations de pouvoirs au titre de Solvabilité II, peuvent être tenus de se conformer à certaines exigences du Règlement DORA.

Le Règlement DORA a attribué de nouvelles tâches et de nouveaux rôles aux autorités européennes de surveillance (EIOPA, ESMA et EBA – les AES), ainsi que l'élaboration de normes techniques de réglementation (NTR) et de normes techniques d'exécution (NTE) concernant certaines dispositions du Règlement DORA. Les NTR et les NTE des AES visent à clarifier les dispositions d'un texte législatif européen et à assurer une harmonisation cohérente des domaines définis.

Etat des lieux

Déclaration des AES sur l'application du Règlement DORA

Le 4 décembre 2024, les AES ont publié une déclaration sur l'application du Règlement DORA. Cette déclaration précise que ce Règlement et ses normes techniques ainsi que les lignes directrices s'appliqueront à compter du 17 janvier 2025 et invite les entités financières et les prestataires tiers à accélérer leurs préparatifs afin d'être prêts à cette date. Elle souligne également qu'il est important que les entités financières adoptent une approche solide et structurée pour se conformer à leurs obligations en temps voulu, étant donné que le Règlement DORA ne prévoit pas de période transitoire.

Parmi les autres messages clés de la déclaration, on peut retenir les suivants :

- les entités financières sont tenues d'identifier et de combler en temps utile les lacunes entre leurs dispositifs internes et les exigences du Règlement DORA;
- les entités financières doivent se préparer aux nouvelles obligations d'informations et, en particulier, les entités financières doivent mettre à la disposition des autorités compétentes des Etats membres, dès le début de l'année 2025, leurs registres des accords contractuels conclus avec des prestataires tiers de TIC, car ces derniers devront les communiquer aux AES avant le 30 avril 2025.

Mesures de niveau 2 du Règlement DORA

Le Règlement DORA mandate les AES d'élaborer une série de mesures de niveau 2 et 3 afin de préciser les exigences de niveau 1. Au cours de l'année écoulée, les mesures suivantes ont notamment été adoptées/publiées/traduites :

- **Règlement délégué (UE) 2024/1772** de la Commission complétant le Règlement DORA par des NTR précisant les critères de classification des incidents liés aux TIC et des cybermenaces, fixant des seuils d'importance significative et précisant les détails des rapports d'incidents majeurs
- **Règlement délégué (UE) 2024/1773** de la Commission complétant le Règlement DORA par des NTR précisant le contenu détaillé de la politique relative aux accords contractuels sur l'utilisation de services TIC soutenant des fonctions critiques ou importantes fournis par des prestataires tiers de services TIC
- **Règlement délégué (UE) 2024/1774** de la Commission complétant le Règlement DORA par des NTR précisant les outils, méthodes, processus et politiques de gestion du risque lié aux TIC et le cadre simplifié de gestion du risque lié aux TIC
- **Règlement délégué (UE) 2025/301** de la Commission complétant le Règlement DORA par des NTR précisant le contenu et les délais pour la notification initiale des

incidents majeurs liés aux TIC, et pour les rapports intermédiaire et final y afférents, et le contenu de la notification volontaire en ce qui concerne les cybermenaces importantes

- **Règlement d'exécution (UE) 2025/302** de la Commission définissant des NTE pour l'application du Règlement DORA en ce qui concerne les formulaires, modèles et procédures types permettant aux entités financières de notifier un incident majeur lié aux TIC et de notifier une cybermenace importante
- **Règlement délégué (UE) 2025/295** de la Commission complétant le Règlement DORA par des NTR relatives à l'harmonisation des conditions permettant l'exercice des activités de supervision
- Le 29 novembre 2024, la Commission a adopté le **Règlement d'exécution (UE) 2024/2956** définissant les NTE en ce qui concerne les modèles types pour le registre d'informations. Il a été publié au Journal officiel de l'Union européenne le 2 décembre et est entré en vigueur le 22 décembre 2024.
- Le 6 novembre 2024, les **AES ont publié des lignes directrices conjointes** sur la **coopération en matière de surveillance et l'échange d'informations entre les AES et les autorités compétentes** au titre du Règlement DORA.
- Le 18 mars 2025, **ESMA a publié les traductions officielles des orientations des AES sur l'estimation des coûts et pertes annuels agrégés occasionnés par des incidents majeurs liés aux TIC** au titre du Règlement DORA. Ces orientations s'appliqueront à compter du 19 mai 2025. Les autorités nationales compétentes (ANC) doivent notifier à l'AES concernée si elles se conforment ou ont l'intention de se conformer aux orientations communes, ou, dans le cas contraire, les raisons de leur non-conformité, au plus tard le 19 mai 2025. En l'absence de notification dans ce délai, les autorités compétentes des Etats membres seront considérées par l'AES concernée comme non conformes.
- Le 24 mars 2025, la **Commission** a adopté le **projet de Règlement délégué C(2025)1682** complétant le Règlement DORA par des NTR précisant les éléments qu'une entité financière doit déterminer et évaluer lorsqu'elle sous-traite des services TIC qui soutiennent des fonctions critiques ou importantes. Si le Parlement européen ou le Conseil de l'UE ne s'y opposent pas, l'acte délégué sera publié au Journal officiel de l'UE et entrera en vigueur le vingtième jour suivant celui de sa publication. La période d'examen dure généralement deux mois à compter de l'adoption de l'acte.

Questions-réponses d'EIOPA sur le Règlement DORA

Conformément à l'article 16 ter du Règlement EIOPA, EIOPA - ainsi qu'ESMA et EBA (et parfois la Commission européenne) - répond régulièrement aux questions relatives à l'interprétation juridique des dispositions du Règlement DORA. Les questions-réponses d'EIOPA ont pour objectif d'assurer une application cohérente et efficace de la réglementation européenne et de favoriser la convergence en matière de surveillance dans l'EEE dans le cadre du champ d'action d'EIOPA.

En janvier 2025, les questions-réponses d'EIOPA sur le Règlement DORA ont été mises à jour et comprennent trois réponses concernant des questions importantes pour notre secteur :

1. *Quels types de services doivent être considérés comme des services TIC ? (en particulier dans le cas où des entités financières fournissent des services TIC à d'autres entités financières en relation avec leurs services financiers)* Réponse d'EIOPA
2. *Les intermédiaires d'assurance exerçant à titre accessoires relevant de l'Article 1(3) de la DDA relèvent-ils du champ d'application de l'article 2(1)(0), du Règlement DORA ?* Réponse d'EIOPA
3. *Nous recevons de nombreuses questions de la part d'intermédiaires d'assurance sur la façon de déterminer pour les structures de groupe si elles entrent dans le champ d'application du Règlement DORA. Le Règlement DORA ne précise pas comment calculer si on remplit le critère des 250 FTE. Nous avons trouvé des orientations de la Commission européenne dans le document 2003/361/CE sur la manière de calculer si une entreprise est petite, moyenne ou grande et comment prendre en considération les entités liées et les entités mères, mais nous ne sommes pas sûrs qu'il s'agisse des orientations à suivre. Pouvez-vous clarifier ces points ?* Réponse d'EIOPA

Ces questions-réponses ont été examinées lors d'un webinaire du BIPAR organisé le 18 février 2025 avec le cabinet d'avocats DLA Piper. La réponse de la Commission publiée par EIOPA concernant la manière de déterminer si les structures de groupe (intermédiaires) relèvent du champ d'application du Règlement DORA a été examinée en détail. Dans sa réponse, la Commission explique que sa recommandation 2003/361/CE est applicable compte tenu des seuils définis dans le Règlement DORA (micro, petites et moyennes entreprises) et que, **lorsque l'intermédiaire fait partie d'un groupe,** les chiffres à utiliser pour calculer le nombre d'employés, le chiffre d'affaires annuel et le total du bilan annuel doivent être calculés au niveau du groupe, en appliquant la notion d'entreprises liées telle qu'expliquée dans la recommandation 2003/361/CE.

Le BIPAR estime que, dans la mesure où il n'est pas fait référence à la recommandation 2003/361/CE de la Commission dans le Règlement DORA, les définitions des intermédiaires qui sont des micro, petites et moyennes entreprises figurant dans le Règlement DORA, qui exigent la prise en considération des comptes des entités individuelles, sont autonomes. Le BIPAR a informé la Commission et EIOPA de ses vues. **Début mai, EIOPA a supprimé la réponse concernée et a changé le statut de cette question-réponse en "en cours de révision".**

Questions-réponses des AES sur le Règlement DORA

Les questions-réponses générales des AES sur le Règlement DORA sont régulièrement mises à jour et comprennent, par exemple, à la fin 2024, trois réponses concernant les services critiques touchés, l'exemption pour les prestataires de services TIC intra-groupe non européens et la duplication des notifications d'incidents liés aux TIC.

Dans le cadre de leur exercice de simulation (voir ci-dessous pour plus d'informations), les AES ont également mis en place une foire aux questions qui répond aux questions fréquemment posées concernant la nature pratique de l'exercice de notification, notamment le remplissage des modèles, la préparation des fichiers de notification, leur soumission et l'utilisation des outils fournis par les AES pour l'exercice de simulation. Les questions-réponses devraient être mises à jour prochainement, notamment en ce qui concerne les services TIC et les entités financières. Les réponses aux questions sont fournies dans la mesure du possible par le personnel des AES et ne constituent donc pas une interprétation juridique ou une orientation convenue avec les autorités compétentes, ni la position officielle des AES.

Exercice volontaire des AES sur la collecte des registres d'information

En vertu du Règlement DORA, les entités financières relevant de son champ d'application doivent tenir un registre complet de leurs accords contractuels avec des prestataires tiers de services TIC (registres d'informations) disponible aux niveaux de l'entité, du sous-groupe et du groupe consolidé. Afin d'aider les entités financières à élaborer ce registre conformément aux exigences énoncées dans les NTE et à être prêtes à le notifier à partir de 2025, les AES et les autorités compétentes ont procédé à un exercice de simulation en 2024. Fin décembre 2024, les AES ont publié un **rapport de synthèse** présentant les principales conclusions de cet exercice. Selon les AES, la qualité des données observées dans les registres soumis par 1.039 entités financières dans l'UE, dont 17 intermédiaires d'assurance ou de réassurance et intermédiaires à titre accessoires, était conforme aux attentes. Parmi les registres analysés, 6,5 % ont satisfait à tous les contrôles de qualité des données, tandis que 50 % des registres restants ont échoué à moins de 5 des 116 contrôles de qualité des données. Parmi les entités financières ayant soumis le plus grand nombre de données, les établissements de crédit ont enregistré la plus faible proportion d'erreurs dans les données par rapport aux points de données soumis (1,9 %), suivis par les entreprises d'investissement (2,4 %) et les entreprises d'assurance et de réassurance (3,3 %). La proportion d'erreurs dans les données des intermédiaires par rapport aux points de données soumis s'est élevée à 2,8 %.

Les AES expliquent que les principales conclusions présentées dans le rapport de synthèse et tous les documents complémentaires fournis devraient être examinés attentivement par toutes les parties prenantes du secteur, y compris les entités financières qui n'ont pas participé à l'exercice de simulation, car ils les aideront à mieux se préparer à la notification des registres en 2025. Tous les documents pertinents, y compris la présentation et l'enregistrement vidéo, sont publiés ici.

Procédures d'infraction contre des Etats membres pour non-transposition du Règlement DORA

Le 27 mars 2025, la Commission européenne a décidé d'ouvrir des procédures d'infraction en envoyant une lettre de mise en demeure à 13 Etats membres (Belgique, Bulgarie, Danemark, Grèce, Espagne, France, Lettonie, Lituanie, Malte, Pologne, Portugal, Roumanie et Slovénie) pour défaut de transposition complète du Règlement DORA. Les Etats membres avaient jusqu'au 17 janvier 2025 pour le transposer en droit national. Ces 13 Etats membres auront deux mois pour répondre et achever leur transposition et notifier leurs mesures à la Commission. En l'absence de réponse satisfaisante, celle-ci pourra décider d'émettre un avis motivé.

Lignes directrices d'EIOPA révoquées et avis modifié pour éviter les doubles emplois et les chevauchements avec le Règlement DORA

Le 19 décembre 2024, EIOPA a annoncé qu'elle retirerait deux lignes directrices précédemment publiées et modifierait un avis - tous liés, au moins en partie, à l'utilisation des TIC par les entreprises. En prenant cette mesure, EIOPA explique qu'elle vise à éliminer les chevauchements et à favoriser un cadre réglementaire unifié pour la résilience opérationnelle numérique dans les secteurs européens de l'assurance et des fonds de pension professionnels. Elle a décidé de **retirer les "Lignes directrices sur la sécurité et la gouvernance des**

technologies de l'information et de la communication" publiées dans le cadre de Solvabilité II et les **"Lignes directrices sur l'externalisation vers des fournisseurs de services cloud"** publiées dans le cadre de Solvabilité II et de modifier l'**"Avis sur la supervision de la gestion des risques opérationnels auxquels sont confrontées les IRP"** publié dans le cadre de l'IRP II, en supprimant la section sur les cyber-risques ainsi que toutes les références et les annexes qui s'y rapportent.

Ces modifications sont entrées en vigueur le 17 janvier 2025.

Position du BIPAR / messages clés

Les intermédiaires d'assurance ont été inclus dans le champ d'application de la proposition de Règlement DORA de la Commission, au même titre que des entités financières beaucoup plus importantes telles que des assureurs ou des établissements de crédit.

Si le BIPAR a salué l'objectif du Règlement DORA d'accroître la résilience opérationnelle numérique du secteur financier, il a informé les législateurs de l'UE que le secteur financier n'est pas uniforme en termes d'échelle et de structure. Les incidents subis par les différentes entités de services financiers, ainsi que leurs conséquences (pour la stabilité financière, les consommateurs, etc.), diffèrent d'un secteur de services financiers à l'autre. Les exigences du Règlement DORA ne seraient tout simplement pas viables d'un point de vue opérationnel et financier pour les (petits) intermédiaires financiers ou d'assurance. L'architecture réglementaire du Règlement DORA n'est pas adaptée au secteur de la distribution d'assurances, et le BIPAR a souligné que l'application proportionnée de ses exigences nombreuses et détaillées serait difficile à assurer dans la pratique (compliquée davantage par les mesures de niveaux 2 et 3).

Pour le BIPAR et ses membres, les intermédiaires d'assurance et financiers (et, en particulier, les micro-entreprises et les PME) devaient donc être totalement exemptés du Règlement DORA. Ce message a été relayé avec succès auprès des députés européens, du Conseil et de la Commission.

En collaboration avec Grant Thornton Ireland, le BIPAR a organisé en décembre 2024 un webinaire sur le Règlement DORA et son impact sur les intermédiaires.

Prochaines étapes

Le BIPAR, en collaboration avec ses associations membres, continuera à surveiller l'application du Règlement DORA dans les Etats membres et son impact sur les intermédiaires.

Liens

- Règlement sur la résilience opérationnelle numérique du secteur financier (DORA)
- Déclaration des AES sur l'application du Règlement DORA
- Règlement délégué (UE) 2024/1772
- Règlement délégué (UE) 2024/1773
- Règlement délégue (UE) 2024/1774
- Règlement délégue (UE) 2025/301
- Règlement d'exécution (UE) 2025/302
- Règlement délégué (UE) 2025/295
- Règlement d'exécution (UE) 2024/2956
- Lignes directrices conjointes des AES (sur la coopération en matière de surveillance et l'échange d'informations entre les AES et les autorités compétentes)
- Traductions officielles des orientations des AES sur l'estimation des coûts et pertes annuels agrégés occasionnés par des incidents majeurs liés aux TIC
- Projet de Règlement délégué C(2025)1682
- Lignes directrices d'EIOPA révoquées et avis modifié :
- Lignes directrices sur la sécurité et la gouvernance des technologies de l'information et de la communication
- Lignes directrices sur l'externalisation vers des fournisseurs de services cloud
- Avis sur la supervision de la gestion des risques opérationnels auxquels sont confrontées les IRP