Finance numérique: loi sur la résilience opérationnelle numérique (DORA)

2020/0266(COD) - 27/12/2022 - Acte final

OBJECTIF : renforcer la sécurité informatique des entités financières telles que les banques, les compagnies d'assurance et les entreprises d'investissement en vue de permettre au secteur financier européen de maintenir des opérations résilientes en cas de perturbation opérationnelle grave.

ACTE LÉGISLATIF : Règlement (UE) 2022/2554 du Parlement européen et du Conseil sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n° 1060/2009, (UE) no 648 /2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011.

CONTENU : le règlement sur la résilience opérationnelle numérique (**règlement DORA**) fixe des **exigences uniformes** pour la sécurité des réseaux et des systèmes d'information des entreprises et des organisations actives dans le secteur financier ainsi que des tiers critiques qui leur fournissent des services liés aux technologies de l'information et de la communication (TIC), tels que des plateformes d'informatique en nuage ou des services d'analyse de données.

DORA crée un **cadre réglementaire sur la résilience opérationnelle numérique** dans lequel toutes les entreprises doivent s’assurer qu’elles peuvent résister à tous les types de perturbations et de menaces liées aux TIC, y réagir et s’en remettre. Les nouvelles règles constitueront un cadre solide qui renforcera la sécurité informatique du secteur financier.

Exigences uniformes

DORA fixe des exigences uniformes pour la sécurité des réseaux et des systèmes d’information des entreprises et des organisations opérant dans le secteur financier, comme suit:

- les exigences applicables aux entités financières en ce qui concerne: i) la **gestion des risques** liés aux technologies de l'information et de la communication (TIC); ii) la **notification**, aux autorités compétentes, des incidents majeurs liés aux TIC et la notification, à titre volontaire, des cybermenaces importantes aux autorités compétentes; iii) la notification aux autorités compétentes, par les entités financières des incidents opérationnels ou de sécurité majeurs liés au paiement; iv) les **tests** de résilience opérationnelle numérique; v) le partage d'informations et de renseignements en rapport avec les cybermenaces et les cybervulnérabilités; vi) les mesures destinées à garantir la **gestion saine du risque** lié aux prestataires tiers de services TIC;

- les exigences relatives aux **accords contractuels conclus entre des prestataires tiers de services TIC et des entités financières**;

- les règles relatives à l'établissement du **cadre de supervision** applicable aux prestataires tiers critiques de services TIC lorsqu'ils fournissent des services à des entités financières, ainsi que celles liées à l’ exercice des tâches dans ce cadre.

- les règles relatives à la **coopération** entre les autorités compétentes, et les règles relatives à la surveillance et à l’exécution par les autorités compétentes en ce qui concerne toutes les questions couvertes par le règlement.

Champ d’application

La nouvelle règlementation **s'appliquera à presque toutes les entités financières**. Elle ne s'appliquera pas aux intermédiaires d'assurance qui sont des microentreprises ou des petites ou moyennes entreprises. Les cabinets d'audit ne seront pas soumis au règlement DORA, mais feront partie d'un futur réexamen du règlement, dans le cadre duquel une éventuelle révision des règles pourrait être envisagée.

Principe de proportionnalité

Les efforts demandés aux entités financières seront proportionnels aux risques potentiels. Le règlement précise que les entités financières devront mettre en œuvre les règles relatives à la gestion des risques conformément au principe de proportionnalité, en tenant compte de leur taille et de leur profil de risque global ainsi que de la nature, de l'ampleur et de la complexité de leurs services, activités et opérations.

Gouvernance et organisation

Les entités financières devront :

- disposer d'un **cadre de gouvernance** et de contrôle interne garantissant une gestion efficace et prudente du risque lié aux TIC en vue d'atteindre un niveau élevé de résilience opérationnelle numérique;

- disposer d'un **cadre de gestion du risque** lié aux TIC solide, complet et bien documenté, qui leur permet de parer au risque lié aux TIC de manière rapide, efficiente et exhaustive et de garantir un niveau élevé de résilience opérationnelle numérique;

- mettre en place des mécanismes permettant de **détecter rapidement les activités anormales**. Tous les mécanismes de détection seront régulièrement testés.

Cadre de supervision des prestataires tiers critiques de services TIC

Les prestataires critiques établis dans un pays tiers qui fournissent des services informatiques aux entités financières dans l'UE seront tenus d'établir **une filiale dans l'UE**, afin que la supervision puisse être correctement mise en œuvre.

Afin que les prestataires tiers critiques de services TIC fassent l'objet d'une supervision appropriée et efficace à l'échelle de l'Union, le règlement prévoit que l'une des trois autorités européennes de surveillance (AES) pourra être désignée comme **superviseur principal**.

Les superviseurs principaux se verront confier les pouvoirs nécessaires pour mener des enquêtes, réaliser des inspections sur place et hors site des locaux et sites des prestataires tiers critiques de services TIC et obtenir des informations complètes et actualisées.

Afin de permettre la coordination des stratégies générales de supervision ainsi que des approches opérationnelles et des méthodes de travail cohérentes, les superviseurs principaux désignés devront mettre en place un **réseau de supervision commun** pour assurer la coordination de leurs activités au cours des phases préparatoires et durant l'exécution des activités de supervision de leurs prestataires tiers critiques de services TIC respectifs qui font l'objet d'une supervision.

Le superviseur principal sera également en mesure d'exercer ses pouvoirs de supervision dans les pays tiers.

Tests de résilience opérationnelle numérique

Afin d'évaluer l'état de préparation en vue du traitement d'incidents liés aux TIC, de recenser les faiblesses, les défaillances et les lacunes en matière de résilience opérationnelle numérique et de mettre rapidement en œuvre des mesures correctives, les entités financières, autres que les microentreprises, devront établir, maintenir et réexaminer un programme solide et complet de tests de résilience opérationnelle numérique, qui fait partie intégrante du cadre de gestion du risque lié aux TIC.

En vertu du règlement, des **tests de pénétration fondés sur la menace** seront effectués en mode fonctionnel et il sera possible d'inclure les autorités de plusieurs États membres dans les procédures de test. Le recours à des auditeurs internes ne sera possible que dans un certain nombre de circonstances strictement limitées, sous réserve de conditions de sauvegarde.

ENTRÉE EN VIGUEUR : 16.1.2023. Le règlement s’applique à partir du 17.1.2025.