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

2020/0266(COD) - 10/11/2022 - Texte adopté du Parlement, 1ère lecture/lecture unique

Le Parlement européen a adopté par 556 voix pour, 18 contre et 38 abstentions, une résolution législative sur la proposition de règlement du Parlement européen et du Conseil sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) nº 1060/2009, (UE) nº 648/2012, (UE) nº 600/2014 et (UE) nº 909/2014.

Le règlement sur la résilience opérationnelle numérique (DORA) vise à **atteindre un niveau élevé de résilience opérationnelle numérique** pour toutes les entités financières réglementées, telles que les banques, les compagnies d'assurance et les entreprises d'investissement.

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.

La position du Parlement européen arrêtée en première lecture dans le cadre de la procédure législative ordinaire modifie la proposition comme suit:

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.

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

Le texte amendé 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. L'organe de direction de l'entité financière définira, approuvera, supervisera et sera responsable de la mise en œuvre de toutes les dispositions relatives au cadre de gestion du risque lié aux TIC.

Prestataires tiers critiques de services TIC établi dans un pays tiers

Les **autorités européennes de surveillance** (AES), agissant par l'intermédiaire du comité mixte et sur recommandation du forum de supervision établi conformément au règlement désigneront les prestataires tiers de services TIC qui sont critiques pour les entités financières, à l'issue d'une évaluation. Afin que la supervision puisse être correctement mise en œuvre, les entités financières ne pourront faire appel aux services d'un prestataire tiers de services TIC établi dans un pays tiers et ayant été désigné comme critique que si ce dernier a établi **une filiale dans l'Union** dans un délai de 12 mois à compter de la désignation.

Cadre de supervision

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. Ces pouvoirs permettront au superviseur principal (à savoir l'AES désignée conformément au règlement) de se faire une idée précise du type, de la dimension et des incidences du risque que les prestataires tiers de services TIC représentent pour les entités financières et, en définitive, pour le système financier de l'Union.

Afin de garantir une approche cohérente en matière d'activités de supervision et en vue 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.** L'exercice de ces pouvoirs dans les pays tiers lui permettra d'examiner les installations à partir desquelles les services TIC ou d'appui technique sont effectivement fournis ou gérés par le prestataire tiers critique de services TIC.

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 amendé, 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.

Protection des données

Les AES et les autorités compétentes ne seront autorisées à traiter des données à caractère personnel que lorsque cela est nécessaire à l'accomplissement de leurs obligations et missions respectives en vertu du présent règlement, en particulier en matière d'enquête, d'inspection, de demande d'informations, de communication, de publication, d'évaluation, de vérification, d'évaluation et d'élaboration de plans de supervision.