Finance numérique: directive modifiant sur les exigences en matière de résilience opérationnelle numérique

2020/0268(COD) - 10/11/2022 - Texte adopté du Parlement, 1ère lecture/lecture unique

Le Parlement européen a adopté par 553 voix pour, 19 contre et 40 abstentions, une résolution législative sur la proposition de directive du Parlement européen et du Conseil modifiant les directives 2006/43/CE, 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/65/UE, (UE) 2015/2366 et (UE) 2016/2341.

La présente directive modificative fait partie du train de mesures sur la finance numérique. Elle introduit des **modifications ciblées aux directives existantes de l'Union** portant sur les services financiers afin de les aligner sur les exigences établies par le règlement sur la résilience opérationnelle numérique du secteur financier (règlement DORA) en matière de gestion des risques et de notification s'agissant de l' informatique et des réseaux et systèmes d'information, et de clarifier certaines dispositions pour garantir une pleine prise en compte des risques informatiques.

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

Objectif des modifications

La directive prévoit une série de modifications qui sont nécessaires pour apporter la clarté et la cohérence juridiques en ce qui concerne l'application, par les entités financières agréées et soumises à une surveillance conformément aux directives existantes, de **diverses exigences en matière de résilience opérationnelle numérique** qui sont nécessaires à l'exercice de leurs activités et à la prestation de services, assurant ainsi le bon fonctionnement du marché intérieur.

Le texte amendé insiste sur la nécessité de veiller à ce que ces exigences soient en adéquation avec les évolutions du marché, tout en encourageant la **proportionnalité** au regard notamment de la taille des entités financières et des régimes spécifiques auxquels elles sont soumises, en vue de réduire les coûts de mise en conformité.

Modification de la directive 2013/36/UE concernant l'accès à l'activité des établissements de crédit et la surveillance prudentielle des établissements de crédit et des entreprises d'investissement (CRD)

Les dispositions pertinentes de la CRD ont été clarifiées de manière à ce que le risque informatique soit explicitement pris en compte.

Les modifications introduites stipulent que les établissements doivent disposer d'un **dispositif solide de gouvernance d'entreprise**, comprenant notamment i) une structure organisationnelle claire avec un partage des responsabilités bien défini, transparent et cohérent, ii) des processus efficaces de détection, de gestion, de suivi et de déclaration des risques auxquels ils sont ou pourraient être exposés, iii) des mécanismes adéquats de contrôle interne, y compris des procédures administratives et comptables saines, des systèmes de réseau et des systèmes d'information mis en place et gérés conformément au règlement DORA et des politiques et pratiques de rémunération permettant une gestion saine et efficace des risques.

En outre, les établissements devront disposer **de politiques et de plans d'urgence** et de poursuite de l' activité adéquats, y compris des politiques et des plans en matière de continuité des activités de

technologies de l'information et des communications (TIC) et des **plans de réponse et de rétablissement** des TIC. Ces plans devront être établis, gérés et testés conformément au règlement DORA afin que les établissements puissent poursuivre leurs activités en cas de grave perturbation de celles-ci et limiter les pertes subies à la suite d'une telle perturbation.

Modification de la directive 2014/59/UE établissant un cadre pour le redressement et la résolution des établissements de crédit et des entreprises d'investissement (BRRD)

Selon le texte amendé, le plan de résolution devra comprendre :

- une démonstration de la façon dont les fonctions critiques et les activités fondamentales pourraient être juridiquement et économiquement séparées des autres fonctions, dans la mesure nécessaire pour assurer leur continuité et la résilience opérationnelle numérique en cas de défaillance de l'établissement;

- une description des principaux systèmes et opérations permettant de maintenir en permanence le fonctionnement des processus opérationnels de l'établissement, y compris des réseaux et des systèmes d'information visés dans le règlement DORA.

Modification de directive (UE) 2015/2366 (services de paiement)

La directive énonce des règles spécifiques relatives à des éléments de maîtrise et d'atténuation des risques en matière de sécurité des TIC aux fins d'obtenir un **agrément** pour la prestation de services de paiement. Ces règles d'agrément doivent être modifiées afin d'être alignées sur le règlement DORA.

En outre, afin de réduire la charge administrative et d'éviter la complexité et la répétition des obligations de notification, les règles relatives à la notification des incidents contenues dans ladite directive cesseront de s'appliquer aux prestataires de services de paiement qui sont régis par ladite directive et qui relèvent également du règlement DORA, leur permettant ainsi de bénéficier d'un mécanisme de notification des incidents unique et entièrement harmonisé, applicable à tous les incidents opérationnels ou de sécurité liés au paiement, que ces incidents soient liés ou non aux TIC.

En vertu du texte amendé, l'obtention de l'agrément en tant qu'établissement de paiement sera subordonnée à la soumission, aux autorités compétentes de l'État membre d'origine, d'une demande accompagnée des informations suivantes :

- une description du dispositif de gouvernance d'entreprise et des mécanismes de contrôle interne, notamment des procédures administratives, de gestion des risques et comptables du demandeur, ainsi que des dispositions relatives à l'utilisation des services TIC conformément au règlement DORA qui démontre que ce dispositif de gouvernance d'entreprise et ces mécanismes de contrôle interne sont proportionnés, adaptés, sains et adéquats;

- une description de la procédure en place pour assurer la surveillance, le traitement et le suivi des incidents de sécurité et des réclamations de clients liées à la sécurité, y compris un mécanisme de signalement des incidents qui tient compte des obligations de notification incombant à l'établissement de paiement fixées au règlement DORA;

- une description des dispositions en matière de continuité des activités, y compris une désignation claire des opérations critiques, une politique et des plans en matière de continuité des activités de TIC et des plans de réponse et de rétablissement des TIC efficaces, ainsi qu'une procédure prévoyant de tester et de réexaminer régulièrement le caractère adéquat et l'efficacité de ces plans.

Transposition

Les États membres doivent transposer la directive au plus tard 24 mois après la date d'entrée en vigueur de la présente directive modificative.