ARTICLE

FINANCE & TECH : ADOPTION DU RÈGLEMENT « DORA » SUR LA RÉSILIENCE OPÉRATIONNELLE INFORMATIQUE DU SECTEUR FINANCIER AJUSTEMENTS NÉCESSAIRES DES PROCESS ET DES CONTRATS

IT et données personnelles | 21/11/22 | Mahasti Razavi

Le 10 novembre 2022, le Parlement européen a adopté le règlement sur la résilience opérationnelle informatique du sect eur financier (« DORA » ou « Digital Operational Resilience Act »).

Ce règlement a pour objet d'harmoniser et renforcer les règles en matière de gestion des risques liés aux nouvelles technologies pesant sur les entités financières de l'Union Européenne.

Il entrera en vigueur le 17 janvier 2025, laissant un délai très court aux entreprises concernées pour ajuster leurs process internes et les relations contractuelles, y compris existantes.

DORA a un impact significatif pour l'ensemble des entités financières et leurs partenaires technologiques, puisque le règlement DORA impose de :

- *renforcer les mécanismes de gouvernance du secteur financier (art. 5) ;*
- *mettre en place et maintenir des procédures de gestion des risques informatiques (art. 6 à 16) ;*
- *notifier les incidents de sécurité (art. 17 à 23) ;*
- *réaliser des tests de résilience opérationnelle (art. 24 à 27) ;*
- *encadrer contractuellement les risques liés aux tiers prestataires de services informatiques (art. 28 à 44) ; et*
- *mettre en place des dispositifs de partage d'informations (art. 45).*

DORA prévoit des dispositions contractuelles impératives minimales quelle que soit la criticité des prestations – notamment en termes de description des niveaux de service, de droit d'audit ou de résiliation – ainsi que des dispositions supplémentaires pour les contrats portant sur des fonctions critiques ou importantes.

Le règlement impose également la mise en place d'un cadre de supervision des prestataires IT critiques, qui seront soumis à une évaluation renforcée en matière de gestion des risques.

Présentation générale

Le règlement DORA a un champ d'application très large et englobe la quasi-totalité du secteur financier. Il s'étend ainsi à vingt-et-une catégories d'entités parmi lesquelles les établissements de crédit, les établissements de paiement, les établissements de monnaie électronique, les entreprises d'assurance, ou les sociétés de gestion. Il s'applique également directement aux tiers prestataires de services informatiques.

D'une manière générale, DORA a pour objectif d'améliorer la résilience opérationnelle informatique des entités financières, ce qui se traduit en particulier par :

- l'adoption de cadres de gouvernance et de contrôle internes garantissant une gestion efficace et prudente de tous les types de risques informatiques ;
- la mise en place et le maintien de politiques de gestion des risques informatiques destinées à protéger efficacement les actifs informationnels et IT des entités financières ;
- des obligations de notifications aux autorités compétentes (et dans certaines hypothèses aux clients finaux) des incidents majeurs liés à l'informatique, selon un modèle commun et une procédure harmonisée ;
- la réalisation de test de la résilience destinés à vérifier le niveau de préparation aux risques, d'identifier les éventuelles faiblesses, et de prendre rapidement des mesures correctives ;
- des mécanismes d'échange entre entités financières d'informations sur les cybermenaces ;
- des exigences contractuels permettant d'encadrer les risques liés aux prestataires de services informatiques tel que détaillé ci-après.

Ces obligations entrainent nécessairement des transformations internes des entités financières concernées mais ont également un impact majeur pour leurs partenaires technologiques.

Focus sur l'encadrement des risques liés aux prestataires de services informatiques tiers

Le règlement DORA encadre les risques liés aux prestataires IT de deux manières :

- en énonçant des principes et dispositions devant figurer dans les contrats conclus par les entités financières, et
- en instaurant un cadre de supervision de ces prestataires.

- *Les dispositions devant figurer dans les contrats conclus par les entités financières*

Selon l'article 28 du règlement, des principes généraux doivent être respectés par les entités financières dans les relations qu'elles nouent avec des tiers prestataires de services informatiques, se traduisant en particulier par :

- l'assurance que leurs prestataires respectent des normes adéquates en matière de sécurité ;
- l'ajout dans leurs contrats de facultés de résiliation dans certaines hypothèses ;
- la possibilité d'exercer leurs droits d'accès, d'inspection et d'audit ;
- l'aménagement de la réversibilité des prestations soutenant des fonctions critiques ou importantes.

DORA énonce également une liste d'éléments devant *a minima* figurer dans tous les contrats conclus entre une entité financière et un prestataire IT, parmi lesquels :

- l'indication des lieux où les services seront fournis et les données seront traitées ;
- des dispositions sur la disponibilité, l'authenticité, l'intégrité et la confidentialité des données, notamment à caractère personnel,
- des dispositions sur la garantie de l'accès, de la récupération et de la restitution des données en cas d'insolvabilité, de résolution, de cessation des activités du prestataire tiers de services IT ou de résiliation ;
- des descriptions des niveaux de service ;
- l'obligation pour le prestataire tiers de services IT de fournir à l'entité financière, sans frais supplémentaires ou à un coût déterminé ex ante, une assistance en cas d'incident ;
- l'obligation pour le prestataire de coopérer pleinement avec les autorités compétentes et les autorités de résolution de l'entité financière ;
- les droits de résiliation et les délais de préavis minimaux ; et
- les conditions de participation des prestataires tiers de services IT aux programmes de sensibilisation à la sécurité et aux formations à la résilience opérationnelle numérique élaborés par les entités financières.

Pour les services IT soutenant des fonctions critiques ou importantes, d'autres obligations s'appliquent notamment celles concernant :

- les niveaux de service et les mesures correctives applicables;
- les délais de préavis et les obligations de notification par le prestataire concernant leurs capacité à fournir des services soutenant des fonctions critiques ou importantes dans certaines conditions ;
- l'obligation de mettre en œuvre et de tester des plans d'urgence ;
- l'obligation de mettre en place des mesures, des outils et des politiques de sécurité complémentaires;
- l'obligation pour le prestataire de participer et de coopérer pleinement aux *pen-tests* réalisés par l'entité financière ;
- le droit d'assurer un suivi permanent des performances du prestataire ; et
- les stratégies de sortie des contrats avec des périodes de transition adéquate obligatoire.

Le règlement encourage par ailleurs le développement de clauses contractuelles types devant être élaborées pour des services particuliers par les autorités européennes de surveillance (AES) et adoptées par la Commission européenne.

- *L'instauration d'un cadre de supervision des prestataires critiques de services informatiques*

Le règlement établit un cadre de supervision des prestataires critiques de services informatiques, qui seront désignés par les AES au regard d'un ensemble de critères : effet systémique sur la stabilité, la continuité ou la qualité de la fourniture de services financiers, dépendance des entités financières, degré de substituabilité, etc.

La supervision des prestataires critiques de services IT consiste en une évaluation des règles, procédures, mécanismes et dispositifs qu'ils ont mis en place pour gérer les risques informatiques qu'ils sont susceptibles de faire peser sur les entités financières. Dans ce cadre, les entités de supervision sont dotées de pouvoirs élargis, parmi lesquels le pouvoir de demander l'ensemble des informations et des documents pertinents, de mener des enquêtes et des inspections générales ou de formuler des recommandations.

Ce corpus de règles sera impactant de part et d'autre, tant d'un point de vue des process que des relations contractuelles, et devra être mis en œuvre dans un délai qui est finalement très court au regard de l'ampleur des taches à mener pour être en conformité à la date d'entrée en vigueur du règlement.