_swissprivacy.law

DORA, le règlement européen sur la résilience opérationnelle numérique du secteur financier

Michael Montavon, le 29 février 2024

Nouvelle pierre à l'édifice numérique européen, DORA vise à renforcer la résilience du secteur financier face aux cybermenaces. Il impose la mise en place de mesures pour gérer les risques liés aux TIC et atténuer les effets d'une défaillance.

Règlement (UE) 2022/2554 sur la résilience opérationnelle numérique du secteur financier

Dans un rapport de 2020 consacré au cyberrisque, le Comité européen du risque systémique (CERS) a mis en évidence que la dématérialisation du secteur financier et le niveau élevé d'interconnexion entre les entités financières, les marchés financiers et les infrastructures des marchés financiers remplissent les conditions d'un risque systémique. À travers les canaux de transmission existant, une atteinte grave à la sécurité des technologies de l'information et de la communication (TIC) qui se produirait auprès d'un établissement financier pourrait rapidement contaminer d'autres acteurs du secteur. Un tel évènement aurait des conséquences préjudiciables pour la stabilité du système financier européen.

Pourtant, les enjeux liés à la résilience opérationnelle numérique du secteur financier et à la sécurité des TIC restent assez peu abordés dans le droit de l'UE. Ils sont rarement traités pour eux-mêmes mais se retrouvent intégrés dans les principales catégories de risques financiers (risque de crédit, risque de marché, risque de liquidité…), ce qui peut conduire à des chevauchements, des lacunes ou des incohérences entre les différents textes. De plus, les actes juridiques qui abordent ces questions privilégient une approche quantitative classique de la gestion du risque, basée sur des exigences de fonds propres, plutôt que de proposer des mesures qualitatives et ciblées.

Pour remédier à cette lacune, l'Union européenne a adopté le 14 décembre 2022 le règlement européen sur la résilience opérationnelle numérique du secteur financier (*Digital Operational Resilience Act*, DORA). Les entités financières et leurs fournisseurs de services TIC ont jusqu'au 17 janvier 2025 pour satisfaire aux nouvelles exigences.

Champ d'application

Le champ d'application de DORA est donné à l'art. 2 du règlement. Il inclut une vingtaine d'entités financières, telles que les établissements de crédit et de paiement, les entreprises d'investissement, les plateformes de négociation, les sociétés de gestion, les entreprises d'assurance ou encore les prestataires de services de financement participatif. L'ensemble des dispositions n'est cependant pas applicable à toutes les entités financières de façon uniforme. Dans un souci de ne pas soumettre les acteurs de taille moindre à des exigences disproportionnées, il est prévu que les entités financières mettent en œuvre les exigences prescrites « 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 » (art. 4 DORA). Ainsi, certaines obligations prévues par DORA ne s'appliquent pas ou pas intégralement aux microentreprises actives dans le secteur financier.

En plus des entités financières elles-mêmes, DORA s'applique (in-)directement à leurs prestataires de services TIC (art. 2 par. 1, let. u DORA). Ceux-ci doivent dès lors s'attendre à une augmentation des demandes d'information de la part de leurs clients d'ici 2025. Certains d'entre eux peuvent, en plus, être désignés comme « critiques », ce qui les soumet à un régime spécial de surveillance, décrit ci-dessous.

Contrairement au RGPD, DORA ne présente pas directement d'effets extraterritoriaux. Le nouveau texte recourt toutefois à une forme de territorialité imposée. Afin d'assurer l'exécution des normes prescrites, les prestataires tiers critiques de services TIC opérant depuis l'étranger sont tenus d'établir une filiale dans l'Union (art. 31 par. 12 DORA). Il est aussi prévu qu'une autorité européenne de surveillance puisse procéder à une inspection en dehors de l'Union au siège ou dans un autre local du prestataire. Pareille inspection est cependant soumise à la double condition que le prestataire ait donné son consentement et que l'autorité de surveillance du pays tiers ne s'y soit pas opposée (art. 36 DORA).

Gouvernance des TIC et gestion du risque

DORA promeut un ensemble de principes facilitant la structure globale de la gestion du risque lié aux TIC. Il exige de chaque entité financière qu'elle se dote d'un cadre de gouvernance et de contrôle interne concernant l'usage des TIC (art. 5 DORA). La responsabilité de l'élaboration et du suivi de ce cadre incombe directement à l'organe de direction de l'entité financière, même si souvent seule une approbation est requise. Le cadre de gouvernance inclut notamment le niveau d'exigence à atteindre en matière de disponibilité, d'authenticité, d'intégrité et de confidentialité des données, la définition des rôles et des différentes responsabilités pour toutes les fonctions liées aux TIC, l'existence d'un plan de continuité, de

réponse et de rétablissement des activités TIC, la détermination du niveau approprié de tolérance au risque, l'allocation des budgets pour satisfaire aux besoins en matière de résilience opérationnelle et de sécurité, l'établissement d'une politique relative aux prestataires tiers de services TIC et la mise en place de canaux de notification permettant à la direction d'être tenue informée des accords passés et de leur suivi.

Les entités financières doivent également disposer d'un cadre de gestion du risque lié aux TIC (art. 6 DORA). Intégré au dispositif global de gestion des risques de chaque entité financière, il s'appuie sur une stratégie de résilience opérationnelle numérique. Cette dernière définit les modalités de mise en œuvre du dispositif et fixe les objectifs à atteindre. Font notamment partie du cadre de gestion du risque lié aux TIC les obligations suivantes :

- l'utilisation et le maintien de systèmes, de protocoles et d'outils adaptés, fiables, performants et capables d'assurer une résilience technologique suffisante pour faire face à des épisodes de tension sur les marchés ou à d'autres situations défavorables (art. 7 DORA) ;
- l'identification, le classement et la documentation de toutes les fonctions « métiers », de tous les rôles et de toutes les responsabilités s'appuyant sur les TIC, ainsi que la mise en évidence des différentes dépendances (art. 8 DORA) ;
- l'adoption de stratégies, de politiques, de procédures et d'outils visant à réduire au minimum les incidences des risques liés aux TIC et à protéger les actifs numériques (art. 9 DORA) ;
- l'institution de mécanismes permettant de détecter rapidement les activités anormales (art. 10 DORA) ;
- la mise en place de plans de continuité des activités reposant sur les TIC, notamment en ce qui concerne les fonctions critiques ou importantes externalisées ou sous-traitées (art. 11 DORA) ;
- l'élaboration de politiques et de procédures de sauvegardes, de restauration et de rétablissement incluant l'usage de systèmes TIC qui sont séparés physiquement et logiquement du système TIC source (art. 12 DORA) ;
- la capacité de recueillir des informations sur les vulnérabilités et les cybermenaces, et sur les incidents liés aux TIC, en particulier les cyberattaques, et d'analyser leurs incidences probables sur la résilience opérationnelle numérique (art. 13 DORA) ;
- la création de plans de communication en situation de crise vis-à-vis du public, de la direction, du personnel interne et des autorités (art. 14 DORA).

La mise en œuvre de ces obligations doit être rigoureusement documentée et être améliorée

en permanence sur la base des enseignements tirés. Des audits internes réguliers doivent être menés par une fonction de contrôle bénéficiant d'un niveau approprié d'indépendance.

Gestion, classification et notification des incidents liés aux TIC

DORA améliore et rationalise la prise en charge et la notification des incidents majeurs liés aux TIC. Elle impose aux institutions financière la mise en place d'un processus de gestion des incidents afin de détecter, de gérer et de notifier ce type d'incidents à l'interne et à l'externe (art. 17 DORA). Les seuils et les taxinomies de notification des incidents sont harmonisés entre eux grâce à des critères uniformes à l'échelle de l'Union (art. 18 DORA), ce qui simplifie la situation des entités financières actives dans plusieurs Etats ou qui font partie d'un groupe financier.

Les incidents majeurs doivent systématiquement être notifiés de manière centralisée à l'autorité nationale de surveillance désignée, mais les entités financières ont aussi la possibilité d'annoncer, à titre volontaire, les cybermenaces qu'elles estiment importantes, si elles sont d'avis que la menace est pertinente pour le système financier, les utilisateurs de services ou les clients (art. 19 DORA). Chaque notification suit un schéma en trois étapes incluant une notification initiale, un rapport intermédiaire sur l'évolution de l'incident et un rapport final, lorsque l'analyse des causes originelles est terminée. Une fois notifiée, l'autorité nationale de surveillance se charge, le cas échéant, d'informer les autorités nationales et européennes concernées.

Les exigences de communication vis-à-vis des clients ne sont pas oubliées. En présence d'un incident majeur ayant une incidence sur les intérêts financiers des clients, les entités financières doivent promptement notifier ces derniers et les informer des mesures prises pour atténuer les effets de l'incident (art. 19 par. 3 DORA). Ce mécanisme n'est pas sans rappeler l'obligation de notification des personnes concernées imposée à l'art. 34 RGPD. Selon cette disposition, les responsables du traitement doivent informer les personnes concernées en cas d'incident de sécurité susceptible de causer un risque élevé pour leurs droits et leurs libertés. Toutefois, DORA va un cran plus loin. En cas de cybermenace importante pouvant constituer une menace pour leurs clients, les entités financières sont tenues de les informer de manière proactive et de leur suggérer toute mesure utile.

Tests de résilience opérationnelle numérique

Le but premier de DORA est de renforcer la résilience opérationnelle numérique des entités financières. On entend par là « la capacité […] à développer, garantir et réévaluer son inté-

grité et sa fiabilité opérationnelles en assurant directement ou indirectement par le recours aux services fournis par des prestataires tiers de services TIC, l'intégralité des capacités liées aux TIC nécessaires pour garantir la sécurité des réseaux et des systèmes d'information qu'elle utilise, et qui sous-tendent la fourniture continue de services financiers et leur qualité, y compris en cas de perturbations » (art. 3 par. 1 DORA).

Pour atteindre cet objectif, les entités financières sont tenues de mettre au point un programme solide et complet de tests de résilience opérationnelle numérique. Pareil programme vise à évaluer l'état de préparation en vue du traitement d'incidents liés aux TIC, à recenser les faiblesses, les défaillances et les lacunes en matière de résilience opérationnelle numérique et à démontrer la capacité de l'entité financière à mettre rapidement en œuvre des mesures correctives (art. 24 DORA).

Les tests à mener vont de l'évaluation des exigences de base (art. 25 DORA : par exemple, évaluations et analyses de la vulnérabilité, analyses de sources ouvertes, évaluations de la sécurité des réseaux, analyses des lacunes, examens de la sécurité physique, questionnaires et solutions logicielles d'analyse, examens du code source lorsque cela est possible, tests fondés sur des scénarios, tests de compatibilité, tests de performance ou tests de bout en bout) à des tests plus avancés au moyen de tests de pénétration fondés sur la menace couvrant les fonctions les plus critiques de l'entité financière, y compris celles ayant été externalisées (art. 26 DORA).

La réalisation des tests peut être confiée soit à des testeurs internes, soit à des testeurs externes, chaque solution étant soumises à des exigences particulières (art. 27 DORA).

Externalisation

DORA met un accent particulier sur la gestion des risques associés aux prestataires tiers de services TIC (fournisseurs de services cloud, de logiciels, d'infrastructures numérique…) mais aussi aux entreprises qui font partie d'un groupe financier et qui fournissent des services TIC principalement à leur entreprise mère ou à des filiales ou succursales de leur entreprise, ainsi qu'aux entités financières fournissant des services TIC à d'autres entités financières.

Pour chaque contrat IT, quel que soit le niveau de criticité ou d'importance, les entités financières doivent veiller à insérer un certain nombre d'éléments minimaux (art. 30 par. 2 DORA), notamment :

- une description claire et exhaustive des fonctions et des services externalisés ;

- l'indication des lieux où les services sont fournis et les données traitées ;
- des dispositions sur la disponibilité, l'authenticité, l'intégrité et la confidentialité des données, notamment des données personnelles ;
- 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 ou de résiliation ;
- des descriptions des niveaux de service ;
- l'obligation pour le prestataire de fournir à l'entité financière, sans frais supplémentaires ou à un coût déterminé par avance, une assistance en cas d'incident ;
- l'obligation pour le prestataire de coopérer pleinement avec les autorités compétentes de l'entité financière ;
- l'insertion de droits de résiliation et de délais de préavis minimaux ;
- les conditions de participation aux programmes de sensibilisation à la sécurité et aux formations à la résilience opérationnelle numérique élaborés par l'entité financière.

Pour les contrats IT relatifs à la fourniture de services TIC, qui soutiennent des fonctions critiques ou importantes de l'entité financière, des exigences supplémentaires sont prévues (art. 30 par. 3 DORA). En plus des éléments déjà cités, les contrats doivent inclure au minimum :

- des descriptions complètes des niveaux de service et les mesures correctives y relatives ;
- les délais de préavis pertinents et les obligations de notification incombant au prestataire en cas d'évolutions susceptibles d'avoir une incidence significative sur la capacité de ce dernier à fournir efficacement les services convenus ;
- 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 de participer et de coopérer pleinement aux tests de pénétration réalisés par l'entité financière ;
- l'exercice des droits d'accès, d'inspection et d'audit par l'entité financière ;
- la coopération du prestataire lors d'inspections et/ou d'audits menées par les autorités européennes de surveillance ;
- les stratégies de sortie des contrats avec des périodes de transition adéquate obligatoires.

Le règlement encourage par ailleurs le développement de clauses contractuelles types par

les autorités européennes de surveillance ou encore par la Commission européenne pour les services d'informatiques en nuage.

Même si DORA renonce à imposer tout plafond rigide dans ce domaine, le règlement oblige encore les entités financières à tenir compte du risque de concentration (art. 29 DORA). Le recours soutenu à des prestataires tiers de services TIC individuels ou multiples est susceptible de conduire à une trop forte dépendance de l'entité financière. En cas d'indisponibilité, de défaillance ou de tout autre type d'insuffisance survenant chez ces catégories de prestataire, il peut en résulter une incapacité de l'entité financière à assumer ses tâches. C'est pourquoi DORA exige des entités financières qu'elles examinent de manière proactive le risque de concentration et qu'elles procèdent à une évaluation attentive des risques avant de conclure tout nouveau contrat portant sur des services TIC qui soutiennent des fonctions critiques ou importantes.

Cadre de supervision des prestataires tiers critiques de services TIC

Constatant que le bon fonctionnement du système financier de l'Union est largement tributaire de fournisseurs tiers de services informatiques, DORA met en place un cadre unique de supervision des prestataires tiers de services TIC dits « critiques » (art. 3 par. 23 DORA).

L'inclusion dans le cadre de supervision dépend d'une liste de critères quantitatifs et qualitatifs (art. 31 DORA), tels que :

- l'effet systémique sur la stabilité, la continuité ou la qualité de la fourniture de services financiers dans les cas où le prestataire tiers de services TIC concerné serait confronté à une défaillance ;
- le caractère ou l'importance systémique de l'entité financière concernée ;
- le degré de dépendance de l'entité financière par rapport au service fourni ;
- les possibilités de substitution du prestataire tiers de services TIC.

La décision d'inclure un prestataire tiers de services TIC dans la liste des prestataires dits critiques incombe aux Autorités européennes de surveillance (Autorité bancaire européenne [ABE] ; Autorité européenne des assurances et des pensions professionnelles [AEAPP] ; Autorité européenne des marchés financiers [AEMF]), mais un prestataire tiers de service TIC peut aussi demander à rejoindre le cadre de supervision sur une base volontaire.

Les prestataires tiers critiques de services TIC sont soumis à une évaluation préalable visant à déterminer s'ils ont mis en place des règles, des procédures, des mécanismes et des dispo-

sitifs complets, solides et efficaces pour gérer le risque lié aux TIC qu'ils font peser sur les entités financières (art. 33 DORA). Cette évaluation sert à l'élaboration d'un plan de supervision individuel décrivant les objectifs annuels de supervision et les principales actions de supervision prévues.

Durant la supervision, l'autorité compétente dispose de différents pouvoirs sur les prestataires concernés. Elle peut :

- formuler des demandes d'informations et exiger la fourniture de tous documents commerciaux ou opérationnels, contrats, documents stratégiques, rapports d'audit de sécurité TIC, rapports d'incidents liés aux TIC et toute autre information relative aux entités financières avec lesquelles travaille le prestataire (art. 37 DORA) ;
- mener des enquêtes générales, examiner des documents, en demander des copies, convoquer les représentants du prestataire et les interroger, obtenir les enregistrements d'échanges téléphoniques (art. 38 DORA) ;
- conduire des inspections dans les locaux du prestataire, investiguer les systèmes, les réseaux, les dispositifs et les données (art. 39 DORA) ;
- contraindre le prestataire à payer des astreintes journalières égales à 1 % au maximum du chiffre d'affaires quotidien moyen réalisé au niveau mondial en cas de refus de coopérer (art. 35 par. 6 DORA) ;
- formuler des recommandations à l'égard du prestataire, notamment pour qu'il mette en place des processus spécifiques de sécurité et de qualité en matière de TIC ou qu'il renonce à travailler avec certains sous-traitants (art. 35 par. 1 let. d DORA).

Lorsqu'une autorité de surveillance formule une recommandation, le prestataire visé dispose d'un délai de 60 jours pour se déterminer. En cas de refus de la recommandation, l'autorité de surveillance a le pouvoir de prononcer une décision par laquelle elle suspend temporairement, en partie ou en totalité, l'utilisation ou le déploiement du service fourni jusqu'à ce que les problèmes identifiés soient résolus. Ultimement, elle peut exiger la résiliation, totale ou partielle, des accords conclus entre l'entité financière et le prestataire (art. 42 DORA).

Commentaire

En Suisse, les normes concernant la résilience opérationnelle numérique et l'externalisation dans le secteur financier figurent dans les circulaires de la FINMA 2023/1 en matière de risques opérationnels et de garantie de la résilience opérationnelle, et 2018/3 en matière d'outsourcing (https://swissprivacy.law/27). Respectant l'approche traditionnelle de la régulation en Suisse, les textes adoptés ne sont néanmoins pas aussi denses et précis que ne l'est

DORA. Il serait cependant inexact de vouloir ranger DORA dans la catégorie des textes rigides ou excessivement prescriptifs de l'UE. Le règlement aborde plutôt une approche hybride, combinant des principes généraux bien expliqués avec des exigences plus précises dans des domaines spécifiques où la clarté, l'uniformité et la précision sont nécessaires pour assurer au secteur financier un niveau de résilience et de sécurité harmonisé à l'échelle de l'Union. L'approche structurée et méthodique du texte devrait par ailleurs grandement en faciliter l'exécution.

Il est vrai, malgré tout, qu'il s'agit d'une matière qui reste extrêmement technique et exigeante. Même si le texte est clair et intelligible, l'exercice pratique consistant à le mettre en œuvre ne sera pas aisé pour autant. En outre, la bonne exécution du cadre de supervision des prestataires tiers critiques de services TIC n'est pas gagnée d'avance en dépit de son évidente légitimité. En plus d'exiger des ressources considérables de la part des autorités de surveillance, l'exécution des mesures et des décisions prises à l'égard de certains prestataires tiers de services TIC risque de se heurter à de réelles difficultés.

Finalement, bien qu'il ait été conçu spécifiquement pour le secteur financier, DORA regroupe l'ensemble des bonnes pratiques actuelles en matière de sécurité de l'information. Les administrations publiques et les entreprises privées qui ont des besoins spécifiques dans ce domaine y trouveront à n'en pas douter une source d'inspiration inestimable tant sous l'angle pratique que réglementaire ou même législatif.

Proposition de citation : Michael Montavon, DORA, le règlement européen sur la résilience opérationnelle numérique du secteur financier , 29 février 2024 *in* www.swissprivacy.law/285