racine
AVOCATS

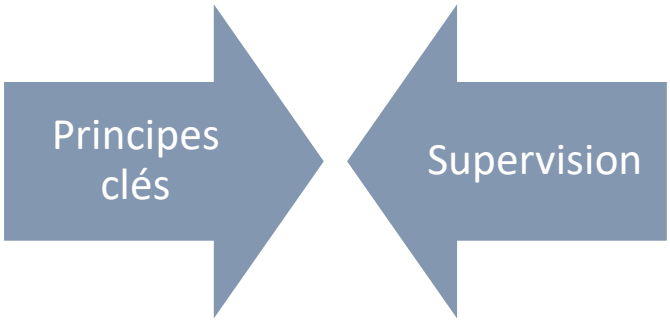
Les RDV Experts

DORA | La série décryptage Banque – Finance – Assurance & IP/IT

DORA #5 : Les prestataires tiers

Nous voici à l'épisode 5 de la réglementation DORA qui complète notre épisode 4 consacré au « Cadre de gestion de risque ».
Nous traiterons ici du cas particulier de la « gestion des risques liés aux prestataires tiers TIC » selon le titre du Chapitre V du règlement.
Ce chapitre intéressera à la fois les métiers, mais aussi les juristes.

Ce chapitre 5 fixe deux types de règles :



En synthèse des articles 28 à 30 de DORA, on retiendra que le règlement :

1. Impose un certain nombre de vérifications avant la conclusion d'un contrat ;
2. Impose un certain nombre de clauses à prévoir dans les contrats ;
3. Impose un certain nombre de documents de nature technico juridique ;
4. Impose la mise en œuvre de dispositifs d'audit ;
5. Impose un certain nombre d'obligations périphériques.

Audit préalable

À l'instar du RGPD, un établissement soumis à DORA devra procéder à certaines vérifications avant la signature du contrat et notamment : qualifier si la prestation porte ou non sur une fonction critique ou importante, évaluer le risque et de la prise en compte des impératifs de sécurité par le prestataire… De ce point de vue, l'envoi d'une grille d'audit préalable à la signature du contrat s'impose. Elle peut être combinée avec la grille RGPD dans le cas où le prestataire agit en tant que sous-traitant.

Clauses contractuelles imposées

DORA s'intéresse également aux clauses contractuelles elles-mêmes comme les conditions de résiliation (article 28.7), les stratégies de sorties (exemple : la réversibilité), l'assistance en cas d'incident (article 30.2 f), obligation de coopération avec les autorités compétentes (article 30.2 g), la participation du prestataire aux programmes de sensibilisation, etc.

Les établissements soumis à DORA devront contrôler la conformité de tous leurs contrats IT à ces exigences et au besoin signer des "avenants DORA" avec les prestataires concernés.

Le règlement prévoit également des règles particulières pour les contrats avec des prestataires qui soutiennent des fonctions critiques ou importantes, comme l'obligation de respecter un délai de notification des développements susceptibles d'avoir une incidence significative sur le client, l'obligation de tester un plan d'urgence ou encore l'obligation de participer pleinement aux tests de pénétration.

De ce fait, DORA impose que soit annexé aux contrats un certain nombre de documents de nature technico-juridique tels que les PAS, SLA ou encore « Plan de sortie ».

Audit des prestataires

Au cas particulier des prestataires IT soutien de fonctions critiques ou importantes, DORA impose la mise en œuvre de clauses spécifiques relatives aux audits.

Le contrat doit nécessairement comporter des dispositions permettant au client :

- De disposer des droits illimités d'accès, d'inspection et d'audit par lui-même ou par une tierce partie (et par l'autorité compétente), et le droit de prendre des copies des documents pertinents sur place dont l'exercice effectif n'est pas entravé ou limité par d'autres accords contractuels ou politiques d'exécution.
- L'obligation pour le prestataire tiers de services TIC de coopérer pleinement lors des inspections sur place et lors des audits effectués par les autorités compétentes, le superviseur principal, l'entité financière ou une tierce partie désignée.

- L’obligation de fournir des précisions sur la portée, les procédures à suivre et la fréquence de ces inspections et audits.

Bien qu’une telle obligation ne soit pas applicable à tous les contrats, nous préconisons cependant de généraliser des clauses d’audit.

Mais une « simple » clause ne suffit pas. Il est indispensable de joindre au contrat (en annexe) la procédure d’audit documentaire ou sur inspection.

Registre

Enfin DORA renforce l’obligation de tenir un registre des prestataires IT et de le tenir à jour.

Les entités soumises à DORA doivent ainsi tenir et mettre à jour, au niveau de l’entité et aux niveaux sous-consolidé et consolidé, un registre d’informations en rapport avec tous les accords contractuels portant sur l’utilisation de services TIC fournis par des prestataires tiers de services TIC.

Ces accords contractuels sont dûment documentés, en opérant une distinction entre ceux qui couvrent des services TIC qui soutiennent des fonctions critiques et ceux qui ne le font pas.

Ces mêmes entités mettent à la disposition de l’autorité compétente, si elle en fait la demande, le registre d’informations complètes ou, le cas échéant, des sections spécifiques de celui-ci, ainsi que toute information jugée nécessaire pour garantir une surveillance efficace de l’entité financière.

Enfin, elles communiquent au moins une fois par an aux autorités compétentes le nombre de nouveaux accords relatifs à l’utilisation de services TIC, les catégories de prestataires tiers de services TIC, le type d’accords contractuels et les services et fonctions de TIC qui sont fournis.

Certains établissements soumis à DORA estiment être déjà conformes, car ils appliquent les règles édictées par l’EBA ou par l’AEAPP.

Il s’agit selon nous d’une erreur d’appréciation qui peut conduire à des non-conformités majeures à compter de janvier 2025.

À titre d’exemple l’EBA fixe un certain nombre de règles concernant les prestations d’externalisation là où DORA s’étend à toute prestation TIC.

De ce fait, tous les contrats TIC doivent être identifiés, répertoriés dans le registre des prestataires tiers et beaucoup de contrats devront faire l’objet d’un avenant pour être conformes à DORA.

Voir nos précédents épisodes

DORA #4 : La gestion du risque lié aux TIC, il ne vous reste qu'un an !
DORA#3 : Le cadre répressif
DORA #2 : Le champ d'application
DORA #1 : La genèse

IP/IT

Eric Barbry
Avocat Associé
ebarbry@racine.eu

Banque – Finance – Assurance

Sonia Oudjhani-Rogez
Avocat Counsel
soudjhanirogez@racine

Lena Chemla
Avocat
lchemla@racine.eu