Les RDV Experts

RISQUES CYBER - RGPD | DORA | NIS2

Le prestataire IT : Qui est responsable ?

Dans notre précédent « RDV Experts » nous évoquions les nouvelles contraintes qui portent sur les entreprises et les acteurs publics pour ce qui concerne les contrats avec les prestataires tiers dans le domaine de l'IT.

Mais la responsabilité n'est pas seulement celle de l'établissement public ou privé en tant que personne morale, deux autres acteurs sont directement visés par les nouvelles règles européennes, notamment :

- **Les « organes de direction » ;**
- **Les « membres de l'encadrement supérieur responsables des TIC »**

La responsabilité des « organes de direction »

Il suffit de lire quelques considérants de NIS2 ou DORA pour prendre la mesure de cette responsabilité. Il en est ainsi du Considérant 137 de NIS2 ou du Considérant 45 de DORA.

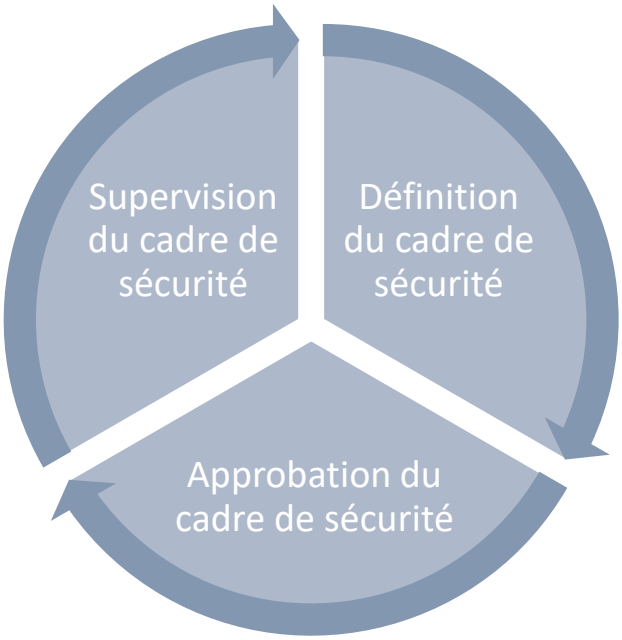
Extrait NIS 2

« La présente directive devrait viser à assurer un niveau de responsabilité important pour les mesures de gestion des risques en matière de cybersécurité et les obligations d'information au niveau des entités essentielles et importantes. Par conséquent, ***les organes de direction*** *des entités essentielles et importantes* ***devraient approuver les mesures de gestion des risques en matière de cybersécurité et superviser leur mise en œuvre****. »*

Extrait DORA

« Pour garantir une concordance complète et une cohérence globale entre les stratégies d'entreprise des entités financières, d'une part, et la mise en œuvre de la gestion du risque lié aux TIC, d'autre part, ***les organes de direction des entités financières devraient être tenus de conserver un rôle actif et déterminant dans la conduite et l'adaptation du cadre de gestion du risque lié aux TIC*** *et de la stratégie globale de résilience opérationnelle numérique. (…)*

En pratique les organes de direction sont tenus par 3 grandes obligations :



NIS2 va même jusqu'à imposer aux organes de direction de suivre une formation de nature à « acquérir des connaissances et des compétences suffisantes pour déterminer les risques et évaluer les pratiques de gestion des risques en matière de cybersécurité et leur impact sur les services fournis par l'entité ».

Quant à DORA elle retient la notion de responsabilité « **ultime** » des organes de direction.

La responsabilité des membres de l'équipe IT

Les nouvelles règles ne visent pas les seuls organes de direction. Elles visent également certains membres de l'équipe en charge de l'IT. L'article 13 de DORA précise par exemple que

« 5. Les membres de **l'encadrement supérieur responsables des TIC** rendent compte au moins une fois par an, à l'organe de direction, des constatations visées au paragraphe 3 et formulent des recommandations. ».

Bien que cette notion de « membres de l'encadrement supérieur » ne soit pas précisée, il est clair que les DSI et les RSSI/CISO dès lors qu'ils ont le statut de cadre supérieur sont visés par cette obligation.

De fait leur responsabilité pourrait être engagée :

- Soit pour ne pas avoir rendu compte à l'organe de direction des résultats des tests de résilience opérationnelle numérique et des incidents liés aux TIC en situation réelle ;
- Soit de ne pas avoir formulé des recommandations adaptées.

Il apparaît dès lors primordial de bien définir les rôles de chacun dans le cadre d'une gouvernance risque IT.

Votre cybersécurité repose sur vos sous-traitants : êtes-vous prêts ?

Pour explorer le sujet plus en détail et répondre à toutes les questions que vous vous posez :

- À quels textes suis-je soumis ?
- Quel est le niveau de maturité attendu ?
- Quelles sont les sanctions encourues ?
- Quel référentiel appliquer ?
- Comment vérifier la conformité de mes prestataires IT ?
- Quelles sont les clauses contractuelles imposées ou impactées ?
- Quelles sont mes obligations en termes d'audit et leurs conséquences ?

Nous vous donnons rendez-vous le 19 mars à 10h pour un webinar inédit, animé par nos experts !

👉 **https://webikeo.fr/webinar/cybersecurite-impact-des-nouvelles-regles-europeennes-sur-vos-relations-avec-vos-prestataires-it**

Eric Barbry
Avocat Associé spécialisé IP/ IT
ebarbry@racine.eu

Marc-Antoine Ledieu
Avocat à la Cour et RSSI legal
marc-antoine@ledieu-avocats.fr

Jean-Philippe Gaulier
CEO de Cyberzen
jpg@cyberzen.com