Note juridique Directive NIS 2

La directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifie le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2).

Cette directive a été publiée au Journal Officiel du 27 décembre 2022 et doit être transposée pour le 17 octobre 2024 au plus tard dans chaque État membre.

La directive NIS 1 était orienté autour de 3 axes :

- atteindre un niveau élevé de préparation des États membres, la directive NIS exige que les États membres adoptent une stratégie nationale sur la sécurité des réseaux et des systèmes d'information. Les États membres sont également tenus de désigner des équipes nationales de réponse aux incidents de sécurité informatique (CSIRT), qui sont responsables du traitement des risques et des incidents, une autorité nationale compétente et un point de contact unique (SPOC). Le SPOC doit exercer une fonction de liaison pour assurer la coopération transfrontalière entre les autorités de l'État membre, les autorités compétentes des autres États membres et le groupe de coopération NIS.

- établir le groupe de coopération NIS pour soutenir et faciliter la coopération stratégique et l'échange d'informations entre les États membres, et le réseau CSIRT qui favorise une coopération opérationnelle rapide et efficace entre les CSIRT nationaux.

- Veiller à ce que des **mesures de cybersécurité** soient prises dans sept secteurs, qui sont vitaux pour l'économie et la société et qui dépendent fortement des TIC :
  - Energie ;
  - Les Transports ;
  - **Les infrastructures bancaires ;**
  - **Les infrastructures des marchés financiers ;**
  - L'eau potable ;
  - Les soins de santé ;
  - Les infrastructures numériques.

La directive NIS 2 augmente considérablement le nombre de secteurs concernés. Pour cela, la directive NIS 2 divise les entreprises en deux groupes :

- Les secteurs **« hautement critiques »** sont identifiés dans l'annexe 1 de la directive NIS 2 :
  - Energie ;
  - Transports ;
  - **Secteur bancaire ;**
  - **Infrastructures des marchés financiers ;**
  - Santé ;

- Eau potable ;
- Eaux usées ;
- Infrastructures numériques ;
- Gestion des services TIC ;
- Administrations publiques ;
- Espace.

- Les « autres secteurs critiques » sont identifiés dans l'annexe 2 de la directive NIS 2 :
  - Services postaux et d'expédition ;
  - Gestion des déchets ;
  - Fabrication, production et distribution de produits chimiques,
  - Production, transformation et distribution des denrées alimentaires,
  - Fabrication,
  - Fournisseurs numériques,
  - Recherche.

Au sein des secteurs identifiés ci-dessus, les obligations sont à géométrie variable en fonction de la taille de l'entité concernée :

- Sont des entités « **essentielles** », celles qui emploient plus de 50 personnes et ont un chiffre d'affaires supérieur à 10 millions d'euros ;
- les entités qui n'atteignent pas ces seuils mais font partie des secteurs identifiés ci-dessus, sont dites « **importantes** ».

La directive demande aux entreprises d'envisager les risques de manière globale, c'est-à-dire que les entreprises vont devoir intégrer dans leur réflexion la prise en compte des risques associés à la chaîne de valeur (sous-traitants, fournisseurs, etc.)

Les dirigeants des entités essentielles et importantes devront s'impliquer davantage dans la mise en conformité de leur société.

L'article 20 de la directive NIS2 dispose :

- Les États membres veillent à ce que les organes de direction des **entités essentielles et importantes** approuvent les **mesures de gestion des risques en matière de cybersécurité** prises par ces entités afin de se conformer à la directive, supervisent sa mise en œuvre et puissent être tenus responsables de la violation de leurs obligations par ces entités.

- Les États membres veillent à ce que les membres des organes de direction des **entités essentielles** et importantes soient tenus de **suivre une formation** et ils encouragent les entités essentielles et importantes à offrir régulièrement une formation similaire aux membres de leur personnel afin que ceux-ci acquièrent 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.

Les obligations pour les entreprises ont été alourdi, les mesure à mettre en place comprennent au moins :

- Les politiques relatives à l'analyse des risques et à la sécurité des systèmes d'information ;
- La gestion des incidents ;
- La continuité des activités, par exemple la gestion des sauvegardes et la reprise des activités, et la gestion des crises ;
- La sécurité de la chaîne d'approvisionnement, y compris les aspects liés à la sécurité concernant les relations entre chaque entité et ses fournisseurs ou prestataires de services directs ;
- La sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information, y compris le traitement et la divulgation des vulnérabilités ;
- Des politiques et des procédures pour évaluer l'efficacité des mesures de gestion des risques en matière de cybersécurité ;
- Les pratiques de base en matière de cyber hygiène et la formation à la cybersécurité ;
- Des politiques et des procédures relatives à l'utilisation de la cryptographie et, le cas échéant, du chiffrement ;
- La sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs ;
- L'utilisation de solutions d'authentification à plusieurs facteurs ou d'authentification continue, de communications vocales, vidéo et textuelles sécurisées et de systèmes sécurisés de communication d'urgence au sein de l'entité, selon les besoins.