BCLP. Client Intelligent

Insights

QUELLES SONT LES IMPLICATIONS DE LA NOUVELLE DIRECTIVE EUROPÉENNE SUR LES RÉSEAUX ET LES SYSTÈMES D'INFORMATION (NIS 2) POUR LES ENTREPRISES ?

DIGITAL SPEAKS SERIES

Dec 06, 2024

SUMMARY

Faisant partie de la stratégie numérique et de cybersécurité de l'Union Européenne, la nouvelle directive 2022/2555 du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union (dite directive **NIS 2**) est entrée en vigueur le 18 octobre 2024 (il s'agit de la date limite à laquelle la directive devait être transposée en droit national, bien que ce processus ne soit pas encore achevé).

Elle remplace la directive 2016/1148 (dite directive NIS1) et vient compléter le règlement sur la Cyber Resilience (discutée dans un récent article de BCLP). La nouvelle directive NIS 2 vise à élargir le champ d'application de la directive NIS 1 et à couvrir un plus grand nombre d'industries et de secteurs. Les entreprises concernées devront s'assurer que des procédures de gestion des risques soient mises en œuvre au sein de leur organisation. Les organes de direction doivent également acquérir les compétences nécessaires pour assurer le suivi des procédures de sécurité, compte tenu de la responsabilité personnelle en cas de manquement à ses obligations en matière de cybersécurité que la directive NIS 2 impose désormais.

QUELLES SONT LES ENTREPRISES CONCERNÉES PAR LA DIRECTIVE NIS 2 ?

La directive NIS2 couvre des entités appartenant à une grande variété d'industries, et plus particulièrement les entités des « secteurs hautement critiques » et celles opérant dans les « autres secteurs critiques », tels que :

- la santé ;

- la fabrication de produits ou de préparations pharmaceutiques, de médicaments ou de dispositifs médicaux ;
- l'énergie et les services publics
- les transports ;
- les institutions financières (à l'exception de celles qui se conforment aux dispositions relatives à la gestion des risques concernant les technologies de l'information et de la communication et celles du Règlement sur la résilience opérationnelle numérique du secteur financier (**DORA**) ;
- le secteur des infrastructures numériques (y compris les fournisseurs de services de cloud) ;
- les fournisseurs numériques tels que les places de marché en ligne, les moteurs de recherche en ligne et les plateformes de réseaux sociaux ;
- la gestion des services TIC interentreprises ;
- la production de produits chimiques ;
- la production, la transformation et la distribution des denrées alimentaires ;
- la construction de véhicules à moteur, de machines et d'équipements de transport ;
- la construction de produits informatiques, électroniques et optiques ;
- la fabrication d'équipements électriques ; et
- les organismes de recherche.

De nouveaux secteurs ont été ajoutés à la liste de la directive NIS 1, en fonction de leur degré de numérisation et d'interconnexion et de leur importance pour l'économie et la société (la liste complète des secteurs hautement critiques et des autres secteurs critiques figure aux annexes 1 et 2 de la directive NIS 2). La directive NIS 2 introduit également des seuils d'application clairs, de sorte que toutes les PME et les grandes entreprises des secteurs listés sont désormais incluses dans son champ d'application. Les États membres ont également la possibilité d'identifier des entités en deçà des seuils mais présentant un profil de risque élevé en matière de sécurité, lesquelles devront se conformer à la directive NIS 2. La distinction entre les opérateurs de services essentiels et les fournisseurs de services numériques a également été supprimée. Les entités sont désormais classées en fonction de leur importance et divisées en deux catégories : les entités essentielles et les entités importantes, qui sont ainsi soumises à des régimes de surveillance différents.

COMMENT FONCTIONNE LA DIRECTIVE NIS2 ?

Si une entreprise opère dans l'un des secteurs énumérés ci-dessus, elle devra déterminer si elle est une « entité essentielle » ou une « *entité importante* ».

Les **entités essentielles** sont les entreprises qui :

- ont plus de 250 salariés ou qui génèrent plus 50 millions d'euros de chiffre d'affaires et sont actives dans l'un des secteurs suivants : énergie, transport, banque, infrastructures des marchés financiers, santé, eau potable, eaux usées, infrastructure numérique, gestion des services TIC (interentreprises), administration publique, ou espace ; ou qui sont
- des fournisseurs de services de confiance
- des fournisseurs de services DNS (Domain Name System)
- des fournisseurs de réseaux publics de communication électronique
- des entités de l'administration publique
- ont été désignées comme entités critiques en vertu de la directive 2022/2557 relative à la résilience des entités critiques ; ou
- ont été désignées par un État membre comme des entités essentielles ou des opérateurs de services essentiels.

Les **entités importantes** sont toutes les autres organisations qui ne sont pas des entités essentielles et qui exercent des activités :

- de services postaux et de messagerie ;
- de gestion des déchets ;
- de fabrication, la production et la distribution de produits chimiques ;
- de production, la transformation et la distribution de denrées alimentaires ;
- de fabrication de produits alimentaires ;
- de fournisseurs de services numériques ; et
- de recherche.

Les États membres peuvent également désigner une entité comme « entité importante » si elle :

- est le fournisseur exclusif d'un service essentiel au maintien d'activités sociétales ou économiques critiques ;

- fournit un service qui, s'il est perturbé, pourrait avoir une incidence significative sur la sécurité publique ou la santé publique, ou pourrait entraîner un risque systémique significatif ; ou
- est critique en raison de son importance spécifique au niveau national ou régional pour le secteur ou le type de service en question, ou pour d'autres secteurs interdépendants dans l'État membre.

LES PRINCIPALES OBLIGATIONS POUR LES ENTITÉS ENTRANT DANS LE CHAMP D'APPLICATION DE LA DIRECTIVE NIS 2

- **Mesures de gestion du risque de cybersécurité - Article 21** : Des mesures techniques, opérationnelles et organisationnelles appropriées et proportionnées doivent être prises pour gérer les risques qui pèsent sur les réseaux et systèmes d'information que ces entités utilisent pour leurs activités ou pour la fourniture de leurs services, et pour prévenir ou réduire au minimum l'impact des incidents sur les destinataires de leurs services. Compte tenu de l'état de l'art et, le cas échéant, des normes européennes et internationales pertinentes, ainsi que du coût de mise en œuvre, ces mesures doivent garantir un niveau de sécurité des réseaux et des systèmes d'information adapté aux risques encourus. Lors de l'évaluation de la proportionnalité de ces mesures, il est tenu compte du degré d'exposition de l'entité aux risques, de la taille de l'entité et de la probabilité d'occurrence d'incidents et de leur gravité, y compris leur impact sociétal et économique.
- **Responsabilités en matière de gouvernance et de gestion - Article 20** : Les organes de direction des entités essentielles et importantes doivent superviser et approuver les mesures de gestion des risques de cybersécurité prises par ces entités, et les membres dirigeants peuvent être tenus personnellement responsables des infractions aux dispositions de l'article 20.
- **Notification des incidents - Article 23** : Les entités essentielles et importantes doivent notifier, sans retard injustifié, à leur Centre de réponse aux incidents de sécurité informatique (CSIRT ou « *Computer Security Incident Response Team* ») compétent ou, le cas échéant, à l'autorité de régulation concernée, tout incident ayant un impact significatif sur la fourniture de leurs services. Le cas échéant, les entités concernées notifient sans délai aux destinataires de leurs services les incidents significatifs susceptibles d'avoir un impact négatif sur la fourniture de ces services. Les informations communiquées doivent inclure toute information permettant au CSIRT ou, le cas échéant, à l'autorité compétent de déterminer l'impact transfrontalier de l'incident. En cas d'incident transfrontalier ou trans-sectoriel important, les autorités compétentes des États membres veillent à ce que leurs points de contact uniques dans les autres États membres reçoivent en temps utile les informations pertinentes.
- **Recours aux schémas européens de certification de cybersécurité - Article 24** : Les entités essentielles et importantes peuvent être tenues d'utiliser des produits, des services et des

processus TIC particuliers (développés en interne ou achetés à des tiers) qui sont certifiés dans le cadre de schémas européens de certification de cybersécurité.

LE NOUVEAU CADRE DE GOUVERNANCE EUROPÉEN

La directive NIS 2 définit également des obligations pour les États membres de l'UE, ainsi qu'un cadre de gouvernance européen pour le suivi de l'application et de la mise en œuvre des règles de la directive NIS 2.

Les États membres de l'UE doivent ainsi désigner une autorité compétente, un point de contact unique pour le signalement des incidents, désigner ou mettre en place un ou plusieurs CSIRT et assurer la liaison avec l'ENISA (Agence de l'Union européenne pour la cybersécurité) et la Commission, ainsi qu'avec le réseau pour la préparation et la gestion des crises cyber de l'ENISA (CyCLONe). Le groupe de coopération NIS 2 de l'UE, en coopération avec la Commission et l'ENISA, peut effectuer des évaluations coordonnées des risques de sécurité de services TIC critiques spécifiques, de systèmes TIC ou de chaînes d'approvisionnement de produits TIC, en tenant compte des facteurs de risque techniques et, le cas échéant, non techniques. Les autorités nationales de régulation peuvent promouvoir l'utilisation de normes et de spécifications techniques européennes et internationales relatives à la sécurité des réseaux et des systèmes d'information.

SANCTIONS EN CAS DE NON-CONFORMITÉ

Les entreprises qui ne se conforment pas aux nouvelles règles de la directive NIS 2 s'exposent à des sanctions spécifiques, dont des :

- **Mesures correctives non pécuniaires** : injonctions de mise en conformité, injonctions de mise en œuvre d'audits de sécurité et injonctions d'informer les personnes physiques ou morales à l'égard desquelles elles fournissent des services de la nature de la cybermenace, ainsi que de toutes mesures préventives ou réparatrices que ces personnes physiques ou morales pourraient prendre en réponse à cette menace.
- **Amendes administratives** : Les « *entités essentielles* » peuvent se voir infliger une amende maximale d'au moins 10.000.000 € ou 2 % du chiffre d'affaires annuel mondial, le montant le plus élevé étant retenu. Les « *entités importantes* » peuvent quant à elles se voir infliger une amende maximale d'au moins 7.000.000 € ou 1,4 % du chiffre d'affaires annuel mondial, le montant le plus élevé étant retenu.
- **Sanctions pénales :** de nouvelles mesures prévoient que les organes de direction peuvent être tenus personnellement responsables en cas de négligence grave à l'origine d'un incident de sécurité.

INTERRELATION ENTRE LA DIRECTIVE NIS 2 ET LA NORME ISO 27001

Il convient de noter que la conformité à la norme ISO 27001 ne préjuge pas de la conformité à la directive NIS2. La norme ISO 27001 doit donc être considérée comme un mécanisme utile offrant des approches et des procédures détaillées pour répondre aux exigences de la directive NIS2.

COMMENT LA DIRECTIVE NIS 2 A-T-IL ÉTÉ MIS EN ŒUVRE DANS LES ÉTATS MEMBRES DE L'UE ?

Le 28 novembre 2024, la Commission européenne a ouvert une procédure d'infraction et a adressé une mise en demeure à 23 États membres (Bulgarie, République tchèque, Danemark, Allemagne, Estonie, Irlande, Grèce, Espagne, France, Chypre, Lettonie, Luxembourg, Hongrie, Malte, Pays-Bas, Autriche, Pologne, Portugal, Roumanie, Slovénie, Slovaquie, Finlande et Suède) pour défaut de transposition complète de la directive NIS2 dans leur droit national. Ces États disposent à présent de deux mois pour réagir et achever la transposition (et en informer la Commission).

COMMENT LE ROYAUME-UNI APPRÉHENDE-T-IL LA RÉGLEMENTATION EN MATIÈRE DE CYBERSÉCURITÉ ?

La directive NIS 2 ne s'applique pas au Royaume-Uni, car elle a été formulée après la fin de la période de transition du Brexit. Toutefois, le Royaume-Uni a modifié ses lois nationales sur la cybersécurité pour actualiser les textes sur les réseaux et les systèmes d'information (qui ont mis en œuvre la directive NIS 1), notamment avec la présentation du projet de loi sur la « *Cybersecurity and Resilience Bill* » (CS&R Bill), attendu de longue date. Bien que le texte du projet de loi n'ait pas encore été publié, les premières indications sur son contenu sont disponibles. L'un des principaux changements sera l'élargissement des secteurs soumis à la réglementation en matière de cybersécurité (à l'instar des changements observés au niveau de l'UE). Le cadre de notification des incidents est un autre domaine clé pour lequel le projet de loi britannique sur la CS&R devrait s'aligner sur les seuils de notification de la directive NIS 2. Dans le cadre de la directive NIS 1, les entités disposent de 72 heures pour signaler un incident de cybersécurité. Toutefois, il semble que, conformément à la directive NIS2, le gouvernement britannique envisage de raccourcir ce délai, en particulier pour les entités critiques. Des normes et des mesures obligatoires en matière de cybersécurité seront également mises en place. Les nouvelles dispositions législatives devraient fixer les bases des mesures de gestion des risques liés à la cybersécurité, de la résilience opérationnelle et des obligations de déclaration dans tous les secteurs concernés.

RELATED CAPABILITIES

- Data Privacy & Security
- Technology Transactions

MEET THE TEAM

Pierre-Emmanuel Froge

Paris

pierreemmanuel.froge@bclplaw.com
+33 (0) 1 44 17 76 21
