Actualité
Cybersécurité

Directive NIS 2

Un changement d'échelle important dans la cybersécurité européenne

L’Union européenne est **de plus en plus touchée** par des cyberattaques dont l’importance ne fait que grandir

La menace cyber reste élevée pour les banques européennes

Cyberattaques à l’hôpital : « A l’hôpital de Versailles, même si la cyberattaque a été “détectée tôt”, il semble que l’impact soit important pour les patients »

Log4j : le ministère belge de la défense victime d’une cyberattaque

La région Guadeloupe victime d’une cyberattaque « de grande ampleur »

Essonne : après l'hôpital de Corbeil, la ville de Brunoy victime d'une cyberattaque de grande ampleur

Cybersécurité : des données volées à Thales publiées sur le darkweb

En réaction, l’armement législatif européen se renforce avec l’entrée en vigueur de la **Directive NIS 2**

L 333/80 FR Journal officiel de l'Union européenne 27.12.2022

DIRECTIVES

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, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2)

(Texte présentant de l'intérêt pour l'EEE)

Cette directive, qui abroge la précédente directive du 16 juillet 2016 (NIS 1), **renforce largement le régime applicable** en matière de cybersécurité

- Entrée en vigueur le **16 janvier 2023**.
- Transposée par les Etats membres de l'Union européenne avant le **17 octobre 2024**.
- Applicable à compter du **18 octobre 2024**, date de l'abrogation de la directive NIS 1.

Les objectifs de la directive NIS 2 sont multiples

1. Réviser le cadre national applicable en matière de cybersécurité
2. Elargir considérablement le champ d'application des règles en matière de cybersécurité
3. Renforcer les obligations de cybersécurité et de notification des organismes concernés

1 La directive NIS 2 **révise le cadre national** applicable en matière de cybersécurité

- Les Etats membres doivent désormais adopter une **stratégie nationale en matière de cybersécurité**.
- Les Etats membres sont dans l'obligation de créer un **cadre national de gestion des crises cyber** ainsi qu'un **plan national de réaction aux crises et incidents de cybersécurité**.
- Chaque Etat membre doit désigner un ou plusieurs centres de réponse aux incidents de sécurité informatique (**CSIRT**).
- Une (ou plusieurs) **autorité compétente** doit être désignée par chaque Etat membre pour assurer le respect de la directive.

1 La directive NIS 2 **révise le cadre national** applicable en matière de cybersécurité

ANSSI | Agence nationale de la sécurité des systèmes d'information

En France, l'ANSSI est toute désignée pour prendre cette place d'autorité compétente, et devrait ainsi voir ses pouvoirs évoluer.

Des pouvoirs de **contrôle** et de **supervision** sont en effet spécifiquement prévus (inspections, audits, scans de sécurité…).

2 Le **champ d'application** de la directive est **considérablement élargi**

Exit les anciens opérateurs de services essentiels et fournisseurs de service numérique…

… place aux **entités essentielles** et aux **entités importantes**.

Cette distinction, essentielle dans le cadre de l'appréciation des obligations de la directive, **est faite selon des critères de taille ou de sensibilité des secteurs d'activité**.

2 Le **champ d'application** de la directive est **considérablement élargi**

Par ailleurs, les deux annexes de la directive prévoient désormais **18 secteurs** (contre 10 auparavant), dont **11 secteurs hautement critiques** (annexe I) et **7 autres secteurs critiques** (annexe II).

Secteurs hautement critiques

1. Energie
2. Transports
3. Secteur bancaire
4. Infrastructures des marchés financiers
5. Santé
6. Eau potable
7. Eaux usées
8. Infrastructures numériques
9. Gestion des services interentreprises
10. Administration publique
11. Espace

Secteurs critiques

1. Services postaux et d'expédition
2. Gestion des déchets
3. Fabrication, production et distribution de produits chimiques
4. Production, transformation et distribution des denrées alimentaires
5. Fabrication
6. Fournisseurs numériques
7. Recherche

2 Le **champ d'application** de la directive est **considérablement élargi**

La **combinaison de la qualification** d'un organisme comme entité essentielle ou entité importante au regard des secteurs d'activité prévus conduit ainsi à soumettre de **très nombreux organismes** à la directive NIS 2.

ANSSI | Agence nationale de la sécurité des systèmes d'information

L'ANSSI estime que cette nomenclature largement élargie devrait concerner plusieurs milliers d'organismes en France, contre quelques centaines pour la directive NIS 1.

La France devra publier, **au plus tard le 17 avril 2025**, une liste des entités essentielles et importantes.

2 Le **champ d'application** de la directive est **considérablement élargi**

Moyennes entreprises

La directive s'applique d'abord aux entités privées ou publiques apparentées à des **moyennes entreprises** au sens du droit de l'Union européenne, c'est-à-dire :

- Qui ont **moins de 250 salariés** ;
- Qui font moins de **50 millions d'euros de C.A annuel** ;
- Et qui ont un **bilan annuel inférieur à 43 millions d'euros**.

2 Le **champ d'application** de la directive est **considérablement élargi**

Petites et micro-entreprises

Les entreprises qui n'atteignent pas les seuils des entreprises moyennes **échappent aux règles** de la directive.

Toutefois, de nombreuses **exceptions** sont prévues :

Pour **certaines activités** (services de confiance, services de noms de domaine…)

Si la perturbation de l'entreprise en question **engendre des impacts importants**

2 Le **champ d'application** de la directive est **considérablement élargi**

Collectivités publiques

Les **administrations centrales de l'Etat** et **certaines administrations régionales** dont la perturbation pourrait avoir des impacts importants sont concernées par la directive.

***Par exception**, les administrations **en dehors du champ du droit de l'Union européenne** (sécurité nationale, défense…) ne sont pas concernées.*

Dans le cadre de la transposition de la directive, les Etats membres pourront également prévoir d'appliquer son contenu aux **administrations locales** et aux **établissements d'enseignement**.

3 Renforcement des obligations de **sécurité** et de **notification**

La directive prévoit l’obligation, modulable selon que l’entité est essentielle ou importante, de mettre en place des **mesures visant à protéger les réseaux et systèmes d’information ainsi que leur environnement physique contre les incidents**.

3 Renforcement des obligations de **sécurité** et de **notification**

Ces obligations reposent sur une appréciation casuistique des menaces. Une **analyse des risques** sera nécessaire pour déterminer les vulnérabilités propres à chaque organisme.

3 Renforcement des obligations de **sécurité** et de **notification**

OBLIGATIONS DE GOUVERNANCE

La directive attache une importance particulière au **facteur humain**, enjeu majeur de la cybersécurité au sein des organismes.

TO DO

- Former les **membres des organes de direction** des entités essentielles et importantes.
- Mettre en œuvre des pratiques de base en matière de **cyberhygiène**.
- Assurer une **formation large à la cybersécurité**.

3 Renforcement des obligations de **sécurité** et de **notification**

OBLIGATIONS DE DOCUMENTATION

Des **procédures** doivent être construites et rédigées afin de **documenter les mesures** prises par l'organisme pour assurer sa sécurité informatique.

TO DO

- Politique de sécurité des systèmes d'information (**PSSI**) et plan de continuité d'activité (**PRA**).
- Politique **d'évaluation de l'efficacité** des mesures.
- Politique RH de **contrôle des accès** et **gestion des actifs**.

3 Renforcement des obligations de **sécurité** et de **notification**

OBLIGATIONS TECHNIQUES

La directive donne également des indications sur les **mesures techniques** qui doivent être mises en place pour garantir la cybersécurité.

TO DO

- Utilisation de la **cryptographie** et du **chiffrement** lorsque c'est pertinent.
- Utilisation de solutions d'authentification à plusieurs facteurs (**MFA**) ou d'authentification continue, de communications vocales, vidéo et textuelles sécurisées et de **systèmes sécurisé de communication d'urgence**

3 Renforcement des obligations de **sécurité** et de **notification**

OBLIGATIONS DE NOTIFICATION

Déjà prévue dans la directive NIS 1, cette obligation est désormais **échelonnée** :

I Une alerte précoce doit être réalisée **dans les 24h** après avoir eu connaissance d'un incident important.

II Une notification d'incident doit ensuite être réalisée, auprès de l'autorité compétente, **dans les 72h**.

III Un rapport final, contenant diverses informations sur l'incident, doit enfin être remis **dans le mois de** la notification.

TO DO

Prévoir et documenter un **plan de gestion des incidents**, en lien avec les autres délais applicables (RGPD, dépôt de plainte pénale…).

3 Renforcement des obligations de **sécurité** et de **notification**

SANCTIONS

La directive NIS 2 prévoit un panel de sanctions en cas de non respect de ses obligation : **avertissements**, **injonctions** diverses de se conformer aux obligations…

Des amendes sont également désormais prévues, **entre 1,4% et 2% du chiffre d'affaires (ou entre 7 et 10 millions d'euros)** des organismes soumis à la directive.

Alors que le menace cyber s’amplifie, un changement de paradigme s’opère ainsi au sein de l’Union européenne en matière de cybersécurité.

De nombreux secteurs et organismes, qui n’étaient jusqu’alors pas concernés par ces règles, vont devoir s’armer pour respecter les nouvelles mesures de la directive NIS 2 qui, couplées au RGPD et aux dispositions en matière de cybercriminalité, exigent une vigilance encore plus accrue.

Les experts Oyat

Marie-Hélène TONNELLIER

Avocat associé

Digital et innovation

Clyde COUTELLIER

Avocat

Digital et innovation

icon:flaticon.com

OYAT

www.oyat.law