# Les midis de l’entreprise

# Directive NIS2 : Anticiper les nouvelles obligations en matière de cybersécurité

**Séminaire**

**Arendt House**

**28 octobre 2025**

# Directive NIS2 : Anticiper les nouvelles obligations en matière de cybersécurité

Vos contacts / orateurs


**Astrid Wagner**

Partner
IP, Communication & Technology

**Sophie Calmes**

Senior Associate
IP, Commercial & Technology

**Julien Pétré**

Senior Associate
IP, Commercial & Technology

**Tristan Vaisière**

Associate
IP, Commercial & Technology


# Table des matières

# 1. Introduction - Pourquoi une directive NIS2?

# Chronologie

NIS 1 | NIS 2 | DORA

**18 mai 2018:** Entrée en vigueur de NIS 1

**Loi du 29 mai 2019:** Transposition nationale de NIS 1

**16 janvier 2023 :** Entrée en vigueur NIS 2

**16 Janvier 2023 :** Entrée en vigueur DORA

**13 mars 2024 :** Dépôt du projet de loi n°8364

**5 janvier 2024 :** Circulaire CSSF 42/874 sur le cadre de notification des incidents liés aux TIC

**16 Janvier 2025 :** Applicabilité DORA

?

Entrée en vigueur de la loi nationale transposant NIS2

# Pourquoi une directive NIS2?


NIS1

Niveau insuffisant de résilience numérique

Mauvaise compréhension commune des principales menaces et défis entre les États membres

**Impossibilité d'harmoniser les cadres légaux nationaux de cybersécurité sous NIS1**

Incohérence entre les États membres et les secteurs

Absence de réponse conjointe aux crises

NIS2

**Modifications apportées par NIS2**

- Distinction entre **entités essentielles** et **importantes**
- Plus grand nombre **d'acteurs et de secteurs visés**
- Obligations renforcées de **gestion des risques cyber** avec une liste de mesures de sécurité minimales
- Règles plus précises pour le **signalement des incidents**, incluant les délais et le contenu des rapports
- Prise en compte des risques liés à la **chaîne d'approvisionnement**
- Mise en place d'un **régime de supervision accru**
- Harmonisation des **sanctions**

# 2. Vue globale sur le projet de loi n°8364 et les autorités compétentes désignées

# Vue globale sur le projet de loi n°8364

Chambre des Députés
GRAND-DUCHÉ DE LUXEMBOURG

**Projet de loi n°8307** sur la résilience des entités critiques transposant la directive CER – **résilience physique des infrastructures critiques**

Le **projet de loi n°8364** transposant la directive (UE) 2022/2555 concernant des mesures destinées à assurer un niveau élevé commun de **cybersécurité** dans l'ensemble de l'Union (« **NIS2** ») et abrogeant la directive NIS1, a été déposé le 13 mars 2024.

Le projet de loi est actuellement **toujours en cours de discussion**.

Le projet de loi, à son état actuel, suit une **transposition fidèle** des dispositions de NIS2, sans faire du *gold-plating*.

Le projet de loi détermine notamment quelles sont les **autorités compétentes** en matière de cybersécurité au niveau national et quels sont **leurs pouvoirs respectifs**.

Surveiller la publication de la loi!

# Autorités compétentes désignées sous le projet de loi n°8364

| Autorités compétentes chargées de la cybersécurité | Centre de réponse aux incidents de sécurité informatique (**CSIRT**) | Point de contact national unique | Autorité de gestion des crises cyber | Stratégie nationale en matière de cybersécurité |
|---|---|---|---|---|
| Institut Luxembourgeois de la Régulation (**ILR**) / Commission de surveillance du secteur financier (**CSSF**) | Haut-Commissariat à la protection nationale (**GOVCERT.LU**) / *Computer Incident Response Center Luxembourg* (**CIRCL**) | Haut-Commissariat à la protection nationale (**HCPN**) | | |
| ❖ Supervision et pouvoirs d'exécution (voir partie 5 de la présentation)<br>- **CSSF**: entités du secteur bancaire et financier, infrastructures numériques et secteur de la gestion des services TIC sous la surveillance de la CSSF<br>- **ILR:** compétence résiduelle | ❖ Gestion des incidents de cybersécurité<br>❖ Soutien technique aux entités<br>❖ CIRCL: coordinateur de la divulgation de vulnérabilités<br>- **GOVCERT.LU:** administrations, secteur public et entités critiques<br>- **CIRCL:** compétence résiduelle | ❖ Fonctions de liaison afin d'assurer la coopération transfrontalière avec les autres autorités UE compétentes et l'ENISA, ainsi que d'assurer la coopération intersectorielle | ❖ Gestion des incidents de cybersécurité majeurs et des crises et représentation du Luxembourg au sein du réseau européen EU-CyCLONe | ❖ Adoption de la stratégie nationale en matière de cybersécurité |

Le secret professionnel ne fait **pas obstacle** à l'échange d'informations et coopérations entre autorités

# 3. Champ d’application

# Compétence et secteurs visés

Secteurs ajoutés par la directive NIS 2

**Principe:** établissement au Grand-duché de Luxembourg, sauf exceptions

## Annexe I : Secteurs hautement critiques

**Énergie**
- Électricité
- Gaz
- Pétrole
- Hydrogène
- Réseaux de chaleur et de froid

**Transports**
- Aériens
- Ferroviaires
- Par eau
- Routiers

**Santé**
- Prestataires de soins de santés
- Fabricants pharmaceutiques

**Espace**

**Eau potable**

**Eaux usées**

**Administration publique**

**Infrastructure numérique**

**Banques**

**Infrastructures des marchés financiers**

**Gestion des services TIC (interentreprises)**

## Annexe II : Autres secteurs critiques

**Services postaux et d'expédition**

**Gestion des déchets**

**Fournisseurs numériques**
- Place de marché en ligne
- Moteurs de recherche en ligne
- Plateformes de réseaux sociaux

**Produits chimiques**
- Fabrication, production et distribution

**Denrées alimentaires**
- Production, transformation et distribution

**Recherche**

**Fabrication**
- Fabrication de dispositifs médicaux et dispositifs médicaux de diagnostic in vitro
- Fabrication de produits informatiques, électroniques et optiques
- Fabrication d'équipements électriques
- Fabrication de machines et équipement n.c.a.
- Construction de véhicule automobile, remorques et semi-remorques
- Fabrication d'autres matériels de transport

# Entités in-scope

## Application selon la taille de l'entité

### Entreprises moyennes ou grandes visées à l'annexe I ou II

Effectif: ≥ 50 personnes
+
CA annuel: ≥ 10 millions d'euros
OU
Bilan total: ≥ 2 millions d'euros

Effectif: ≥ 250 personnes
+
CA annuel: ≥ 50 millions d'euros
OU
Bilan total: ≥ 10 millions d'euros

OU

## Application peu importe la taille de l'entité

### N'importe quelle entité d'un type visé à l'annexe I ou II, qui :

I. Services fournis par:

- un fournisseur de réseaux de communications électroniques publics ou de services de communications électroniques accessibles au public ;
- un prestataire de services de confiance ;
- un registre des noms de domaine de premier niveau et des fournisseurs de services de système de noms de domaine ;

II. Une entité de l'administration publique telle que définie à l'article 2, point 34° de NIS2

III. Unique prestataire d'un service essentiel au maintien d'activités sociétales ou économiques critiques

IV. Entité dont la perturbation du service fourni pourrait avoir un impact important sur la sécurité publique, la sûreté publique ou la santé publique

V. Entité dont la perturbation du service fourni pourrait induire un risque systémique important, surtout en cas d'impact transfrontière

VI. Entité 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 au Luxembourg

OU

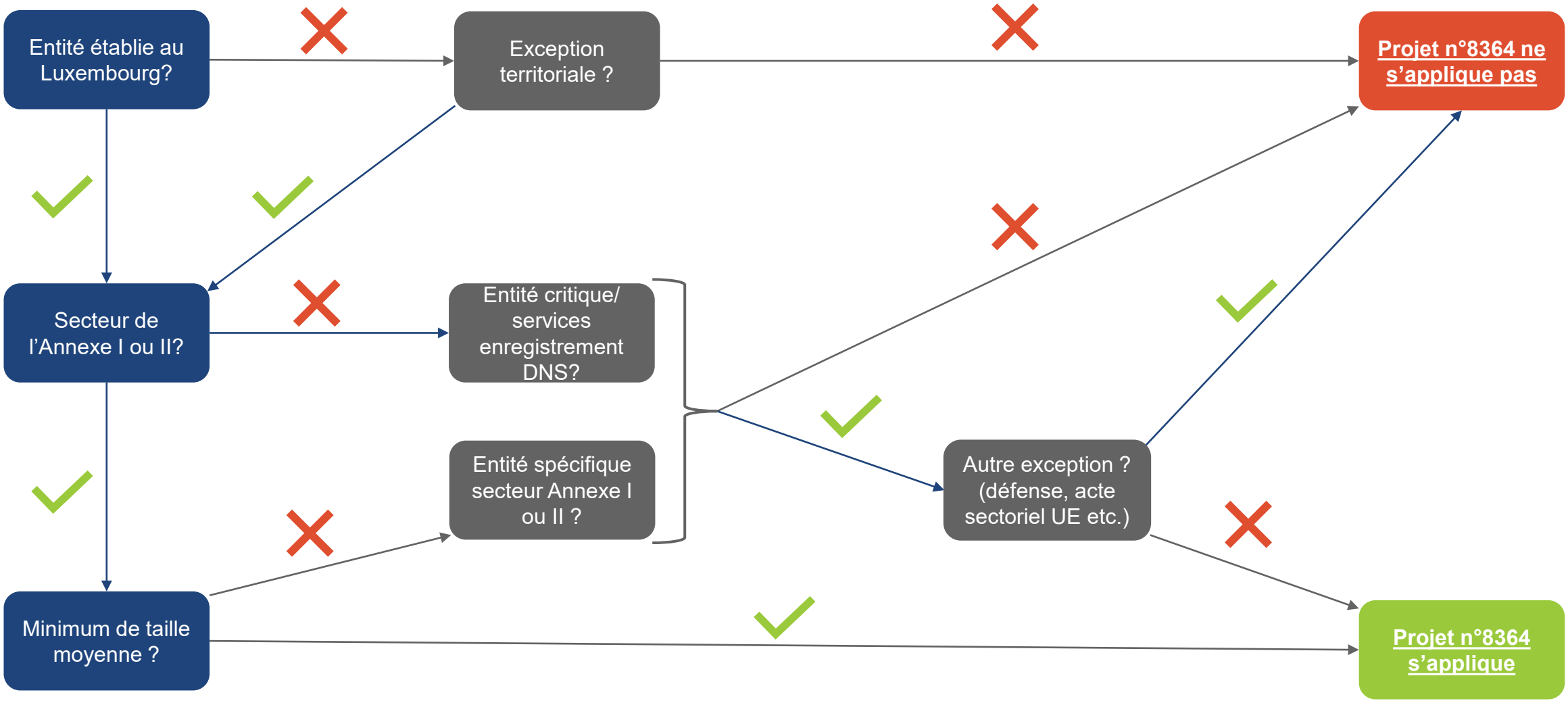
Entités critiques d'après le projet de loi n°8307

Entités fournissant des services d'enregistrement de noms de domaine

## Exceptions

- Entités de l'administration publique qui exercent leurs activités dans les domaines de la défense et de la sécurité nationale
- Systèmes de communication et d'information où sont conservées ou traitées des pièces classifiées
- Entités soumises à des mesures équivalentes par des actes juridiques sectoriels de l'UE (ex. DORA)
- Entités exclues du champ d'application de DORA conformément à l'article 2 §4 dudit règlement

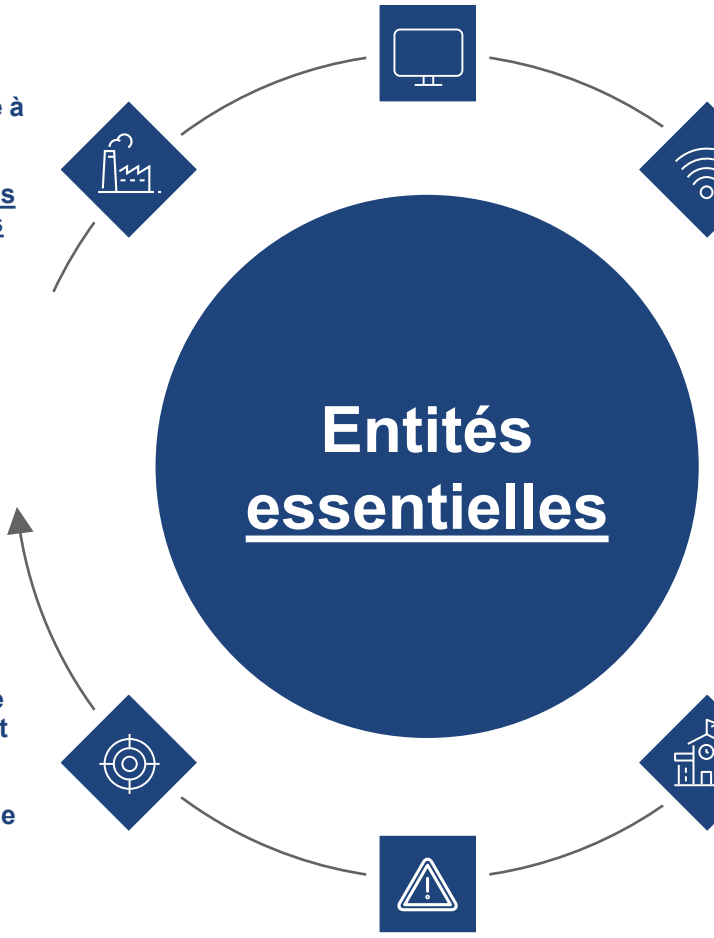
# Arborescence



# 4. Vers de nouvelles obligations pour renforcer la cybersécurité et la résilience opérationnelle

# Différence entité essentielle vs. importante

**Entités importantes:** toute autre entités d'un type visé à l'annexe I ou II qui n'est pas une entité essentielle




- Prestataires de services de confiance qualifiés
- registres de noms de domaine de premier niveau
- fournisseurs de services DNS

→ quelle que soit leur taille

- fournisseurs de réseaux publics de communications électroniques publics
- Fournisseur de services de communications électroniques accessibles au public

→ qui constituent des moyennes entreprises

Entités d'un type visé à l'annexe I

→ qui constituent des grandes entreprises

Entités identifiées par les autorités compétentes comme opérateurs de services essentiels sous NIS 1

Entités de l'administration publique

Entités critiques (projet de loi n° 8307)

Toute autre entité d'un type visé à l'annexe I ou II qui est identifiée par le biais d'une décision administrative individuelle de ILR/CSSF en tant qu'entité essentielle

# Obligations

Attention aux entités soumises à des actes juridiques sectoriels de l'UE (par exemple DORA)

**Auto-enregistrement**
(sous 2 mois)

**Mesures techniques, opérationnelles et organisationnelles**

**Mesures de suivi**
(Responsabilité organe de direction si non-respect)

**Notifications**
(incidents et cybermenaces)

**Obligations propres aux infrastructures numériques**
(noms de domaines)

À titre volontaire: partage d'informations entre entités

**Obligations exclusivement imposées aux entités essentielles**

- **Notification des mesures** techniques, opérationnelles et organisationnelles à ILR/CSSF (modalités à définir)
- **Régime de supervision** étendu
- **Mesures d'exécution** plus contraignantes

# 5. Sanctions et pouvoirs des autorités compétentes

# Sanctions et pouvoirs des autorités compétentes

Articulation avec RGPD en cas de violation de données à caractère personnel

| | Entités essentielles | Entités importantes |
|---|---|---|
| SUPERVISION | Inspections sur place et contrôles à distance, audits réguliers et ciblés, scans de sécurité, demandes d'informations nécessaires à l'évaluation des mesures et demandes d'accès à des données, documents et à toute autre information, demandes de preuves de la mise en œuvre de politique cyber<br>+ pour entités essentielles : audits ad hoc | |
| POUVOIRS | Avertissements, instructions contraignantes ou injonction, mettre un terme à un comportement, garantir la conformité de leurs mesures de gestion des risques, informer les personnes à l'égard desquelles les services sont fournis ou qui sont susceptibles d'être affectées, recommandations, ordre de rendre public les aspects de violations, amende administrative<br>+ pour entités essentielles :<br>• désignation pour une période déterminée d'un responsable du contrôle ;<br>• suspension temporaire des services ou activités ;<br>• interdiction temporaire d'exercer des responsabilités dirigeantes de l'entité<br>Prise en comptes des circonstances : gravité de la violation, durée, violation antérieure, dommages, délibérément/par négligence, mesures de prévention, application de codes de conduite, degré de coopération | |
| | **Toute personne physique responsable ou agissant en tant que représentant légal** peut être tenue responsable des manquements à son devoir de veiller au respect de la loi | |
| € | Violations relatives aux mesures ou incidents importants: Maximum **10M € ou 2% du CA mondial** | Violations relatives aux mesures ou incidents importants: Maximum **7M € ou 1,4% du CA mondial** |
| | Autres violations : avertissement, blâme, amende administrative ne pouvant excéder **250.000 €** | |

# 6. Comment se préparer?

# Points d’action

01 **Vérifier l’applicabilité de NIS2**

02 **Procéder à une analyse des lacunes**

03 **Gestion des vulnérabilités**

- Mise en place des mesures de cybersécurité et de gestion des risques nécessaires
- Revue et mise à jour éventuelle des politiques internes, des prestataires externes et des contrats pertinents

04 **Approbation des actions et des mesures de gestion des risques et de cybersécurité par l’organe de direction**

05 **Notification auprès de l’autorité compétente dans le délai de 2 mois après entrée en vigueur de la loi**

06 **Veille réglementaire**

# Q & A

## Vos contacts / orateurs

**Astrid Wagner**

Partner
IP, Commercial & Technology
astrid.wagner@arendt.com
+352 40 78 78 698

**Sophie Calmes**

Senior Associate
IP, Commercial & Technology
sophie.calmes@arendt.com
+352 40 78 78 267

**Julien Pétré**

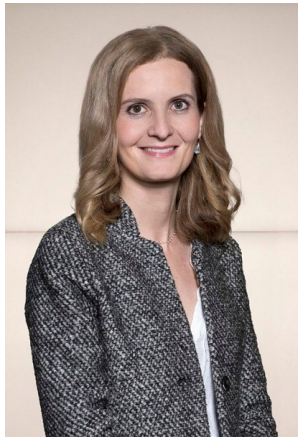
Senior Associate
IP, Commercial & Technology
julien.petre@arendt.com
+352 40 78 78 2139

**Tristan Vaisière**

Associate
IP, Commercial & Technology
tristan.vaisiere@arendt.com
+352 40 78 78 2107

**Bénédicte d'Allard**

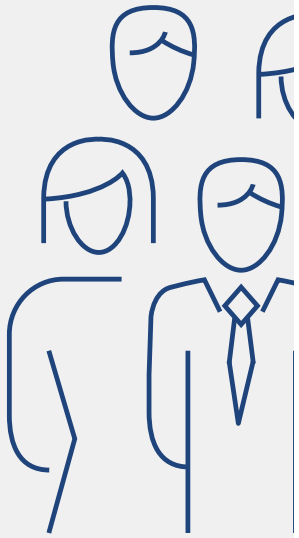
Director
Regulatory & Consulting
benedicte.dallard@arendt.com
+352 26 09 10 77 31



**Delphine Garnier**

Senior Manager
Regulatory & Consulting
delphine.garnier@arendt.com
+352 40 78 78 7796

# Prochain Midi de l'Entreprise



**Save the date**

**-**

**2 ou 4 décembre à 12h30**

**-**

**sujet tbc**


arendt