REGUVARA · GUIDE PRATIQUE GRATUIT

# NIS2 : préparer les circuits de notification et les preuves

Un premier outil pratique pour la direction, l'informatique/la sécurité, le juridique et la conformité. Repères sur le périmètre, les principaux délais de notification et cinq premières actions.

**Objectif : faire apparaître rapidement les bonnes questions. Ce guide ne détermine pas de manière contraignante si une entité juridique donnée relève de NIS2.**

## 1. Évaluer d'abord le périmètre

• Relier l'activité, le service et l'entité juridique aux secteurs des annexes I et II de la directive NIS2. Le seul nom du secteur ne suffit pas à établir l'inclusion.

• Vérifier la taille, les liens de groupe, le type de service, les désignations critiques, les exemptions et les règles de l'État membre concerné. Certaines entités ou certains services peuvent être couverts indépendamment du seuil de taille habituel.

• Pour chaque entité potentiellement concernée, consigner les pays, sites, services, autorités compétentes, obligations d'enregistrement et de contact, ainsi que le raisonnement.

## 2. Étapes de notification prévues au niveau de l'UE pour un incident important

| Étape | Base de l'UE au titre de l'article 23 | Question de préparation |
|---|---|---|
| **Alerte précoce** | Sans retard injustifié et au plus tard dans les 24 heures suivant la prise de connaissance de l'incident important. | Qui déclenche le délai, prend la décision et identifie l'autorité compétente ? |
| **Notification de l'incident** | Sans retard injustifié et au plus tard dans les 72 heures suivant la prise de connaissance ; première évaluation de la gravité et de l'impact et indicateurs, s'ils sont disponibles. | Comment recueillir en parallèle les faits, les horodatages et les éléments inconnus ? |
| **Rapport intermédiaire** | Si le CSIRT ou l'autorité compétente le demande. | Qui suit les évolutions et répond aux demandes de suivi ? |
| **Rapport final** | En principe dans le mois suivant la notification de l'incident. Si l'incident est toujours en cours, un rapport d'avancement est dû à cette échéance et le rapport final dans le mois suivant son traitement. | Qui confirme le délai national et le contenu requis ? |

Ces délais concernent les incidents importants et le moment où l'entité en prend connaissance. Les prestataires de services de confiance sont soumis à une règle particulière de notification de l'incident dans les 24 heures. Vérifier la transposition nationale, les règles sectorielles et les autres actes de l'UE applicables.

FEUILLE DE TRAVAIL

# Du texte juridique au premier processus opérationnel

NIS2 exige des mesures techniques, opérationnelles et organisationnelles proportionnées et fondées sur les risques. Cette synthèse aide à réunir les premiers responsables.

## 3. Thèmes visés par l'article 21

Les mesures protègent les réseaux et les systèmes d'information utilisés pour les services, y compris leur environnement physique. Leur portée et leur conception dépendent des risques et de la proportionnalité.

| Domaine | Exemple de question de travail |
|---|---|
| **Analyse des risques et sécurité des systèmes** | Quels services, systèmes, menaces et dépendances sont concernés ? Qui actualise l'évaluation ? |
| **Gestion des incidents** | Comment organiser la détection, la classification, le confinement, l'escalade, la préservation des preuves et le retour d'expérience ? |
| **Continuité et crise** | Les sauvegardes, la reprise, les rôles de crise et les objectifs de rétablissement sont-ils documentés et testés ? |
| **Chaîne d'approvisionnement** | Les fournisseurs directs, les dépendances critiques et les informations de sécurité sont-ils recensés ? |
| **Acquisition et développement sécurisés** | Comment sélectionner et maintenir les systèmes en sécurité et traiter ou divulguer les vulnérabilités ? |
| **Vérification de l'efficacité** | Comment l'organisation détermine-t-elle si les mesures de sécurité sont efficaces ? |
| **Hygiène informatique et formation** | Quelles pratiques de base et formations sont prévues et documentées ? |
| **Cryptographie** | Quelles règles s'appliquent à la cryptographie et, le cas échéant, au chiffrement ? |
| **Personnel, accès et actifs** | Comment contrôler les autorisations, les changements de personnel, les actifs et les accès ? |
| **Authentification et communication** | Où la MFA ou l'authentification continue, les communications sécurisées et les canaux d'urgence sont-ils adaptés ? |

## 4. Cinq premières étapes utiles

- Désigner une personne chargée de coordonner les questions de périmètre et les points en suspens.
- Recenser les services, entités juridiques, systèmes et fournisseurs directs critiques.
- Désigner la direction, le responsable des incidents, les équipes informatique/sécurité, juridique/conformité et communication, avec des suppléants.
- Vérifier l'autorité nationale compétente, le CSIRT, l'enregistrement, le canal de notification et les obligations sectorielles éventuelles.
- Réaliser un exercice court : détecter un incident, consigner le moment de prise de connaissance, déclencher l'escalade et réunir les faits.

**NIS2 ne s'applique pas automatiquement à toutes les entreprises. Le périmètre dépend notamment de l'activité, de la taille, de l'entité juridique, de l'État membre, des cas particuliers et des règles sectorielles.**

### SOURCES ET ÉTAT JURIDIQUE

Source principale : directive (UE) 2022/2555, notamment articles 2-4, 20, 21 et 23 et annexes I-II. La proposition COM(2026) 13 final n'est pas une loi en vigueur. Le 8 octobre 2026, la procédure 2026/0012(COD) du Parlement européen était en attente d'une décision de commission ; un projet de rapport de commission avait été publié le 24 septembre 2026. La transposition nationale et les règles sectorielles n'ont pas été examinées pays par pays.
NIS2 Directive (EUR-Lex) · European Commission FAQ · National transposition · EP procedure 2026/0012(COD) · COM(2026) 13 proposal