UNION EUROPÉENNE

DIRECTIVE NIS2

(Directive UE 2022/2555)

Mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union

Résumé en français pour les RSSI et les responsables conformité

Référence du document

Champ	Valeur
Nom officiel	Directive (UE) 2022/2555
Date d'adoption	14 décembre 2022
Date de publication	27 décembre 2022 (JO L 333/80)
Entrée en vigueur	16 janvier 2023
Délai de transposition nationale	17 octobre 2024
Instrument abrogé	Directive (UE) 2016/1148 (SRI 1)

> Ce document est un résumé non officiel de la directive NIS2 de l'UE du 14 décembre 2022 ; il ne constitue pas une traduction faisant autorité. Pour une interprétation contraignante, consulter le texte officiel au JO L 333/80, 27.12.2022.

Table des matières

1. Résumé exécutif

La **directive NIS2** (Directive UE 2022/2555), adoptée par le Parlement européen et le Conseil le 14 décembre 2022, est la directive de référence de l'UE en matière de cybersécurité. Elle abroge et remplace la précédente directive SRI 1 (2016/1148) avec effet au 18 octobre 2024.

Les examens ont conclu que si la SRI 1 avait contribué à relever le niveau de cyberrésilience dans l'Union, elle s'est avérée insuffisante pour faire face aux cybermenaces actuelles et futures. La NIS2 élargit considérablement le champ d'application, introduit des critères uniformes, renforce les obligations de gestion des risques et de notification des incidents, et prévoit des dispositions d'exécution plus dissuasives.

Les cinq piliers de la directive

1. **Champ d'application élargi** : davantage de secteurs et d'entreprises soumis à la réglementation.
2. **Gestion des risques renforcée** : 10 mesures techniques et organisationnelles minimales rendues obligatoires au titre de l'article 21.
3. **Notification d'incidents rapide et progressive** : alerte précoce sous 24 heures, notification d'incident sous 72 heures, rapport final sous 1 mois.
4. **Responsabilité de l'organe de direction** : la direction générale peut être tenue personnellement responsable.
5. **Sanctions dissuasives** : amendes administratives pouvant atteindre 2 % du chiffre d'affaires annuel mondial ou 10 millions d'EUR.

2. Objectif et base juridique

La base juridique de la directive est **l'article 114 du traité sur le fonctionnement de l'Union européenne (TFUE)**, qui autorise les mesures de rapprochement des règles nationales en vue d'établir et d'assurer le fonctionnement du marché intérieur.

Les principaux objectifs de la directive sont :

- Éliminer les divergences importantes entre les États membres et établir des règles minimales communes en matière de cybersécurité ;
- Établir des mécanismes efficaces de coopération transfrontière et de partage d'informations ;
- Mettre à jour la liste des secteurs et activités soumis aux obligations de cybersécurité pour refléter le paysage actuel des menaces ;
- Fournir des mécanismes d'exécution et de recours assurant la mise en oeuvre effective des obligations ;
- Renforcer les capacités de cyberrésilience des opérateurs d'infrastructures critiques et des fournisseurs de services numériques.

La directive s'applique sans préjudice et en conformité avec le droit de l'UE relatif à la protection des données à caractère personnel (RGPD, Règlement UE 2016/679) et à la protection de la vie privée dans les communications électroniques (Directive 2002/58/CE).

3. De NIS1 à NIS2 : pourquoi un nouveau règlement ?

La SRI 1, entrée en vigueur en 2016, était la première réglementation horizontale de l'UE en matière de cybersécurité. Le processus d'examen a révélé de sérieuses divergences de mise en oeuvre entre les États membres, la délimitation du champ d'application ayant été largement laissée à l'appréciation de chaque État membre, fragmentant ainsi le marché intérieur.

Lacunes identifiées de la SRI 1

Domaine concerné	Situation SRI 1	Solution NIS2
Délimitation du champ d'application	Laissée à l'appréciation des États membres ; variations significatives dans la pratique.	Règle uniforme de « plafond de taille » dans toute l'UE (entreprises moyennes et grandes).
Liste des secteurs	Nombre limité de secteurs ; une part significative de l'économie numérique exclue.	Couverture sectorielle beaucoup plus large ; infrastructures numériques, administration publique, espace, etc. inclus.
Notification des incidents	Procédure en une seule étape ; délais et contenu variables entre États membres.	Notification en plusieurs phases : alerte précoce 24h + notification 72h + rapport final 1 mois.
Gestion des risques	Formulation générale ; mesures minimales spécifiques peu claires.	L'article 21 liste 10 catégories de mesures minimales obligatoires.
Sanctions	Appliquées à des niveaux très différents selon les États membres.	Amendes maximales harmonisées au niveau de l'UE (10 M EUR / 2 % du chiffre d'affaires).
Responsabilité de la direction	Non clairement définie.	Organe de direction personnellement responsable de la conformité ; formation obligatoire.

La NIS2 n'est pas une mise à jour de la SRI 1 ; c'est un remplacement conçu pour produire un **cadre de cybersécurité unique, harmonisé et exécutoire** dans l'ensemble de l'Union.

4. Champ d'application et exclusions

La directive couvre principalement les entités opérant dans les secteurs de **l'Annexe I (haute criticité)** ou de **l'Annexe II (autres secteurs critiques)** au sein de l'UE et répondant à la définition d'au moins une entreprise de taille moyenne. En vertu de l'article 2 de l'annexe de la recommandation 2003/361/CE de la Commission, une entreprise de taille moyenne est une entreprise employant moins de 250 personnes et dont le chiffre d'affaires annuel ne dépasse pas 50 millions d'EUR (ou dont le total du bilan ne dépasse pas 43 millions d'EUR). La NIS2 concerne les entités atteignant ou dépassant ce seuil : le plancher pratique pour les entités concernées est de 50 salariés ou 10 millions d'EUR de chiffre d'affaires (la limite supérieure de la « petite entreprise » au sens de la même recommandation).

Entités concernées quelle que soit leur taille

- Fournisseurs de réseaux publics de communications électroniques et fournisseurs de services de communications électroniques accessibles au public ;
- Prestataires de services de confiance (au titre du règlement eIDAS, UE 910/2014) ;
- Registres de noms de domaine de premier niveau (TLD) et fournisseurs de services DNS ;
- Entités étant le seul fournisseur d'un service dans un État membre ou dont l'interruption pourrait avoir un impact significatif sur la sécurité publique, la santé ou la sûreté ;
- Toutes les entités de l'administration publique centrale (définies au niveau national par les États membres).

Domaines exclus du champ d'application

Les entités publiques dont les activités sont principalement exercées dans les domaines de la **sécurité nationale, de la sécurité publique, de la défense ou de l'application de la loi** (prévention, enquête, détection et poursuite des infractions pénales) sont exclues du champ d'application de la directive. Les représentations diplomatiques et consulaires des États membres dans des pays tiers ainsi que les services de confiance utilisés dans des systèmes fermés sont également exclus.

5. Définitions clés

Certains concepts fondamentaux doivent être clairement compris pour une interprétation correcte de la directive.

Terme	Définition
Réseau et système d'information	Réseaux de communications électroniques, tout dispositif ou groupe de dispositifs traitant des données numériques, et toutes les données numériques traitées pour l'exploitation, l'utilisation, la protection et la maintenance de ces réseaux et systèmes.
Cybersécurité	Toutes les activités nécessaires pour protéger les réseaux et les systèmes d'information, leurs utilisateurs et les autres personnes contre les cybermenaces.
Incident	Événement compromettant la disponibilité, l'authenticité, l'intégrité ou la confidentialité de données stockées, transmises ou traitées, ou des services offerts par des réseaux et systèmes d'information ou accessibles via ceux-ci.
Incident important	Incident ayant causé ou étant susceptible de causer une perturbation opérationnelle grave des services ou des pertes financières pour l'entité concernée, ou ayant affecté ou étant susceptible d'affecter d'autres personnes physiques ou morales en causant des dommages matériels, corporels ou moraux considérables.
Cybermenace	Toute circonstance, événement ou action potentiel susceptible de nuire, de perturber ou d'avoir un impact négatif sur les réseaux et systèmes d'information.
Cybermenace significative	Cybermenace qui, en raison de ses caractéristiques techniques, peut être considérée comme ayant le potentiel d'avoir un impact grave sur les réseaux et systèmes d'information d'une entité, ses utilisateurs ou d'autres personnes, en causant des dommages matériels, corporels ou moraux considérables.
Vulnérabilité	Faiblesse, susceptibilité ou faille de produits ou services TIC pouvant être exploitée par une cybermenace.
Incident évité	Événement qui aurait pu compromettre la disponibilité, l'authenticité, l'intégrité ou la confidentialité de données ou de services, mais qui a été évité avec succès.
CSIRT	Centre de réponse aux incidents de sécurité informatique (Computer Security Incident Response Team), équipe technique responsable du traitement des incidents.
ENISA	Agence de l'Union européenne pour la cybersécurité, joue un rôle central de conseil et de soutien dans la mise en oeuvre de la directive.

6. Catégories d'entités : entités essentielles et entités importantes

La directive divise toutes les entités concernées en deux grandes catégories. Cette distinction détermine la manière dont les obligations et le régime de supervision/exécution s'appliquent.

Critère	Entités essentielles	Entités importantes
Secteur	Annexe I, secteurs de haute criticité	Annexe II, autres secteurs critiques (et entités de taille moyenne relevant de l'Annexe I)
Taille	Grandes entreprises (250 salariés ou plus, ou chiffre d'affaires supérieur à 50 millions d'EUR)	Entreprises de taille moyenne (50 à 249 salariés)
Régime de supervision	Supervision ex ante et ex post	Supervision ex post uniquement, sur preuve ou plainte
Amende administrative maximale	10 millions d'EUR ou 2 % du chiffre d'affaires annuel mondial (le montant le plus élevé s'applique)	7 millions d'EUR ou 1,4 % du chiffre d'affaires annuel mondial (le montant le plus élevé s'applique)
Sanctions à l'encontre de la direction	Interdiction temporaire d'exercice des fonctions dirigeantes possible	Interdiction temporaire d'exercice des fonctions dirigeantes non applicable

> **Note importante :** Si une entité a été identifiée comme « opérateur de services essentiels » au titre de la SRI 1, l'État membre peut décider que cette entité est directement une entité essentielle au titre de la NIS2. Par ailleurs, toutes les entités identifiées comme « entités critiques » au titre de la directive 2022/2557 (CER) sont automatiquement considérées comme des entités essentielles au titre de la NIS2.

7. Secteurs concernés (Annexe I et Annexe II)

Annexe I, secteurs de haute criticité

Les grandes entreprises de ces secteurs sont des entités essentielles ; les entreprises de taille moyenne sont des entités importantes.

Secteur	Sous-secteur / Type d'entité
Énergie	Électricité (production, transport, distribution, fourniture) ; Chaleur ou froid urbain ; Pétrole (oléoducs, production, stockage, transport) ; Gaz naturel ; Production, stockage et transport d'hydrogène
Transports	Aérien (transporteurs aériens, aéroports, gestion du trafic aérien) ; Ferroviaire (gestionnaires d'infrastructure, opérateurs ferroviaires) ; Maritime et fluvial (opérateurs maritime et voies navigables intérieures) ; Routier (systèmes de transport intelligents, opérateurs routiers)
Secteur bancaire	Établissements de crédit au sens du règlement (UE) 575/2013
Infrastructures des marchés financiers	Plates-formes de négociation (bourses) et contreparties centrales (CCP)
Santé	Prestataires de soins de santé ; Laboratoires de référence de l'UE ; Entités conduisant des activités de R&D sur des médicaments ; Fabricants de produits pharmaceutiques ; Fabricants de dispositifs médicaux considérés comme critiques lors d'urgences de santé publique (au titre du règlement (UE) 2022/123)
Eau potable	Fournisseurs et distributeurs d'eau destinée à la consommation humaine
Eaux usées	Entités assurant la collecte, l'évacuation ou le traitement des eaux urbaines résiduaires, des eaux usées domestiques ou industrielles
Infrastructures numériques	Points d'échange Internet (IXP) ; Fournisseurs de services DNS (à l'exclusion du DNS racine) ; Registres de noms de domaine de premier niveau ; Fournisseurs de services d'informatique en nuage ; Fournisseurs de services de centres de données ; Fournisseurs de réseaux de diffusion de contenu (CDN) ; Prestataires de services de confiance ; Fournisseurs de réseaux publics de communications électroniques
Gestion des services TIC (B2B)	Fournisseurs de services gérés (MSP) ; Fournisseurs de services de sécurité gérés (MSSP)
Administration publique	Entités de l'administration centrale et régionale telles que définies par les États membres
Espace	Opérateurs d'infrastructures terrestres exploitées par l'État membre ou le secteur privé

Annexe II, autres secteurs critiques

Secteur	Sous-secteur / Type d'entité
Services postaux et d'expédition	Prestataires de services postaux (y compris les services de messagerie)
Gestion des déchets	Entités fournissant des services de collecte, de recyclage et d'élimination des déchets
Fabrication, production et distribution de produits chimiques	Entités engagées dans la production, la transformation et la distribution de produits chimiques
Production, transformation et distribution de denrées alimentaires	Grandes entreprises engagées dans la production, la transformation et la distribution en gros de denrées alimentaires
Fabrication	Dispositifs médicaux / dispositifs médicaux de diagnostic in vitro ; Produits informatiques, électroniques et optiques ; Équipements électriques ; Machines et équipements n.c.a. ; Véhicules automobiles, remorques et semi-remorques ; Fabrication d'autres matériels de transport
Fournisseurs numériques	Places de marché en ligne ; Moteurs de recherche en ligne ; Plateformes de services de réseaux sociaux
Recherche	Organismes de recherche menant des activités de recherche à des fins commerciales

8. Obligations des États membres

La directive impose des obligations aux États membres ainsi qu'aux entités du secteur privé. Chaque État membre doit prendre les mesures suivantes :

Stratégie nationale de cybersécurité. Adopter une stratégie nationale de cybersécurité assortie d'objectifs stratégiques clairs, de priorités et d'un cadre de gouvernance. La stratégie aborde des sujets tels que la sécurité de la chaîne d'approvisionnement, les rançongiciels, le soutien aux PME, les logiciels libres et la cyberdéfense active.

Autorité(s) compétente(s). Désigner ou établir une ou plusieurs autorités compétentes pour assurer la mise en oeuvre et la supervision de la directive.

Point de contact unique (PCU). Désigner un point de contact unique chargé de la coordination transfrontière au niveau de l'UE.

CSIRT. Établir ou désigner un ou plusieurs CSIRT responsables du traitement des incidents, de la surveillance proactive, de la divulgation coordonnée des vulnérabilités, et de la coopération nationale et internationale.

Liste des entités. Tenir, mettre régulièrement à jour et transmettre à la Commission une liste des entités essentielles et importantes ainsi que des entités fournissant des services d'enregistrement de noms de domaine.

Divulgation coordonnée des vulnérabilités. Désigner un CSIRT comme coordinateur ; promouvoir la sécurité juridique pour les chercheurs en vulnérabilités.

Assistance mutuelle. Fournir une assistance mutuelle aux autres États membres dans le cadre de la supervision et de l'exécution transfrontières.

Soutien aux PME. Fournir des orientations, des outils gratuits et un point de contact national ou régional pour les petites et microentreprises.

9. Mesures de gestion des risques en matière de cybersécurité (Article 21)

La disposition technique la plus importante de la directive est l'article 21. Elle énumère les mesures techniques, opérationnelles et organisationnelles minimales que les entités essentielles et importantes doivent mettre en oeuvre. L'approche est fondée sur une **perspective « tous risques »** ; non seulement les cyberattaques, mais aussi les menaces telles que les dommages physiques, les catastrophes naturelles, les défaillances d'équipements et les erreurs humaines sont couvertes.

Article 21, dix mesures minimales

N°	Mesure	Description
1	Politiques relatives à l'analyse des risques et à la sécurité des systèmes d'information	Analyse de tous les risques et rédaction de politiques générales de sécurité de l'information.
2	Gestion des incidents	Processus de prévention, de détection, de réponse et de reprise en cas d'incident.
3	Continuité des activités	Gestion des sauvegardes, reprise des activités après sinistre et gestion de crise.
4	Sécurité de la chaîne d'approvisionnement	Y compris les pratiques de sécurité des fournisseurs ; dispositions contractuelles en matière de cybersécurité avec les fournisseurs directs.
5	Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information	Sécurité tout au long du cycle de vie, y compris le traitement et la divulgation des vulnérabilités.
6	Politiques et procédures pour évaluer l'efficacité des mesures de gestion des risques	Évaluation régulière de l'efficacité des mesures de gestion des risques.
7	Pratiques de base en matière de cyberhygiène et formation à la cybersécurité	Pratiques de cyberhygiène et formation à la sensibilisation pour le personnel.
8	Politiques et procédures relatives à l'utilisation de la cryptographie et, le cas échéant, du chiffrement	Politiques sur l'utilisation du chiffrement ; chiffrement de bout en bout le cas échéant.
9	Sécurité des ressources humaines, politiques de contrôle d'accès et gestion des actifs	Vérifications de sécurité du personnel, autorisations et inventaire des actifs.
10	Utilisation de solutions d'authentification à plusieurs facteurs ou d'authentification	Authentification multifacteur le cas échéant, authentification continue, communications

10. Obligations d'information en cas d'incident (Article 23)

L'innovation opérationnelle la plus importante de la directive est le régime de notification des incidents en plusieurs étapes. Les entités essentielles ou importantes doivent notifier les **incidents importants**, définis comme ceux causant une perturbation opérationnelle grave, des pertes financières ou un impact substantiel sur d'autres personnes, au CSIRT ou à l'autorité compétente dans les délais suivants.

Étape	Délai	Contenu
Alerte précoce	Dans les 24 heures après avoir eu connaissance de l'incident	Suspicion que l'incident est causé par un acte illicite ou malveillant ; possibilité d'impact transfrontière ; informations de base permettant la prise de conscience du CSIRT.
Notification d'incident	Dans les 72 heures après avoir eu connaissance de l'incident	Mise à jour de l'alerte précoce ; gravité, impact et, le cas échéant, indicateurs de compromission (IoC).
Rapport intermédiaire / final	Au plus tard 1 mois après la notification d'incident	Description détaillée de l'incident, sa gravité et son impact ; type de menace exploitée ; mesures d'atténuation prises et prévues ; impact transfrontière le cas échéant.
Rapport d'avancement	Si l'incident est toujours en cours à l'échéance du rapport final	Rapport d'avancement sur l'état actuel de l'incident ; rapport final 1 mois après la clôture du traitement de l'incident.

Notification aux destinataires des services : Lorsqu'une cybermenace importante est susceptible de se produire, les entités doivent, sans retard injustifié et gratuitement, informer les destinataires de leurs services des mesures d'atténuation possibles et, le cas échéant, de la menace elle-même, en termes clairs et compréhensibles.

Incidents évités et déclarations volontaires

En plus des incidents, les entités **peuvent déclarer volontairement des incidents évités et des cybermenaces significatives** au CSIRT ou à l'autorité compétente. Les entités ne relevant pas du champ d'application de la directive peuvent également déclarer volontairement. La déclaration volontaire n'impose pas d'obligations supplémentaires au déclarant.

> **Impact pratique :** L'alerte précoce sous 24 heures oblige les entités à disposer d'un plan de réponse aux incidents cybernétiques et d'un flux de communication prêts à être activés immédiatement dès la détection d'un incident. Respecter ce délai au moyen de processus manuels et fragmentés est extrêmement difficile.

11. Sécurité de la chaîne d'approvisionnement

La plupart des grandes cyberattaques de ces dernières années ont atteint leurs organisations cibles par le biais de fournisseurs et de prestataires de logiciels, et non par une attaque directe contre l'organisation elle-même. La directive place donc le risque lié à la chaîne d'approvisionnement au coeur des obligations de gestion des risques.

- Les entités doivent évaluer la **qualité, les pratiques de sécurité et les processus de développement sécurisé** des produits et services de leurs fournisseurs et prestataires de services.
- **Les exigences de cybersécurité doivent être incluses dans les contrats** avec les fournisseurs directs.
- Une diligence particulière doit être exercée lors de la sélection des **fournisseurs de services de sécurité gérés (MSSP)** ; ces prestataires constituent des cibles de grande valeur pour les attaquants.
- Le groupe de coopération, en collaboration avec la Commission et l'ENISA, procède à des **évaluations coordonnées des risques pour la sécurité** des chaînes d'approvisionnement critiques (comme cela a été fait pour les réseaux 5G).
- Les **facteurs de risque non techniques** sont également dans le champ de l'évaluation, notamment l'influence indue potentielle de pays tiers sur les fournisseurs, les vulnérabilités cachées ou portes dérobées, et la dépendance vis-à-vis d'un prestataire.

12. Responsabilité de l'organe de direction

La directive fait en sorte que la cybersécurité ne soit plus un sujet confiné aux départements techniques mais relève du **domaine de responsabilité directe de la direction générale**. En vertu de l'article 20, les organes de direction des entités essentielles et importantes :

- Sont responsables de **l'approbation des mesures de gestion des risques** au titre de l'article 21 et de la supervision de leur mise en oeuvre ;
- Peuvent être **tenus personnellement responsables** du non-respect de ces obligations ;
- Doivent régulièrement recevoir une formation en cybersécurité afin d'acquérir les connaissances et compétences suffisantes ;
- Doivent encourager une formation similaire pour leur personnel.

> **Important :** Dans les entités essentielles, l'autorité compétente peut demander l'application de **suspensions temporaires d'exercice des fonctions dirigeantes** à la direction générale (les personnes au niveau de PDG ou de représentant légal). Il s'agit d'une mesure de dernier recours, applicable uniquement après que toutes les autres options d'exécution ont été épuisées.

13. Structures de coopération au niveau de l'UE

La directive réglemente ou renforce diverses structures assurant une coopération efficace entre les États membres :

Structure	Fonction
Groupe de coopération	Soutient la coopération au niveau stratégique ; prépare des programmes de travail bisannuels ; publie des documents d'orientation ; procède à des évaluations coordonnées des risques pour les chaînes d'approvisionnement critiques.
Réseau des CSIRT	Coopération au niveau opérationnel ; partage d'informations sur les incidents ; assistance mutuelle ; réponse conjointe.
EU-CyCLONe	Réseau européen des organisations de liaison en cas de cybercrises ; fait le lien entre les niveaux technique et politique lors d'incidents et de crises de grande envergure ; prépare des analyses d'impact.
ENISA	Établit et gère la base de données européenne des vulnérabilités ; fournit un soutien technique ; élabore des orientations ; surveille les politiques de cyberhygiène des États membres.
Dispositifs IPCR	Dispositifs de réponse intégrée aux crises politiques de l'UE (décision d'exécution du Conseil 2018/1993), gestion des crises de grande envergure au niveau de l'Union.
Coordinateur CVD des CSIRT de l'UE	Un CSIRT dans chaque État membre est désigné coordinateur pour gérer la divulgation coordonnée transfrontière des vulnérabilités.

Coopération avec des pays tiers : L'UE peut conclure des accords internationaux avec des pays tiers ou des organisations internationales au titre de l'article 218 du TFUE. Ces accords peuvent, tout en préservant les intérêts de l'Union et la protection des données, permettre à ces parties de participer aux activités du groupe de coopération, du réseau des CSIRT ou d'EU-CyCLONe.

14. Supervision et exécution

La directive prévoit des régimes de supervision différents pour les deux catégories d'entités. Les **entités essentielles** sont soumises à une supervision à la fois ex ante et ex post, tandis que les **entités importantes** ne sont supervisées qu'ex post, sur preuve ou plainte.

Pouvoirs de supervision des autorités compétentes

- Procéder à des inspections sur place et à une supervision à distance ;
- Demander des audits de sécurité ciblés (avec prise en charge potentielle des coûts par l'entité) ;
- Ordonner des analyses de sécurité ;
- Demander la documentation attestant de la conformité aux mesures de gestion des risques ;
- Demander des informations sur des actes soupçonnés d'enfreindre la directive ;
- Demander des informations nécessitant l'accès à des données à caractère personnel et à des données de trafic lorsque cela est nécessaire.

Mesures d'exécution applicables

- Émettre des avertissements et des instructions contraignantes ;
- Ordonner la mise en oeuvre de mesures spécifiques ou la remédiation de vulnérabilités dans un délai déterminé ;
- Ordonner un audit indépendant pour vérifier les mesures de gestion des risques ;
- Ordonner aux entités d'informer les destinataires de services sur la nature de la violation ;
- Publier des déclarations (divulgant le nom de l'entité et la nature de la violation) ;
- Pour les entités essentielles (en dernier recours) : suspension temporaire de certifications ou d'autorisations et interdictions temporaires d'exercice des fonctions dirigeantes pour la direction générale ;
- Imposer ou solliciter l'imposition d'amendes administratives.

15. Amendes administratives

La directive fixe des **seuils maximaux harmonisés au niveau de l'UE** pour les amendes administratives appliquées par les États membres. Ces seuils sont indexés sur le chiffre d'affaires mondial de l'entité, à l'instar du RGPD.

Type d'entité	Montant maximal (le montant le plus élevé s'applique)
Entités essentielles	10 000 000 EUR ou 2 % du chiffre d'affaires annuel mondial
Entités importantes	7 000 000 EUR ou 1,4 % du chiffre d'affaires annuel mondial

Facteurs pris en compte pour déterminer les amendes

- Nature, gravité et durée de l'infraction ;
- Dommages matériels ou moraux causés ;
- Caractère intentionnel ou négligent de l'infraction ;
- Mesures prises pour prévenir ou atténuer les dommages ;
- Degré de responsabilité et infractions antérieures ;
- Degré de coopération avec l'autorité compétente ;
- Autres facteurs aggravants ou atténuants.

Les amendes doivent être **proportionnées**, et des droits fondamentaux tels que le droit à la défense, la présomption d'innocence et le droit à un recours effectif doivent être respectés lors de leur application. Les États membres peuvent également prévoir des sanctions pénales pour les violations du droit national ; toutefois, nul ne peut être sanctionné deux fois pour le même acte en violation du principe **ne bis in idem**.

16. Calendrier de mise en oeuvre et transition

Date	Événement
14 décembre 2022	Adoption de la directive par le Parlement européen et le Conseil
27 décembre 2022	Publication au Journal officiel de l'UE (JO L 333/80)
16 janvier 2023	Entrée en vigueur de la directive (20 jours après la publication)
17 octobre 2024	Délai de transposition de la directive en droit national par les États membres
18 octobre 2024	Début d'application de la directive
18 octobre 2024	Abrogation de la directive (UE) 2016/1148 (SRI 1)
17 avril 2025	Délai de transmission par les États membres à la Commission de la liste des entités essentielles et importantes
À partir du 17 octobre 2027	Réexamen périodique de la mise en oeuvre de la directive par la Commission (tous les 36 mois)

> **Important :** La NIS2 est une directive ; elle ne s'applique pas directement. Chaque État membre doit transposer la directive dans son droit national. Par conséquent, les obligations et sanctions précises applicables à une entité dépendent de la loi de transposition nationale adoptée par l'État membre dans lequel elle opère.

17. Implications pour les entreprises hors UE

Bien que la NIS2 soit une directive de l'UE, elle a des implications substantielles pour les entreprises hors UE, en particulier celles servant le marché européen ou fournissant des entités critiques établies dans l'UE :

Entreprises hors UE directement concernées

- Les **fournisseurs de services DNS, fournisseurs de services d'informatique en nuage, opérateurs de centres de données, fournisseurs de CDN, fournisseurs de services gérés et de services de sécurité gérés, places de marché en ligne, moteurs de recherche et plateformes de réseaux sociaux** hors UE offrant des services dans l'UE doivent désigner un représentant dans l'UE et se conformer aux obligations de la directive ;
- Les entreprises hors UE ayant des filiales ou des succursales dans l'UE peuvent être soumises à la directive par le biais de ces entités ;
- Les fournisseurs hors UE fournissant des produits ou services à des entités essentielles ou importantes de l'UE seront soumis aux **exigences contractuelles de sécurité de la chaîne d'approvisionnement** imposées par leurs clients (article 21(2)(d)) ;
- Les MSP et MSSP hors UE servant des infrastructures numériques ou des entités financières de l'UE peuvent relever directement du champ d'application.

Effets indirects

- Les évaluations des risques liés à la chaîne d'approvisionnement par les clients de l'UE contraignent les fournisseurs hors UE à relever leurs normes de cybersécurité ;
- Les normes introduites par la directive (ISO/IEC 27001, orientations de l'ENISA, etc.) deviennent des **références de facto** sur le marché mondial ;
- Les pays hors UE utilisent de plus en plus la NIS2 comme référence pour élaborer leur propre législation en matière de cybersécurité.

18. Feuille de route pratique de mise en conformité (10 étapes)

La feuille de route suivante en 10 étapes sert de guide pratique tant pour les entreprises opérant au sein de l'UE que pour celles souhaitant s'aligner volontairement sur les normes NIS2.

Étape	Activité
1. Détermination du champ d'application	Déterminer si l'entreprise relève des secteurs de l'Annexe I ou de l'Annexe II, si elle répond aux critères de taille, et identifier sa catégorie (essentielle/importante).
2. Analyse des écarts	Évaluer le système de gestion de la sécurité de l'information existant par rapport aux 10 catégories de mesures de l'article 21 ; cartographier les lacunes.
3. Structure de gouvernance	Établir les responsabilités, les lignes hiérarchiques et les processus d'approbation au niveau du conseil d'administration ou de la direction générale ; mettre en place un programme de formation régulier.
4. Politiques et documentation	Préparer ou mettre à jour la politique de sécurité de l'information, la politique de gestion des risques, la politique de réponse aux incidents, la politique d'utilisation acceptable et d'autres documents.
5. Évaluation des risques	Réaliser un inventaire des actifs, une analyse des menaces et une évaluation des risques selon une approche tous risques ; établir les critères d'acceptation des risques.
6. Mise en oeuvre des contrôles techniques	Mettre en oeuvre l'authentification multifacteur, le chiffrement, la segmentation réseau, l'architecture de confiance zéro, la gestion des journaux, le SIEM, les solutions EDR/XDR, de sauvegarde et de reprise après sinistre.
7. Capacité de réponse aux incidents	Documenter le plan de réponse aux incidents ; attribuer les rôles et responsabilités ; établir le flux de communication d'alerte précoce de 24 heures ; réaliser des exercices de simulation sur table.
8. Gestion de la chaîne d'approvisionnement	Dresser l'inventaire des fournisseurs ; les classer par niveau de risque ; ajouter des clauses de cybersécurité aux modèles de contrats ; réaliser des audits périodiques.
9. Formation et sensibilisation	Organiser une formation annuelle à la cyberhygiène pour l'ensemble du personnel ; fournir une formation spécialisée à l'organe de direction ; mener des simulations de hameçonnage.
10. Amélioration continue	Réaliser des audits internes et externes ; suivre les KPI ; tirer les enseignements de chaque incident ; mettre à jour l'évaluation des risques annuellement ; rechercher une certification (ISO/IEC 27001, certification de cybersécurité de l'UE).

19. Conclusion et évaluation

La directive NIS2 relève substantiellement le niveau de référence en matière de cybersécurité dans l'Union européenne. Elle n'impose pas seulement des exigences techniques ; elle fait également de la cybersécurité une **partie intégrante de la structure de gouvernance et des opérations commerciales des entreprises**.

Points forts de la directive

- **Large portée** : environ 18 secteurs et plus de 100 000 entités concernées dans les 27 États membres ;
- **Harmonisation** : conditions de concurrence équitables sur le marché intérieur grâce à des critères uniformes et un régime d'exécution commun dans toute l'UE ;
- **Accent sur la gouvernance** : en responsabilisant la direction générale, la directive garantit que la cybersécurité imprègne toutes les couches de l'entreprise ;
- **Accent sur la chaîne d'approvisionnement** : répond à la réalité que la majorité des attaques modernes proviennent de la chaîne d'approvisionnement ;
- **Structures de coopération** : coordination multicouche au niveau de l'UE par le groupe de coopération, le réseau des CSIRT et EU-CyCLONe.

Critiques et défis

- Retards et divergences dans la transposition par les États membres ; dans la pratique, la mise en oeuvre uniforme au sein des 27 est inégale ;
- Pour les entreprises de taille moyenne en particulier, le coût de la mise en conformité et la réduction des lacunes en matière de capacités techniques constituent un défi sérieux ;
- La mise en oeuvre du délai d'alerte précoce de 24 heures avant qu'un niveau de maturité suffisant soit atteint peut conduire à des flux de notification superficiels ou erronés ;
- Les chevauchements avec les réglementations sectorielles (DORA, finance ; eIDAS, services de confiance ; réglementations sectorielles de l'aviation, etc.) peuvent créer de la complexité pour les entités.

Évaluation globale

La NIS2 repositionne la cybersécurité, qui n'est plus une préoccupation technique mais une question de **continuité des activités, de gouvernance d'entreprise et de confiance des clients**. Pour les entités opérant dans l'UE ou interagissant avec elle, la conformité est à la fois une obligation légale et un moyen de renforcer la résilience opérationnelle.

Pour les entreprises hors UE, la NIS2 établit une nouvelle **norme de facto** pour l'accès au marché européen et relève les attentes mondiales en matière de cybersécurité. Une mise en conformité anticipée facilite le respect des obligations contractuelles et améliore la cyberrésilience globale.

> **Note finale :** Ce document résume les principales dispositions de la directive pour les lecteurs francophones. Pour les exigences de conformité spécifiques à votre organisation, consultez le texte officiel (JO L 333/80, 27.12.2022), la loi de transposition nationale de votre État membre et les réglementations sectorielles ; faites appel à des conseillers juridiques et en cybersécurité le cas échéant.

Sources

- Directive (UE) 2022/2555, numéro CELEX EUR-Lex 32022L2555
- Journal officiel de l'UE L 333/80, 27 décembre 2022
- ENISA, Agence de l'Union européenne pour la cybersécurité (www.enisa.europa.eu)
- Portail de stratégie numérique de la Commission européenne (digital-strategy.ec.europa.eu)

En savoir plus sur la NIS2 avec Rediacc

Ce résumé cartographie la structure et les obligations de la directive. Les guides complémentaires sur rediacc.com traduisent ces obligations en décisions opérationnelles et d'approvisionnement concrètes.

Trois guides complémentaires

- **Article 21(2)(d) et l'auto-hébergement.** Pourquoi le registre des TIC tiers se réduit lorsque le plan de données ne quitte jamais votre infrastructure. Pour les RSSI et les responsables achats renégociant leurs DPA en 2026.
- **Efficacité continue sans simulacre.** Les articles 21(2)(e), (f) et 23 lus ensemble. Le fork à temps constant qui rend les exercices hebdomadaires réalistes, et le calendrier de notification de l'article 23 que vous ne pouvez pas respecter sans artéfacts de qualité forensique. Pour les responsables SRE et opérations.
- **Le coût structurel de la conformité NIS2.** La pile de cinq outils que les entités essentielles du marché intermédiaire assemblent discrètement, ce qu'un plan de contrôle auto-hébergé fait disparaître, et les postes budgétaires qui restent de toute façon à votre charge. Pour les directeurs financiers et les acheteurs abordant un cycle de renouvellement.

Où les trouver

Ces trois guides, ainsi que ce résumé en PDF téléchargeable, sont disponibles sur :

rediacc.com/resources/nis2-directive-summary

Rediacc OÜ est une plateforme d'infrastructure auto-hébergée enregistrée en Estonie (Code de registre 17363830, TVA EE102920091). Le produit ne se substitue pas à un programme de sécurité ; il s'agit d'une couche d'outillage qui supprime le risque fournisseur du plan de données que les outils traditionnels de sauvegarde, de reprise après sinistre et de données de test ne peuvent pas éliminer. Niveau Community gratuit et niveaux payants à partir de 349 $/mois.

> Ce document et ses guides complémentaires sont des supports éducatifs. Les décisions de conformité spécifiques à votre organisation nécessitent un conseil juridique et une référence à la loi de transposition nationale applicable dans votre juridiction.