TROIS (point) QUATORZE avocats

NEWSLETTER · NOVEMBRE 2026

Loi cybersécurité : vos engagements de sécurité

NIS 2



LE CONSTAT

Un texte voté, des engagements déjà signés

Le 17 novembre 2026, l'Assemblée nationale a adopté, par 464 voix contre 64, le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité. Il transpose NIS 2, REC et DORA, avec deux ans de retard.

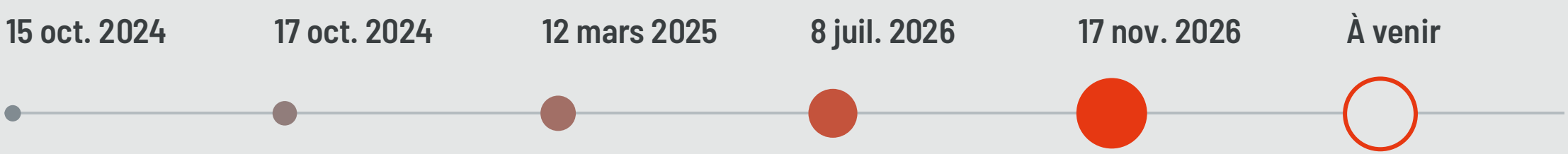
Députés et sénateurs doivent maintenant s'accorder sur un texte commun. Vos clients vous demandent déjà de vous engager sur votre niveau de sécurité.

À RETENIR

Vos engagements de sécurité sont déjà signés. Le cadre de contrôle se précise.

LE CALENDRIER

Un texte attendu depuis deux ans



15 oct. 2024

Dépôt du projet de loi au Sénat, procédure accélérée.

17 oct. 2024

Date limite de transposition de NIS 2.

12 mars 2025

Adoption du texte par le Sénat.

8 juil. 2026

La Commission européenne saisit la Cour de justice de l'UE.

17 nov. 2026

Adoption par l'Assemblée nationale : 464 voix contre 64.

À venir

Commission mixte paritaire, promulgation, puis décrets d'application.

À SURVEILLER

Le texte peut encore évoluer en commission mixte paritaire, et les décrets fixeront une bonne partie du détail opérationnel. Pour savoir si vous êtes concerné : l'espace NIS 2 de l'ANSSI, monespacenis2.cyber.gouv.fr.

Ce que le texte change pour vous

Un périmètre large

Près de 15 000 entités sont concernées, dans 18 secteurs, contre quelques centaines aujourd'hui. L'ANSSI est cheffe de file. Les députés ont ajouté la facturation électronique (plateformes agréées) et les établissements de santé privés d'intérêt collectif.

Un contrôle, parfois à votre charge

L'ANSSI pourra prescrire des référentiels, contrôler sur place ou à distance, auditer. Les audits confiés à un prestataire qualifié que vous choisissez sont à votre charge. Faire obstacle au contrôle est sanctionné.

Une charge de la preuve pour l'assureur

Pour une cyberattaque, l'assureur ne pourra opposer l'exclusion de guerre étrangère que s'il prouve que le sinistre en résulte (article 58 bis, non définitif).

Confidentiel – tous droits réservés – Troispointquatorze – novembre 2026

Ce que le texte vous demande concrètement

La direction aux commandes

Les organes de direction approuvent et **supervisent** les mesures de sécurité, et sont **formés** à la cybersécurité. En dernier recours, un dirigeant d'entité essentielle peut se voir interdire d'exercer ses responsabilités dirigeantes.

Des fournisseurs sous contrôle

Il faut **identifier** vos fournisseurs et prestataires, **évaluer** leur criticité et revoir cette liste chaque année. En cas de sous-traitance, les rôles et les responsabilités de chacun sont précisés à l'avance.

Une notification en trois temps

Pour un incident important : alerte sous 24 heures, notification sous 72 heures, rapport final sous un mois. Un guichet unique ANSSI-CNIL est prévu.

SANCTIONS

Jusqu'à 10 M€ ou 2 % du chiffre d'affaires mondial pour les entités essentielles, 7 M€ ou 1,4 % pour les entités importantes (le montant le plus élevé est retenu). Les entités importantes ne sont contrôlées que sur indices de manquement.

Confidentiel – tous droits réservés – Troispointquatorze – novembre 2026

Un prestataire attaqué, des clients fragilisés

1er-2 NOVEMBRE · EFS

Un prestataire de l'Établissement français du sang est visé. La température des chambres froides, maintenue à -30 °C, est portée à +110 °C.

4 NOVEMBRE · CRÉDIT MUTUEL ARKÉA

Une attaque permet des opérations frauduleuses sur le compte propre du groupe. Coût estimé : une centaine de millions d'euros.

14 NOVEMBRE · MAILEVA (DOCAPOSTE)

Vol des noms et adresses de 22 millions de personnes. L'attaque date de la mi-septembre : les personnes concernées l'ont appris le 14 novembre.

NOTRE LECTURE

Le texte place la sécurité de la chaîne d'approvisionnement parmi les mesures obligatoires. Vos clients doivent surveiller leurs prestataires : c'est pour cela qu'ils vous demandent des engagements. « Un prestataire compromis, ce sont des dizaines de clients fragilisés », a résumé la députée Patricia Lemoine le 17 novembre (compte rendu de séance).

Confidentiel – tous droits réservés – Troispointquatorze – novembre 2026

PLAN D'ACTION · VOS PRIORITÉS

Ce que vous devez faire

01

Relire vos engagements

Recensez les contrats et documents d'adhésion qui contiennent des engagements de sécurité. Repérez les engagements de résultat, l'absence de plafond et les délais de notification d'incident.

02

Faire auditer votre sécurité

Faites auditer votre sécurité IT par un tiers pour connaître vos failles avant de vous engager davantage. Listez aussi vos prestataires critiques et vérifiez leurs engagements envers vous.

03

Vérifier votre assurance cyber

Souscrivez une assurance cyber, ou relisez la vôtre à la lumière de la charge de la preuve que le texte met sur l'assureur en cas de guerre étrangère.

04

Négocier le document

Challengez le document de votre client, plafond de responsabilité compris, au lieu de le signer tel quel.

Confidentiel – tous droits réservés – Troispointquatorze – novembre 2026

On regarde vos engagements avec vous ?

Audit de vos engagements de sécurité

Relecture de vos contrats et documents d'adhésion : engagements de résultat, plafond de responsabilité, obligations de notification.

Négociation et mise en conformité

Accompagnement pour challenger les documents de vos clients et vous préparer au cadre NIS 2.

Prenez 30 minutes pour en parler : contact@troispointquatorze.fr

TROIS QUATORZE avocats

Membre du réseau GOJI avocats

Confidentiel – tous droits réservés – Troispointquatorze – novembre 2026 · www.troispointquatorze.fr