Cyber Resilience Act : calendrier de mise en œuvre prévu dans le Règlement

Le Cyber resilience Act est adopté

23/11/2024

Entrée en application des principales mesures

11/06/2026

Dispositions relatives à la notification des organismes d'évaluation de la conformité (Chapitre IV, article 34 à 51)

11/09/2026

Obligations en matière de communication d'informations / signalements incombant aux fabricants (article 14)

11/12/2027

Entrée en application des autres dispositions du CRA

3 ans après entrée en vigueur du CRA (puis tous les 4 ans)

La Commission fournira au Parlement un rapport d'audit concernant la bonne mise en œuvre et application du CRA

Calendrier précisé par la Commission européenne en décembre 2025

2025

28/11 : Règlement d'exécution relatif à la description technique des **catégories de produits importants et critiques** comportant des éléments numériques

11/12 : Règlement délégué précisant les conditions d'application des motifs ayant trait à la cybersécurité en ce qui concerne le **report de la diffusion des notifications**

2026

Q1 2026 : Lignes directrices élaborées par la Commission européenne

11/06 : Dispositions relatives à la notification des organismes d'évaluation de la conformité (Chap. IV, article 34 à 51)

Q3 2026 : Premiers livrables en matière de **normalisation** (normes horizontales et spécifiques aux produits)

11/09 : Obligations en matière de communication d'informations / signalements incombant aux **fabricants** (article 14)

2027

30/11 : Nouveaux livrables en matière de **normalisation**

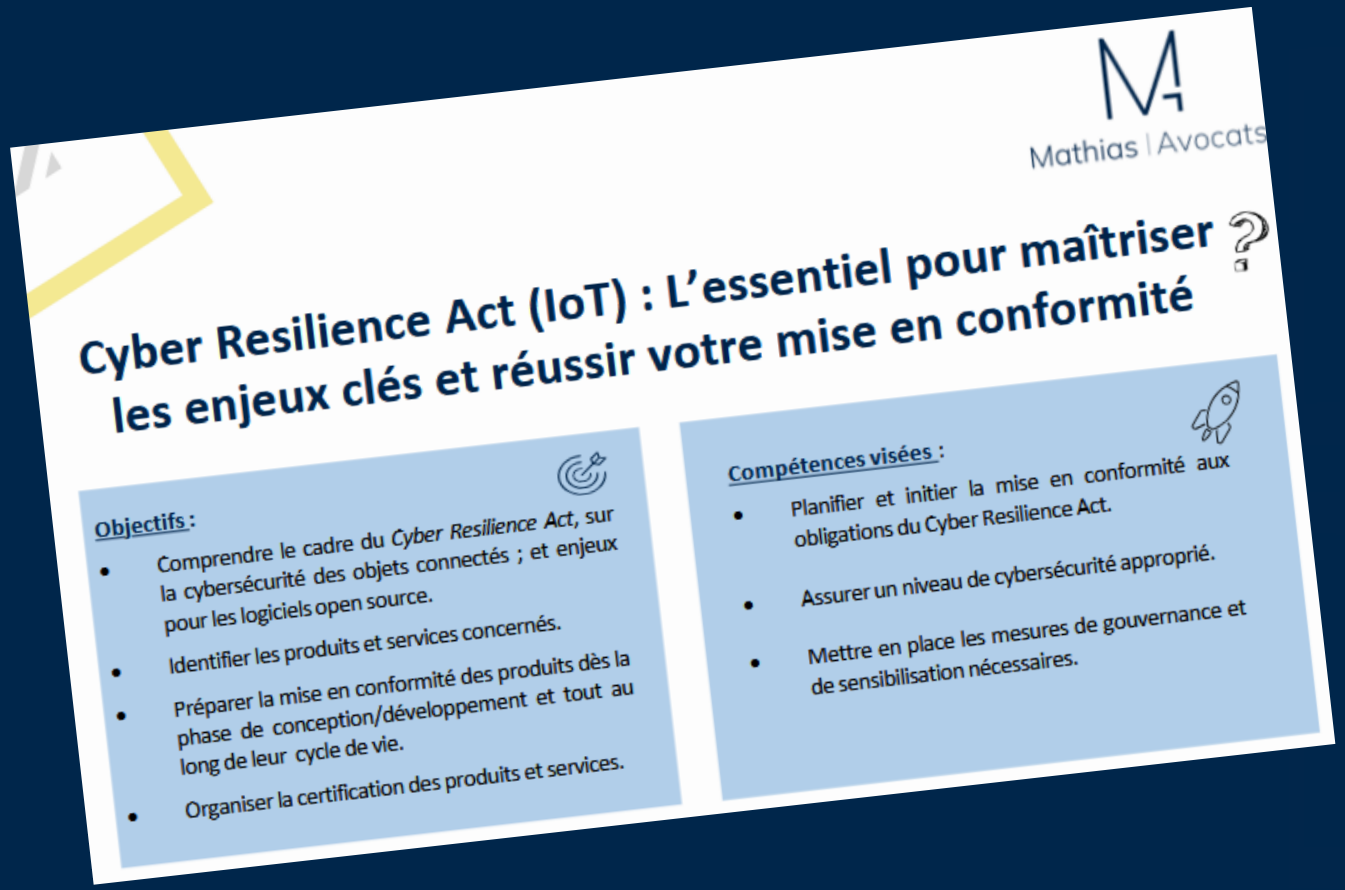
11/12 : **Pleine entrée en application du CRA**

CRA

Texte UE	Règlement CRA
Objectifs principaux	Vise à renforcer la sécurité des produits comportant des éléments numériques dans l'UE
Champ d'application	Tous les produits TIC (matériels et logiciels), appareils connectés, etc.
Gestion des risques	Mesures de sécurité durant tout le cycle de vie du produit (conception, développement, mise à jour, etc.)
Notification des incidents	Délai de 24h pour la notification par le fabricant (art.14) aux CSIRT (première alerte) ; 72h (précisions du signalement)
Régulation / Supervision	ENISA, autorité nationales de cybersécurité, équipes CSIRT (*Computer Security Incident Response Team)*
Sanctions	Jusqu'à 15 millions € ou 2,5% du CA mondial total notamment pour violation des obligations incombant au fabricant

MATHIAS Avocats

20 ans d'expertise en droit du numérique



Catalogue des formations

Mathias | Avocats

Parmi nos formations en cybersécurité :

Mathias | Avocats

Conformité | Cybersécurité | NIS 2

NIS 2 & REC : Maîtriser les principes-clés et réussir votre mise en conformité

Conformité | Cybersécurité | NIS 2

NIS 2 : L'essentiel pour maîtriser les principes clés et réussir votre mise en conformité

Conformité | Cybersécurité | DORA

DORA : Maîtriser les principes clés et réussir votre mise en conformité

Conformité | Cyber Resilience Act – CRA | Cybersécurité

Cyber Resilience Act (IoT) : L'essentiel pour maîtriser les enjeux clés et réussir votre mise en conformité

Mathias | Avocats

Besoin d'une veille juridique sur mesure ?

Sur les thématiques qui vous intéressent, sur votre secteur d'activité, votre métier, les nouvelles exigences / le cadre juridique de vos missions, vos opportunités…

NOUS CONTACTER

Mathias Avocats réalise des veilles sur-mesure pour ses clients, selon les thématiques sélectionnées, secteurs d'activités, métiers.

- **Une veille pour vous et vos équipes, chaque mois dans votre boîte mail**
- **Contenu, format, périodicité, tarif : contactez-nous !**

Mathias | Avocats

SUIVEZ VOTRE ACTUALITÉ, ABONNEZ-VOUS !

UNE NEWSLETTER MENSUELLE OFFERTE

Mathias | Avocats

JANVIER 2026

Newsletter

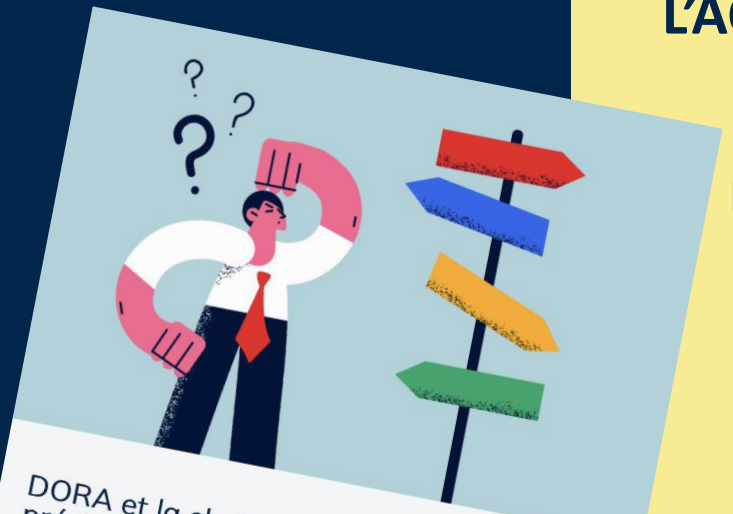
VOUS AVEZ PEUT-ÊTRE MANQUÉ...

Déploiement d'outils d'IA dans l'entreprise : le rôle du CSE

L'introduction de nouvelles technologies, dont l'IA, au sein des entreprises nécessite la consultation et l'information du Comité Social et Economique (CSE) dès lors que cette nouvelle technologie peut modifier les conditions de travail (article L 2312-8 du code du travail).

Quelles sont les bonnes pratiques lors du déploiement d'outils d'IA ? Quels sont les apports de décisions de justice récentes concernant le rôle, à cet égard, du CSE ?

EN SAVOIR PLUS



DORA et la chaîne de sous-traitance : Les précisions apportées et points d'attention

15 Déc, 2025 | Conformité, Contrats, Cybersécurité / Cybercriminalité, Droit du numérique

Le Règlement européen sur la résilience opérationnelle numérique du secteur financier, dit « DORA » (Digital operational resilience act) est entré en application le 17 janvier 2025. La mise en œuvre d'un certain nombre de dispositions de ce texte est...

lire plus

L'ACTUALITÉ DÉCRYPTÉE POUR VOUS !

ENSEMBLE, DÉVELOPPONS VOS PROJETS
ET FORMONS VOS ÉQUIPES !
PARTAGEONS NOS EXPERTISES !

AU QUOTIDIEN

Catalogue des formations