



CRA : Comment se mettre en conformité ?

Les essentiels à retenir

JUILLET 2026

Mathias Avocats



AVIS IMPORTANT

Les informations contenues dans le présent document ne constituent pas des conseils juridiques et ne peuvent s'y substituer.



Cyber Resilience Act : pour la sécurité des produits connectés

Quel contexte ?

Les entités telles utilisent de nombreux objets connectés au sein de leurs activités quotidiennes.

Toutefois, un certain nombre de ces produits présentent des **normes de sécurité insuffisantes**, **constituant ainsi une cible pour les cyberattaques**. Ces **attaques peuvent avoir de graves conséquences sur le fonctionnement de ces entités** (perte de chiffre d'affaires, atteinte réputationnelle etc.).

Face à cet enjeu, le CRA permet de **s'assurer que les fabricants proposent des produits présentant un niveau de cybersécurité plus élevé**, et ce, tout au long de la vie des produits.

➡ Cette législation répond à une **prise de conscience croissante des vulnérabilités** auxquelles sont exposés les utilisateurs dans un monde de plus en plus interconnecté.



Cyber Resilience Act : pour la sécurité des produits connectés



Le **Règlement sur la Cyber résilience** adopté le **23 octobre 2024** (et publié le 20 novembre 2024) vise à compléter NIS 2 et DORA en **protégeant les consommateurs et les entreprises** qui utilisent des **produits** ou des **logiciels** comportant un **composant numérique**.

Le CRA concerne **tous les produits connectés** (directement ou indirectement).

Il comprend des exceptions : SaaS, secteur médical, aviation...

Objectifs

- Améliorer la **sécurité des produits comportant des éléments numériques** dès la phase de conception/développement et tout au long du cycle de vie ;
- Mettre en place un **cadre cohérent** au niveau de l'UE en matière de cybersécurité ;
- Améliorer la **transparence** sur la sécurité des produits ; et
- Permettre aux **entreprises** et aux **consommateurs** d'utiliser les produits comportant des éléments numériques en toute sécurité.

Cyber Resilience Act : quelques chiffres

ENISA : Rapport d'enquête du CRA sur les PME

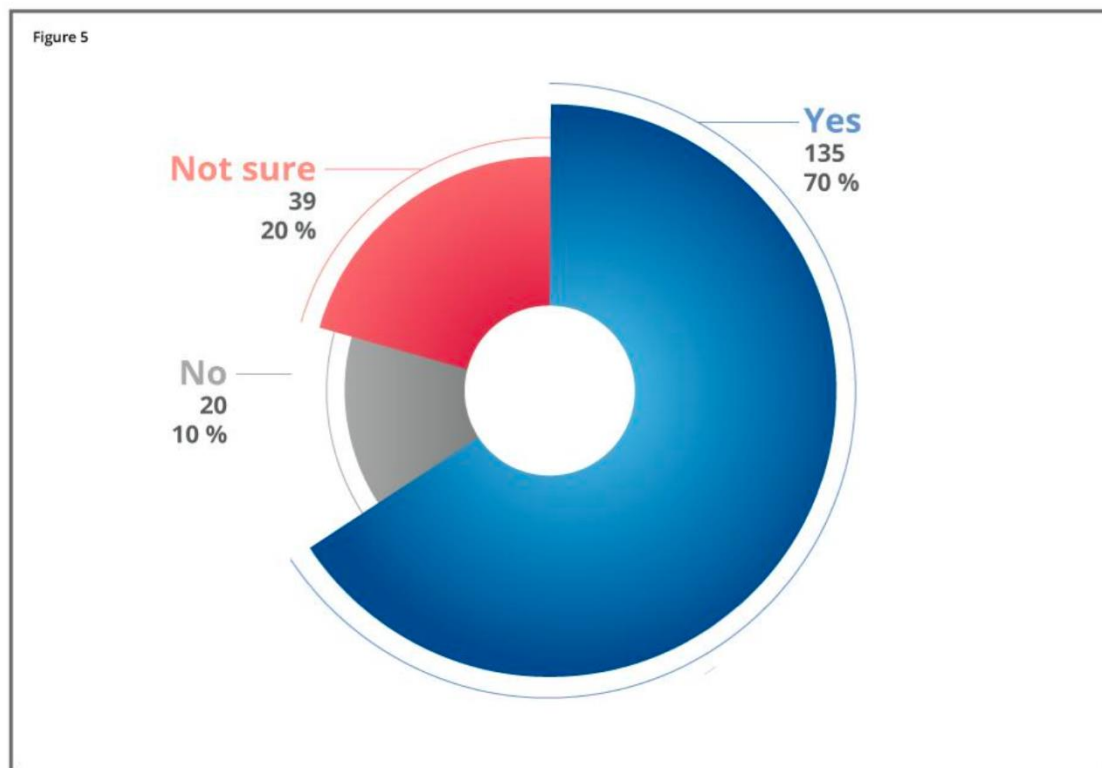


Figure 5: CRA scope (Q1.6: Do you fall under the CRA scope?)

Source : ENISA, SME CRA Survey Report, juin 2026

S'agissant de l'application du CRA aux PME, l'enquête révèle que :

- 70% des PME répondantes relèvent du champ d'application du CRA ;
- 20 % ne sont pas sûres ;
- Et 10 % estiment que le CRA ne leur est pas applicable.



Cyber Resilience Act : quelques chiffres

ENISA : Rapport d'enquête du CRA sur les PME

CRA TOPIC AREA	NONE	LIMITED	MODERATE	GOOD	VERY GOOD
Essential cybersecurity requirements	7%	24%	28%	25%	6%
Vulnerability handling obligations	10%	22%	29%	23%	5%
Secure development and security by design	7%	25%	29%	20%	9%
Required documentation	13%	29%	35%	9%	4%
Conformity assessment and compliance	14%	40%	22%	10%	4%

Les PME ont également indiqué avoir une certaine connaissance préalable du CRA. **Au total, 128 des 19 410 répondantes (66 %) ont indiqué qu'elles connaissaient cette réglementation avant de répondre à l'enquête.**

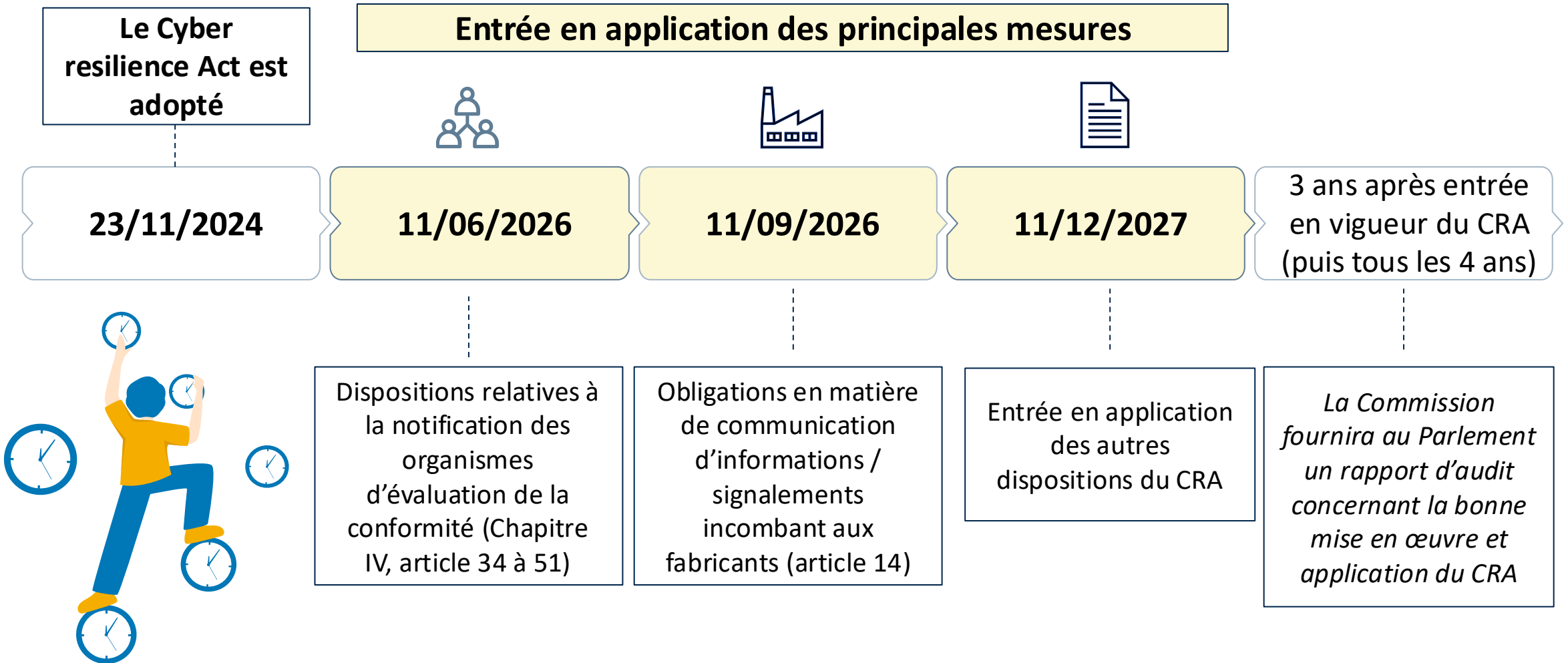
Il s'agit toutefois d'une connaissance générale de l'existence du CRA et non d'une compréhension détaillée de ses exigences.



Table 3: Understanding of the CRA (percentage of respondents) (Q2.2: How would you rate your understanding of the CRA?) (N = 194. "No Answer" responses (n = 20, 10.31%) are excluded from this figure)

Source : ENISA, SME CRA Survey Report, juin 2026

Calendrier de mise en œuvre prévu dans le Règlement



Exemption d'application du CRA (non-exhaustif)



Article 69§2 du CRA

« Les produits comportant des éléments numériques qui ont été mis sur le marché avant le 11 décembre 2027 ne sont soumis aux exigences énoncées dans le présent règlement que si, à compter de cette date, ces produits font l'objet d'une modification substantielle ».



Bonne démarche : Identifier, cartographier vos produits qui font l'objet d'une « *modification substantielle* ».

Article 3§30 du CRA : « *une modification apportée au produit comportant des éléments numériques à la suite de sa mise sur le marché, qui a une incidence sur la conformité du produit comportant des éléments numériques aux exigences essentielles de cybersécurité énoncées à l'annexe I, partie I, ou qui entraîne une modification de l'utilisation prévue pour laquelle le produit comportant des éléments numériques a été évalué* ».



Quelles principales étapes à suivre pour se mettre en conformité ?

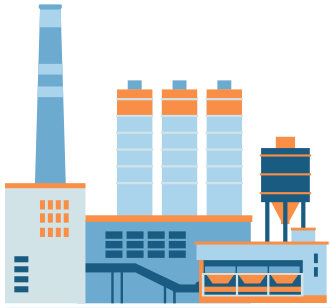
Évaluer
l'application du
CRA à mon entité
et/ou ses impact
sur cette
dernière.

Identifier les obligations
du CRA applicable à mon
entité au regard de sa
qualification ainsi qu'au
regard de la qualification
des produits.

Opérer une qualification de
mon entité (fabricant,
fournisseur, utilisateur, etc.),
ainsi qu'une qualification des
produits (produits importants
comportant des éléments
numérique etc.).

Mettre en place
une gouvernance
adaptée.





Quelles sont les principales obligations du fabricant ? (non-exhaustives)

Distribution et sécurité des mises à jour.

Identifier et documenter les vulnérabilités.

Obligations de communication
(découverte de vulnérabilités ou incidents graves).

Formaliser la documentation technique.

Établir la déclaration UE de conformité.

Apposer le marquage CE.



Le fabricant doit également intégrer la sécurité dès la conception (security by design).





Quelles sont les principales obligations de l'importateur ? (non-exhaustives)

Vérifier la conformité avant la mise sur le marché.

Conserver la documentation et la déclaration de conformité pendant au moins 10 ans.

Refuser la mise sur le marché de produits non conformes.

Signaler tout risque de cybersécurité au fabricant et aux autorités.





Quelles sont les principales obligations du distributeur? (non-exhaustives)

S'assurer que le fabricant et l'importateur ont respecté leurs obligations (traçabilité, information, conformité, documentation).

Refuser la distribution de produits non conformes.

Informers sans délai le fabricant et les autorités en cas de risque ou de vulnérabilité grave.

Participer aux mesures correctives (retrait, rappel, mise en conformité).





Quel principal enjeu lié à la qualification du produit ?

La qualification du produit pour l'évaluation de la conformité des produits comportant des éléments numériques incombe au fabricant.

	Par défaut	Importants de classe I	Importants de classe II	Critiques
Exigences	Exigences de l'Annexe I ou standard harmonisé ou spécification commune ou schéma CSA	Annexe I ou standard harmonisé ou spécification commune	Annexe I ou standard harmonisé ou spécification commune	Annexe I ou standard harmonisé ou spécification commune
	Standard harmonisé (JOUE) ou Spécification commune (selon acte d'exécution) ou Certification CSA (selon acte délégué*)			Présomption de conformité
Evaluation	✓ Autoévaluation (module A) ou ✓ Evaluation par un tiers (modules B + C ou module H) ou ✓ Certification*	✓ Module A selon standard harmonisé, spécification ou schéma CSA sinon ✓ Modules B + C ou module H selon Annexe I ou standard harmonisé ou spécification commune ou ✓ Certification niveau Substantiel*	✗ Module A ✓ Modules B + C ou module H ou ✓ Certification niveau Substantiel*	✗ Module A ✓ Modules B + C ou module H sauf si certification CSA imposée via acte délégué** ou ✓ Certification niveau Substantiel ou Elevé*

* Un acte délégué doit spécifier les schémas CSA permettant de bénéficier de la présomption de conformité

** La Commission peut adopter un acte délégué rendant la certification CSA obligatoire pour certains produits critiques au niveau au moins Substantiel

Source :
[ANSSI](#)

Quelle gouvernance mettre en place ?

En tant que fabricant, notamment :



Effectuer des audits de sécurité.

Formaliser, conserver et mettre à jour la documentation technique : impliquer les équipes juridiques, de conformité et de développement.

Formaliser une procédure d'urgence pour la notification d'incidents graves de sécurité et de vulnérabilités.

Auditer et sélectionner les fournisseurs de composants (matériels ou logiciels) sur la base de critères de sécurité stricts, afin de prévenir l'importation de vulnérabilités dans le produit final.

Effectuer une mise à jour des contrats.



Quelle gouvernance mettre en place ?

En tant que distributeur/importateur, notamment :

Conserver la documentation technique permettant de démontrer la conformité du produit au CRA.

Élaborer un plan de continuité/gestion de crise incluant des procédures pour le retrait de marché et les campagnes de rappel.

Effectuer une mise à jour des contrats en y intégrant des clauses CRA.

Mettre en place une procédure de vérification de la conformité du produit avant sa mise sur le marché.

Pour le distributeur : existence du marquage CE, existence d'informations et d'instructions destinées à l'utilisateur, existence de la déclaration UE de conformité etc.)

Pour l'importateur : existence d'une procédure d'évaluation de la conformité, de la documentation technique, etc.)



Quelle gouvernance mettre en place ?

En tant qu'utilisateur, notamment :

Identifier les dépendances de l'entité (fournisseurs), ainsi que la qualification de l'entité au regard du CRA (fabriquant ? Importateur ? Etc.).

Mise en place d'un processus de *due diligence* (Intégrer les questionnaires fournisseurs ainsi que des grilles d'évaluation de ces derniers dans les appels d'offre et dans les contrats, etc.).

Cartographier l'ensemble des produits comportant des éléments numériques.

Intégrer les critères du CRA dans la politique globale de gestion des risques liés aux tiers.



Publication d'un projet d'orientation par la Commission européenne



La Commission européenne a publié le 3 mars 2026 un **projet** d'orientations, ayant pour objectif d'aider les entreprises à respecter les obligations issues du CRA.

Ce projet vise notamment à préciser le champ d'application des dispositions du CRA, en accordant une attention particulière à la simplification de leur mise en conformité pour les microentreprises ainsi que pour les petites et moyennes entreprises.

 Ref. Ares(2026)2319816 - 03/03/2026



Brussels, XXX
[...] (2026) XXX draft

ANNEX

ANNEX

Communication to the Commission

Approval of the content of the draft Communication from the Commission -
Commission guidance on the application of Regulation (EU) 2024/2847 (Cyber
Resilience Act)

[Consulter le projet de la
Commission européenne](#)

Des formations sur-mesure pour vous et vos équipes, Contactez-nous !

FORMATIONS

Retrouvez les programmes proposés par l'organisme de formation Mathias Avocats



[Retrouvez l'intégralité du Catalogue des formations](#)

Conformité Cyber Resilience Act – CRA Cybersécurité

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



4 heures, en présentiel - continu

Télécharger
293,55 Ko - pdf

Cybersécurité

Aspects juridiques de la cybersécurité: Fondements, obligations et gestion des risques



Durée : 4 heures, en présentiel - continu

Télécharger
240,77 Ko - pdf

Cybersécurité

Gestion de crise, réponse à incident : L'essentiel pour maîtriser les principes clés et réussir votre mise en conformité



Durée : 4 heures, en présentiel - continu

Télécharger
245,67 Ko - pdf

MATHIAS Avocats

20 ans d'expertise en droit du numérique



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...



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 !

& DROIT

GARANCE MATHIAS, EVA ASPE
ET FRANÇOIS GORRIEZ

PRÉFACE DE MYRIAM QUÉMENER

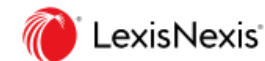
IA, cybersécurité et data : garantir la conformité numérique

**Prix Cybersécurité
du Forum InCyber Europe**



Pour vous et vos équipes !

Disponible chez votre libraire (ou achat en ligne)



Cet ouvrage décrypte les réglementations (*NIS 2, DORA, AI Act, Data Act, Cyber Resilience Act, etc.*) pour vous permettre de maîtriser les risques juridiques, de la contractualisation à la gestion de crise et à sa remédiation, en intégrant également la R&D et l'innovation.

Il contient des **schémas, infographies, interviews de professionnels** (dirigeants, responsables cybersécurité, conformité IA, data, etc.), **des recommandations et outils** (notamment des « **check-lists** » de questions à se poser, des **points de vigilance** sur les **contrats** et la **gestion de crise**).

Conçu comme un **guide pratique**, cet ouvrage propose un parcours de conformité en 5 étapes-clés : **Gouverner, Concevoir, Contractualiser, Gérer les crises et Anticiper**, qui vous accompagnera pour piloter votre conformité numérique.

Par Garance MATHIAS, Eva ASPE et François GORRIEZ,
Editions LexisNexis, Janvier 2026.

SUIVEZ VOTRE ACTUALITÉ, ABONNEZ-VOUS !

UNE NEWSLETTER MENSUELLE OFFERTE

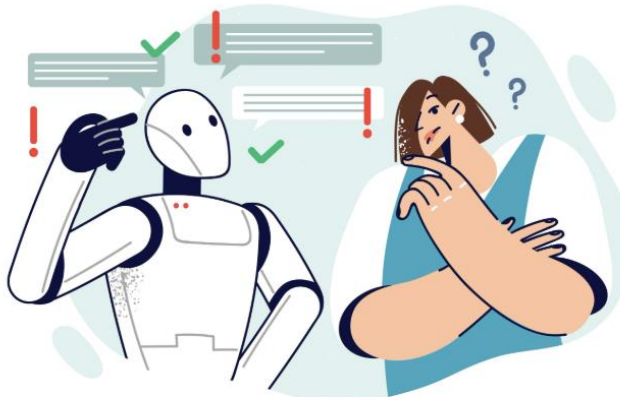


L'établissement d'une documentation technique prévu par le CRA : Focus sur la SBOM

03 Déc , 2025 | Conformité, Cybersécurité / Cybercriminalité, Droit du numérique

Pierre angulaire de la stratégie européenne en matière de cybersécurité, le Règlement sur la cyber-résilience (Cyber Resilience Act ou CRA) concerne les produits ou logiciels comportant des éléments numériques. Il vise à mettre en place le cadre...

[lire plus](#)



NDA : Une nécessaire prise en compte de l'IA

21 Mai , 2026 | Contrats, Droit du numérique, Intelligence artificielle

Loin d'être un simple document accessoire, le Non-Disclosure Agreement (NDA, ou accord de confidentialité) constitue souvent le premier acte de la gouvernance contractuelle : celui où les parties testent leur capacité à structurer leur relation, à...

[lire plus](#)

L'ACTUALITÉ DÉCRYPTÉE POUR VOUS !

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



[AU QUOTIDIEN](#)

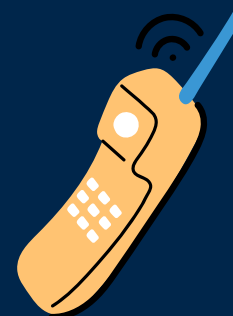
[Catalogue des formations](#)





Mathias | Avocats

CONTACTEZ-NOUS !



19 rue Vernier 75017 PARIS

+33 (0)1 43 80 02 01

contact@avocats-mathias.com

<https://www.avocats-mathias.com/>



@MathiasAvocats

