Vos **ACTUALITÉS** – Offertes par Mathias Avocats

- *Digital Omnibus*
- *Cybersecurity Package*
- *New toolbox – ICT supply chain security*

Cybersécurité

DIGITAL OMNIBUS

Pour un corpus réglementaire simplifié

19 novembre 2025

Contexte :

Le rapport Draghi 2024 attribue en partie le déficit de compétitivité de l'UE aux charges administratives et aux complexités de mise en œuvre de certaines dispositions réglementaires :

- contraintes à l'innovation, en particulier dans le secteur numérique ;
- freins pour les jeunes entreprises européennes qui cherchent à se développer.

➔ Pour son mandat 2024-2029, la Commission s'est engagée à remédier aux manquements recensés dans le rapport Draghi et a entrepris un effort de simplification.

DIGITAL OMNIBUS

Pour un corpus réglementaire simplifié

L'Omnibus numérique adopté par la Commission européenne en **novembre 2025** prend la forme de deux propositions de règlements distinctes :

1 **Omnibus numérique couvrant les règles en matière de données, de cybersécurité et de respect de la vie privée**

Notamment :

- ✓ Un point d'entrée unique pour tous les rapports d'incidents de cybersécurité et de violations de données ; et
- ✓ La fusion des dispositions du Règlement sur la gouvernance des données (DGA), de la Directive sur les données ouvertes et Ru règlement sur la libre circulation des données à caractère non personnel en un texte législatif unique et restructuré sur les données.

2 **Omnibus numérique sur l'IA**, contenant une série de modifications ciblées de la législation sur l'IA, notamment :

- ✓ Aligner le délai d'application des obligations de SIA à haut risque sur la disponibilité de normes et recommandations ;
- ✓ Extension de certaines simplifications accordées aux PME;
- ✓ Rationaliser la gouvernance en accordant au Bureau de l'IA une surveillance accrue.

DIGITAL OMNIBUS

Pour un corpus réglementaire simplifié

Il est à noter que **l'Omnibus numérique** de novembre 2025 est accompagné de deux propositions supplémentaires « paquet numérique » (**Digital Package**) :

- **Stratégie de l'Union des données** pour améliorer l'accès à des données de qualité ;
- **Portefeuilles d'affaires européens** *(European Business Wallets)* pour simplifier les contraintes administratives et faciliter la conduite des affaires dans l'ensemble des États membres de l'UE.

Prochaines étapes, suite à la proposition d'Omnibus numérique par la Commission européenne :

- Examen par les co-législateurs (Parlement européen et le Conseil de l'UE)
- **Appel à contributions** ouvert du 19 novembre 2025 au 11 mars 2026

CYBERSECURITY PACKAGE

De nouvelles mesures européennes pour renforcer la résilience et les capacités en matière de cybersécurité

20 janvier 2026

Objectifs :

- Réviser le **Règlement sur la cybersécurité** *(Cybersecurity Act)*, afin de :
  - Simplifier le respect des règles de cybersécurité de l'UE et des exigences en matière de gestion des risques pour les entreprises exerçant leurs activités dans l'UE, en complément du point d'entrée unique pour la notification des incidents proposé dans le Digital Omnibus ;
  - Garantir que les produits et services numériques utilisés dans l'UE soient soumis à des tests de sécurité de manière plus efficace, en clarifiant les règles et en simplifiant les procédures dans le cadre du système européen de certification de cybersécurité.

- Apporter des modifications ciblées de la **Directive NIS 2** visant à notamment à organiser et faciliter la collecte de données sur les attaques par ransomware, ainsi que la surveillance des entités transfrontières, l'**ENISA** jouant un rôle de coordination renforcé.

CYBERSECURITY PACKAGE

20 janvier 2026

Propositions de modifications de NIS 2

Elle comprennent notamment :

- Introduction d'une nouvelle catégorie d'entreprises, l**es "Small Mid-caps" (Petites entreprises de taille intermédiaire) :** les entités qui dépasseraient les plafonds des PME mais resteraient sous une certaine taille (définie par une recommandation de la Commission de 2025) seraient soumises à des obligations allégées (en termes de conformité et de supervision) ;
- Pour faciliter la démonstration de la conformité, les entités pourront obtenir des **certificats dans le cadre de schémas européens de certification de cybersécurité** ;
- **Cryptographie post-quantique (PQC) :** Les États membres devront adopter des politiques de migration vers la cryptographie post-quantique au sein de leur stratégie nationale de cybersécurité, avec des objectifs de transition allant jusqu'en 2030 ou 2035 selon l'importance des cas d'usage ;
- **Signalement des ransomwares :** La proposition introduit une collecte de données harmonisée sur les attaques par rançongiciels (vecteur d'attaque, mesures d'atténuation prises, si une rançon a été payée, etc.)

Prochaines étapes, suite à la proposition, par la Commission européenne, du **Règlement révisé sur la cybersécurité** *(Cybersecurity Act 2)* et des modifications apportées à la **Directive NIS 2** : Examen par les co-législateurs Parlement européen et le Conseil de l'UE

Nouvelle boîte à outils pour renforcer la sécurité de la chaîne d'approvisionnement des TIC

13 février 2026

Contexte :

Le groupe de coopération NIS, composé de représentants des États membres de l'UE, de la Commission européenne et de l'Agence de l'UE pour la cybersécurité (ENISA), a adopté une **boîte à outils** *(toolbox)* pour la sécurité de la chaîne d'approvisionnement des TIC.

Nouvelle boîte à outils pour renforcer la sécurité de la chaîne d'approvisionnement des TIC

13 février 2026

La **boîte à outils** *(toolbox)* fournit une approche commune sur la **manière d'identifier, d'évaluer et d'atténuer les risques de cybersécurité des** chaînes d'approvisionnement en TIC.

Elle décrit également des scénarios de risque et recommande des mesures d'atténuation, y compris pour surmonter les risques liés aux dépendances à l'égard des fournisseurs à haut risque.

La boîte à outils aidera les États membres et les acteurs publics et privés à renforcer la sécurité des chaînes d'approvisionnement en TIC dans l'UE, comme le prévoit le Règlement révisé sur la cybersécurité présenté le 20 janvier 2026.

Cette boîte à outils est accompagnée de deux évaluations des risques concernant les **véhicules connectés et automatisés** et les **équipements de détection.**

1. EU ICT Supply Chain Security Toolbox — Download

2. Risk assessment - Connected and automated vehicles (CAV) — Download

3. Risk assessment - Detection equipment — Download

Nouvelle boîte à outils pour renforcer la sécurité de la chaîne d'approvisionnement des TIC

Recommendations
Robust framework for ICT supply chain risk management
R01. Establish and carry out ICT supply chain risk assessments
R02. Ensure a structured approach to ICT supply chain risk management
Flexible, diverse and resilient ICT supply chains
R03. Promote multi-vendor strategies and policies to address strategic dependency risks
R04. Manage and, if necessary, restrict or exclude high-risk suppliers at national level
Situational awareness and operational cooperation
R05. Promote information exchange, awareness, and training
A resilient, trusted and transparent industrial base
R06. Develop and support an interoperable ecosystem for secure supply chains
R07. Promote interoperability through the development and adoption of appropriate standards and certification

MATHIAS Avocats

20 ans d'expertise en droit du numérique

Mathias | Avocats

VOS FORMATIONS sur-mesure!

Mathias | Avocat

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

Objectifs :

- Savoir gérer les enjeux juridiques d'une crise, une réponse à incident
- Connaître les obligations légales et d'information des personnes
- Préparer votre organisme à gérer les crises

Compétences visées :

- Gérer les obligations, les délais en cas d'incidents (RGPD, NIS 2, DORA, etc.)
- Mettre en œuvre une politique de gestion des crises, de communication avec des bonnes pratiques
- Sensibiliser et former ses équipes

Pour qui ? Aucun prérequis

Toute personne concernée par la gestion de crise (RSSI, juriste, DPO, métier, etc.)

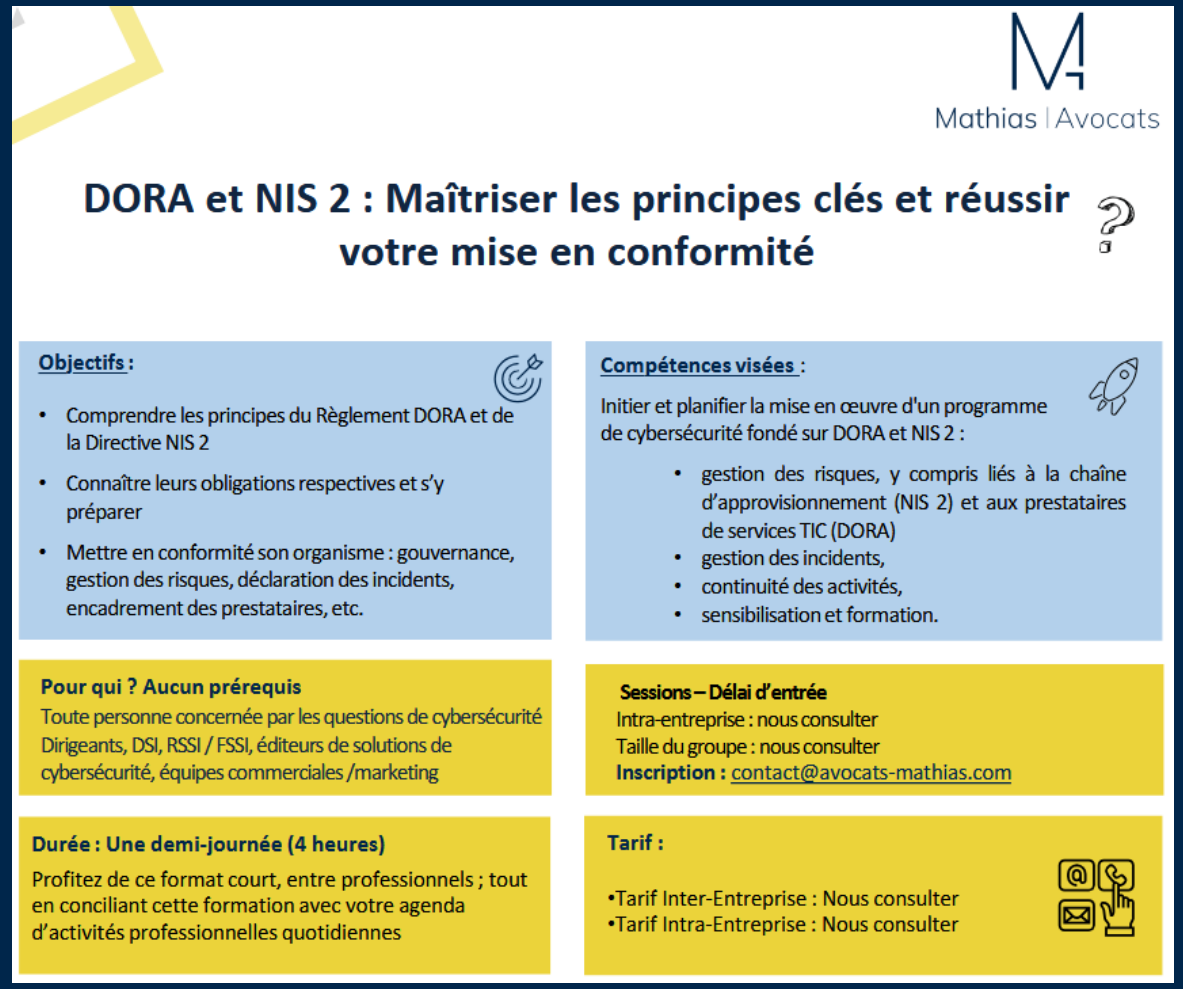
Sessions – Délai d'entrée

Intra-entreprise : nous consulter
Taille du groupe : nous consulter
Inscription : contact@avocats-mathias.com

Durée : 4 heures, en présentiel - continu

Profitez de ce format court et concis, entre professionnels ; tout en conciliant cette formation avec votre agenda d'activités professionnelles quotidiennes.

Tarif :
Stage / personne : sur devis
Option repas : sur demande
Conditions commerciales : nous consulter



Mathias | Avocats

DORA et NIS 2 : Maîtriser les principes clés et réussir votre mise en conformité

Objectifs :

- Comprendre les principes du Règlement DORA et de la Directive NIS 2
- Connaître leurs obligations respectives et s'y préparer
- Mettre en conformité son organisme : gouvernance, gestion des risques, déclaration des incidents, encadrement des prestataires, etc.

Compétences visées :

Initier et planifier la mise en œuvre d'un programme de cybersécurité fondé sur DORA et NIS 2 :

- gestion des risques, y compris liés à la chaîne d'approvisionnement (NIS 2) et aux prestataires de services TIC (DORA)
- gestion des incidents,
- continuité des activités,
- sensibilisation et formation.

Pour qui ? Aucun prérequis

Toute personne concernée par les questions de cybersécurité
Dirigeants, DSI, RSSI / FSSI, éditeurs de solutions de cybersécurité, équipes commerciales /marketing

Sessions – Délai d'entrée

Intra-entreprise : nous consulter
Taille du groupe : nous consulter
Inscription : contact@avocats-mathias.com

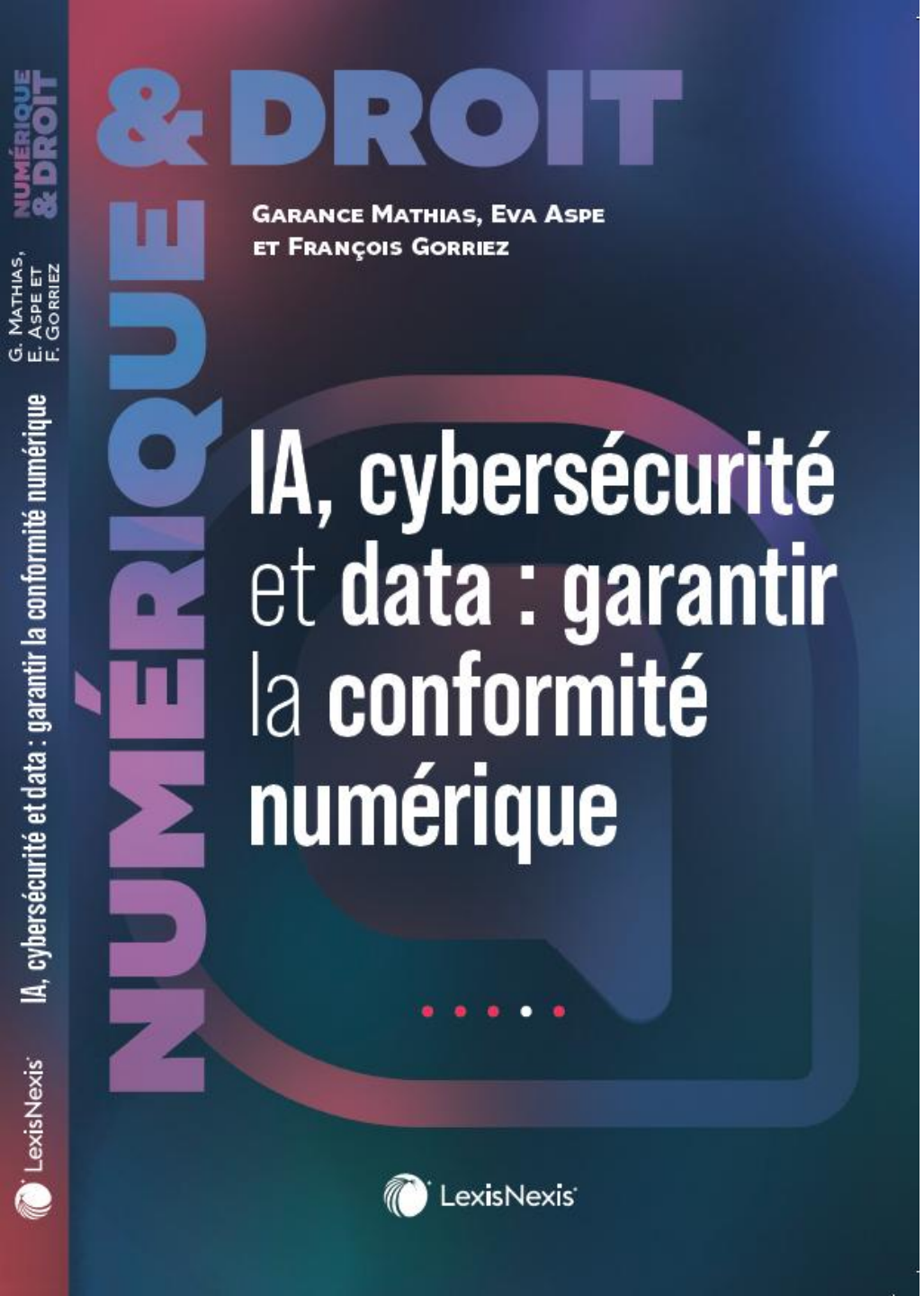
Durée : Une demi-journée (4 heures)

Profitez de ce format court, entre professionnels ; tout en conciliant cette formation avec votre agenda d'activités professionnelles quotidiennes

Tarif :

•Tarif Inter-Entreprise : Nous consulter
•Tarif Intra-Entreprise : Nous consulter

Catalogue des formations



Pour vous et vos équipes !

Paru en janvier 2026

Disponible en libraire ou sur commande

LexisNexis

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, la gestion de crise**, etc.). 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.

Mathias | Avocats

SUIVEZ VOTRE ACTUALITÉ, ABONNEZ-VOUS !

UNE NEWSLETTER MENSUELLE OFFERTE

Mathias | Avocats

JANVIER 2026

Newsletter

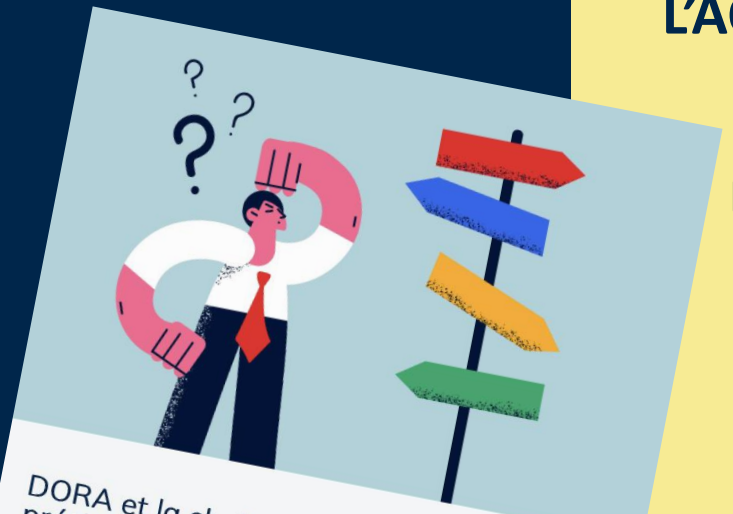
VOUS AVEZ PEUT-ÊTRE MANQUÉ...

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