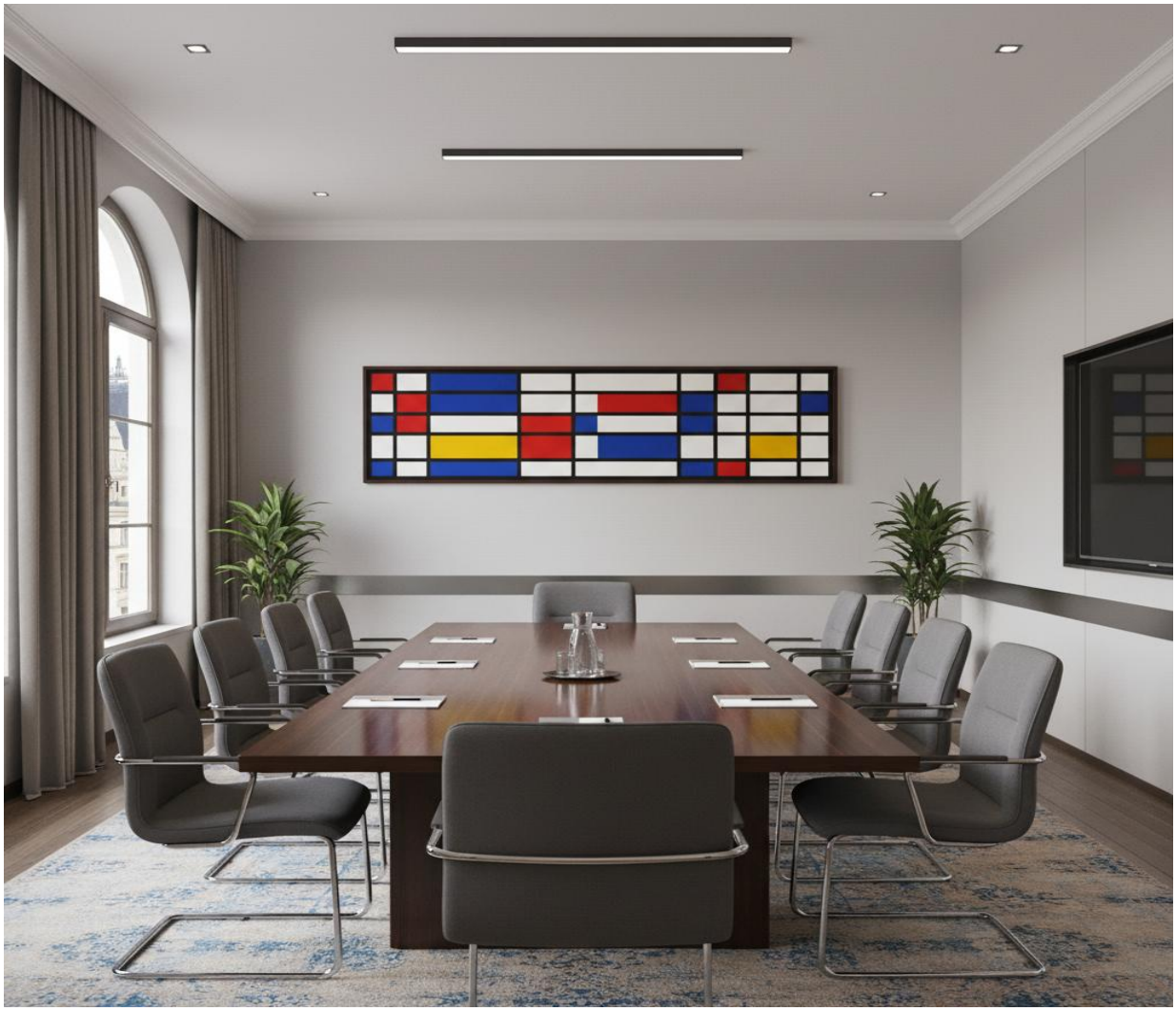
CATALOGUE DES FORMATIONS CYBERSECURITE 2026



Lexing
Société d'exercice libéral par actions simplifiée
58 boulevard Gouvion-Saint-Cyr 75017 Paris
Tél. : 01 82 73 05 05 - Mél : formation@lexing.law
Société d'avocats au capital de 10.936.190 euros - RCS PARIS 452 160 856
Siret : 452 160 856 00046 - TVA : FR 48 452 160 856 - APE N° 6910Z

Le mot du Président

Alain Bensoussan

Président fondateur du cabinet d'avocat Lexing et du réseau international d'avocats Lexing®

La cybersécurité est aujourd'hui le moteur de la confiance numérique et le pivot de la résilience opérationnelle. Véritable passeport stratégique pour les entités publiques et privées, elle s'affirme comme la condition essentielle à l'exercice de toute activité durable.

Désormais ancrée au cœur des exigences réglementaires et des relations contractuelles, elle garantit la fluidité des échanges, le respect des droits fondamentaux et la continuité de vos missions. Maîtriser ses enjeux, c'est transformer une norme de sécurité en un levier de performance pour évoluer avec assurance dans un environnement interconnecté.

Chez Lexing, nous sommes convaincus que la maîtrise du droit de la cybersécurité est indispensable pour accompagner l'innovation tout en sécurisant les infrastructures et les usages numériques. C'est pourquoi nous avons conçu un programme de formations spécialisées, destinées aux juristes, dirigeants, responsables conformité, DPO, RSSI et à tous les professionnels confrontés aux enjeux de la cybersécurité dans leur activité.

Ces formations offrent des outils concrets et une expertise pointue pour comprendre les nouvelles obligations, anticiper les cybermenaces et renforcer la protection des systèmes d'information dans un cadre conforme et responsable.

En vous formant aujourd'hui, vous préparez votre organisation aux défis de demain. Nous espérons que ce catalogue vous permettra de trouver la formation la plus adaptée à vos besoins.

INFORMATIONS PRATIQUES

Organisme de formation

Lexing est enregistré en tant qu'organisme de formation sous le numéro de déclaration d'activité (NDA) 11 75 38676 75. Cet enregistrement ne vaut pas agrément de l'Etat.

Les avocats formateurs, qui animent régulièrement des formations juridiques inter ou intra-entreprises, possèdent une expertise de haut niveau en droit de l'intelligence artificielle.

Moyens techniques

Les sessions de formation en présentiel au cabinet sont réalisées dans une salle de formation permettant d'accueillir un groupe de 15 stagiaires. La salle est équipée d'un vidéoprojecteur et d'un écran, ainsi que d'un accès Wi-Fi sécurisé.

Prérequis

Nos formations ne nécessitent pas de prérequis.

Démarche, outils pédagogiques et méthodes d'animation

La démarche de réalisation des sessions de formation suit les étapes suivantes :

1. Conception du support de formation
2. Animation de la formation par un avocat formateur
3. Évaluation des acquis des participants

La formation est dispensée en utilisant une variété d'outils pédagogiques et de méthodes d'animation destinés à favoriser l'apprentissage et l'engagement des participants. Ces outils comprennent :

- un support de formation servant de fil conducteur tout au long de la session, incluant, selon le cas, des études de cas pratiques, des fiches réflexes, des résumés des concepts clés et des règles applicables, ainsi qu'une sélection de références et ressources complémentaires (telle qu'une bibliographie sélective d'ouvrages et d'articles spécialisés) ;
- des discussions et échanges encourageant la participation active de chacun et favorisant la mise en commun des connaissances et des expériences entre les participants et le formateur ;
- un dossier pédagogique remis à chaque participant comprenant un recueil de textes de loi et de décisions de justice et un glossaire des termes techniques du Règlement sur l'intelligence artificielle à vocation juridique.

Modalités d'évaluation des acquis

Les modalités d'évaluation des acquis sont les suivantes :

- Un questionnaire d'autoévaluation pour consolider les acquis
- Un questionnaire de satisfaction « à chaud », distribué immédiatement après la formation, permettant de recueillir les impressions et suggestions des participants sur l'animation, le contenu et les supports utilisés
- Un questionnaire de satisfaction « à froid », envoyé plusieurs semaines ou mois après la formation, afin d'évaluer l'impact concret de la formation sur la pratique professionnelle des participants et d'identifier d'éventuels besoins de formation complémentaires

Modalités d'inscription

Pour vous inscrire :
E-mail: formation@lexing.law
Téléphone : 01 82 73 05 05

Modalités d'inscription, d'annulation et de report : consulter les conditions générales de vente **ici**

Accessibilité : Si vous avez besoin d'une adaptation, contactez-nous.

Tarifs

900 euros HT par participant, pour une formation d'une demi-journée (3 heures) en présentiel, à distance ou en mode hybride.

2.000 euros HT par participant pour une formation d'une journée (6 heures) en présentiel, à distance ou en mode hybride (hors déjeuner, frais de déplacement et d'hébergement).

Modalités de suivi de l'exécution et de l'assiduité

Les modalités de suivi sont les suivantes :

- Feuille d'émargement
- Attestation de suivi de formation

Renseignements pratiques

Durée et lieu : la formation, d'une journée ou d'une demi-journée peut se dérouler en présentiel dans les locaux du cabinet, dans ceux du client, à distance via Google Meet ou Microsoft Teams ou sous forme hybride, combinant les deux modalités.
Dans le cas d'une formation dispensée pour plusieurs clients (formation interentreprises), celle-ci se déroule nécessairement soit dans les locaux du cabinet, soit à distance, soit en mode hybride.

Règlement intérieur ici

Adresse du cabinet : Lexing, 58 boulevard Gouvion Saint-Cyr 75017 Paris (3e étage)

Moyens de transport :
Métro : ligne 1 Porte Maillot
RER : lignes C et E Neuilly Porte Maillot
Tramway : T3 Porte Maillot

Stations de bus et de Vélib'

Stations de recharge pour véhicules électriques et parkings publics situés à proximité

FORMATEURS

Alain Bensoussan

Président fondateur du cabinet d'avocats Lexing

Alexandra Massaux

Avocate, Directice du département Technologies émergentes Contentieux

Anthony Coquer

Expert, cybersécurité et IA, Directeur général de Lexing Technologies

Katharina Berbett

Avocate, Directrice du département Informatique contentieux complexe

Marion Catier

Avocate, Directice du département Données personnelles Contentieux

Raphaël Liotier

Avocat, Directeur du département Droit pénal de l'informatique et du numérique

Virginie Bensoussan-Brulé

Avocate, Directrice du pôle Contentieux du numérique

Sommaire des formations

La gestion de crise et la réponse à une cyberattaque

Raphaël Liotier

Raphaël Liotier est avocat à la Cour d'appel de Paris et directeur du département droit pénal de l'informatique et du numérique du cabinet Lexing.

Objectifs

- Anticiper et organiser la réponse à une cybercrise
- Gérer l'incident de l'identification à la résolution en protégeant les preuves
- Garantir la conformité réglementaire et piloter une communication interne et externe adaptée

Outils

- Support de formation
- Dossier pédagogique

Participants

- Responsables juridiques
- Juristes d'entreprise
- Délégués à la Protection des Données (DPO)
- Juristes conformité
- Directeur des systèmes d'information (DSI)
- Responsables de la sécurité des systèmes d'information (RSSI)
- Consultants en cybersécurité
- Avocats

PROGRAMME DE LA FORMATION

APPROCHE GÉNÉRALE

Préambule
Objectifs pédagogiques de la formation (apports théoriques, études de cas pratiques et échange interactifs avec les participants)

PREPARATION ET ANTICIPATION DE CRISE

Gouvernance de crise et rôles clés
Organisation de la cellule de crise

PRÉPARATION AUX SCENARIOS

Exercices de simulation de crise
Mise en situation

OBLIGATIONS JURIDIQUES ET REGLEMENTAIRES

Notification aux autorités compétentes
Informations des personnes concernées
Gestion des relations avec les tiers

COMMUNICATION DE CRISE

Communication interne
Communication externe
Gestion des médias et réseaux sociaux
Validation juridique des messages diffusés

IA et cybercriminalité : aspect juridiques

Virginie Bensoussan-Brulé

Virginie Bensoussan-Brulé est avocate à la Cour d'appel de Paris et dirige le pôle Contentieux du numérique du cabinet Lexing spécialisé en droit de la presse, droit pénal du numérique, contentieux de l'Internet et droit des données personnelles. Reconnue internationalement pour son expertise en droit du numérique, elle est distinguée dans plusieurs classements juridiques, dont Best Lawyers et Legal 500. Elle intervient également dans la formation et l'enseignement en droit du numérique, cybersécurité et de la protection des données.

Objectifs

- Comprendre les usages malveillants de l'IA en cybersécurité et leurs enjeux juridiques et éthiques
- Connaître le cadre pénal des atteintes aux STAD et les risques associés
- Identifier les procédures judiciaires, les acteurs et les règles de preuve

Outils

- Support de formation
- Dossier pédagogique

Participants

- Responsable juridique/juriste d'entreprise
- Juriste en administration et en collectivité territoriale
- Délégué à la protection des données
- Juriste conformité
- DSI/ RSSI

PROGRAMME DE LA FORMATION

APPROCHE GÉNÉRALE

Panorama des cybermenaces et des formes de cybercriminalité
La et cybersécurité : nouvelles opportunités et nouveaux risques
Présentation des ressources institutionnelles

L'IA ET CYBERCRIMINALITE

Automatisation des attaques via l'intelligence artificielle
Deepfakes et manipulation de l'information et des marches
Ingénierie sociale renforcée par l'IA (phishing, faux profils, voix synthétiques)

INFRACTIONS AUX STAD

Définition et cadre légal (art. 323-1 à 323-8 du code pénal)
Atteintes aux systèmes de traitement automatise de données (STAD)
Principales infractions pénales liées à la cybercriminalité
Risques pour l'entreprise : impact financier, juridique et réputationnel
Responsabilité liée a la sécurisation des systèmes d'information

REPONSE JUDICIAIRE

Acteurs spécialises de la cybercriminalité et coopération internationale
Procédures de dépôt de plainte et suites judiciaires
Prescription des infractions cyber
Accès à la preuve numérique : OSINT, analyse des fuites de données
Investigations numériques, réquisitions et saisies de données

La recherche de fuites d'informations (OSINT) dans le respect du RGPD et de la loi

Raphaël Liotier

Raphaël Liotier est avocat à la Cour d'appel de Paris et directeur du département droit pénal de l'informatique et du numérique du cabinet Lexing.

Objectifs

- Maîtriser le cadre pénal encadrant l'OSINT
- Réaliser des recherches d'informations dans le respect du droit de la protection des données à caractère personnel
- Sécuriser les données collectées et identifier les limites légales pour prévenir les risques

Outils

- Support de formation
- Dossier pédagogique

Participants

- Responsables juridiques
- Juristes d'entreprise
- Délégués à la Protection des Données (DPO)
- Responsables de la sécurité des systèmes d'information (RSSI)
- Consultant en cybersécurité
- Avocats

PROGRAMME DE LA FORMATION

APPROCHE GÉNÉRALE

Préambule
Objectifs pédagogiques de la formation (alternance théorie et mise en pratique, échanges)

CADRE DE L'INVESTIGATION EN SOURCE OUVERTES

Définition et limites de l'OSINT loyauté de la preuve

CADRE PÉNAL DE L'OSINT

Atteintes aux systèmes de traitement automatisé (STAD) usurpation d'identité et avatars d'enquête
Atteintes à la vie privée et secret des correspondances

PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

Conformité RGPD
Mise en place du traitement

LA MISE EN PLACE DE LA RECHERCHE EN SOURCE OUVERTE

Méthodes de capture et préservation
Outils d'investigation et sécurité de l'enquêteur

GESTION DE LA PREUVE NUMÉRIQUE

Chaîne de traçabilité et intégrité des données
Force probante : captures, logs et constats

DE LA RECHERCHE À L'ACTION JURIDIQUE

Rédaction de rapports factuels exploitables
Emploi au support d'actions judiciaires

Cyberattaques et violation de données à caractères personnel

Marion Catier

Marion Catier est avocate à la Cour d'appel de Paris et directrice du département Données personnelles Contentieux du cabinet Lexing.

Objectifs

- Comprendre et qualifier une violation de données à caractère personnel conformément au cadre du RGPD
- Mettre en œuvre les procédures de gestion de crise, de notification et de sécurisation
- Identifier les risques cyber et adopter les bons réflexes juridiques, techniques et organisationnels

Outils

- Support de formation
- Dossier pédagogique

Participants

- Directeur des systèmes d'information (DSI)
- Responsable Sécurité des Systèmes d'Information (RSSI)
- Consultant en cybersécurité
- Délégués à la protection des données (DPO)
- Juristes d'entreprises
- Juristes conformité
- Responsables juridiques
- Avocats spécialisés en droit du numérique ou du contentieux

PROGRAMME DE LA FORMATION

APPROCHE GÉNÉRALE

Préambule
Objectifs pédagogiques de la formation (alternance théorie et mise en pratique, échanges)

LE CADRE JURIDIQUE RGPD

Principe : licéité, finalité, minimisation, sécurité
Définition juridique
Distinction violation/incident de sécurité
Responsabilité du responsable de traitement
Obligations du sous-traitant

IDENTIFICATION ET EVALUATION DU RISQUE

Détection d'un incident cyber
Typologie des atteintes : confidentialité, intégrité, disponibilité
Analyse des données impactées
Volume et sensibilité des données
Critère d'évaluation du risque et qualification

GESTION OPERATIONNELLE DE CRISE

Activation cellule de crise
Mesures conservatoires immédiates
Isolation des systèmes / comptes compromis
Sécurisation des accès et journaux
Investigation technique et forensique
Traçabilité et conservation des preuves

NOTIFICATION ET COMMUNICATION

Notification sous 72h à la Cnil
Informations des personnes concernées
Contenu minimal obligatoire
Communication interne et externe maitrise

RISQUES JURIDIQUES ET CONTENTIEUX

Sanctions par le RGPD
Amendes et mises en demeure
Responsabilité civile et pénale
Gestion des relations contractuelles en cas d'incident

PREVENTION ET GOUVERNANCE

Plan de continuité et de reprise d'activité
Renforcement des mesures techniques et organisationnelles
Retours d'expérience

La directive NIS 2 : Mise en conformité, mode d'emploi

Raphaël Liotier

Raphaël Liotier est avocat à la Cour d'appel de Paris et directeur du département droit pénal de l'informatique et du numérique du cabinet Lexing.

Objectifs

- Comprendre les enjeux stratégiques et les obligations réglementaires liées à la directive NIS 2
- Elaborer et déployer un plan de mise en conformité Cyber
- Maintenir une conformité durable et valoriser les bénéfices organisationnels

Outils

- Support de formation
- Dossier pédagogique

Participants

- Directeur des systèmes d'information (DSI)
- Responsables de la sécurité des systèmes d'information (RSSI)
- Consultant en cybersécurité
- Juristes d'entreprise
- Délégués à la protection des données (DPO)
- Avocats

PROGRAMME DE LA FORMATION

APPROCHE GÉNÉRALE

Préambule
Objectifs pédagogiques de la formation (alternance théorie et mise en pratique, échanges)

DIRECTIVE NIS 2 : ENJEUX ET OBLIGATIONS

Contexte règlementaire européen de la cybersécurité
Identification des entités concernées
Exigences en matière de gouvernance
Gestion des risques et obligation de notification des incidents

PLAN DE MISE EN CONFORMITE

Élaboration d'un plan d'action cybersécurité et opérationnel
Déploiement de solutions techniques, organisationnelles et humaines
Gestion des incidents : détection, confinement et réponse
Intégration des exigences sécurité dans la chaîne d'approvisionnement

CONTROLES ET SANCTIONS

Pouvoir de supervision des autorités nationales
Régime des amendes administratives

ACTION DE VEILLE ET DE FORMATION

Formation et sensibilisation des dirigeants et des collaborateurs aux bonnes pratiques cyber
Veille réglementaire

Le règlement européen DORA : Mise en conformité, mode d'emploi

Alexandra Massaux - Anthony Coquer

En coanimation par Anthony Coquer, expert cybersécurité et IA, et Alexandra Massaux, avocat à la Cour d'appel de Paris et directice du département Technologies émergentes Contentieux du cabinet Lexing.

Objectifs

- Comprendre les enjeux stratégiques, le périmètre d'application et les obligations du règlement DORA
- Mettre en place un plan opérationnel de mise en conformité adapté aux risques liés à la résilience numérique
- Assurer une conformité durable et valoriser les bénéfices de la sécurité financière et informatique

Outils

- Support de formation
- Dossier pédagogique

Participants

- Directeur des systèmes d'information (DSI)
- Responsable de la sécurité des systèmes d'information (RSSI)
- Consultant en cybersécurité
- Juristes d'entreprise
- Responsables de la conformité
- Avocats

PROGRAMME DE LA FORMATION

APPROCHE GÉNÉRALE

Préambule
Recueil des attentes des participants
Présentation des objectifs de la formation

REGLEMENT DORA : LES CINQ, PILIERS

Gouvernance et gestion des risques TIC
Identification continue des risques TIC
Définition d'une stratégie cybersécurité adaptée
Mise en place de politiques et procédures de sécurité
Surveillance et contrôle des risques technologiques
Communication efficace sur les risques organisationnels

TEST DE RESILIENCE OPERATIONNELLE

Réalisation de tests de résistance des systèmes
Vérification des capacités de reprise d'activité
Simulation de perturbations majeures
Contrôle de la continuité des services critiques

GESTION DES INCIDENTS TIC

Détection et analyse des incidents de cybersécurité
Organisation des procédures de gestion des incidents
Notification des incidents aux autorités compétentes
Amélioration continue des dispositifs de sécurité

EXTERNALISATION DES FONCTIONS CRITIQUES

Évaluation des risques lies aux prestataires TIC
Sélection de fournisseurs fiables et sécurises
Surveillance des activités externalisée
Plan de continuité en cas de défaillance fournisseur

PARTAGE D'INFORMATIONS CYBER

Échange d'informations sur les menaces et incidents
Diffusion des indicateurs de compromission
Suivi des vulnérabilités émergentes
Promotion des bonnes pratiques cybersécurité

Cyber Resilience Act (CRA) : guide pratique pour réussir sa mise en conformité

Katharina Berbett - Anthony Coquer

En coanimation par Anthony Coquer, expert cybersécurité et IA, et Katharina Berbett, Avocate, Directrice du département Informatique contentieux complexe du cabinet Lexing.

Objectifs

- Comprendre le champ d'application du Cyber Resilience Act et classer les produits numériques selon leur criticité ;
- Intégrer les principes de security by design et réaliser une analyse des risques conforme aux exigences réglementaire
- Structurer la conformité technique et opérationnelle : évaluation, dossier technique, gestion du cycle de vie et obligation de notification

Outils

- Support de formation
- Dossier pédagogique

Participants

- Responsables juridiques
- Juristes d'entreprise et conformité
- Délégués à la Protection des Données (DPO)
- Direceur des systèmes d'information (DSI)
- Responsables de ma sécurité des systèmes d'information (RSSI)
- Consultat en cybersécurité
- Avocats

PROGRAMME DE LA FORMATION

APPROCHE GÉNÉRALE

Préambule
Présentation des objectifs de la formation
Programme de la journée (alternance entre apports théoriques, échanges, études de cas et mises en pratique)

CYBER RESILIENCE ACT : ENJEUX ET PERIMETRE

Contexte réglementaire
Cadre européen du marché numérique
Articulations avec NIS 2, RIA, DORA et Data Act
Objectifs du CRA : renforcer la cybersécurité par conception
Produits concernes : produits intégrant des éléments numériques
Acteurs vises : fabricants, importateurs, distributeurs
Exclusions sectorielles prévues par le règlement

CLASSIFICATION ET EXIGENCES DE SECURITE

Cartographie
Classification selon le niveau de risque cyber
Produits non critiques ? Classe i et classe ii
Security by design : protection des systèmes dès la conception
Gestion des vulnérabilités : mise à jour, correctifs et support sécurité

MISE EN CONFORMITE CRA

Obligations du fabricant
Choix de la procédure de conformité
Constitution du dossier technique et déclaration UE
Analyse des risques intégrée a la conception
Notification des vulnérabilités aux autorités compétentes
Définition du cycle de vie et du support produit

IMPACT CHAINE DE VALEUR

Vérification du marquage ce
Intégration du CRA dans les contrats fournisseurs
Transmission des obligations aux sous-traitants
Régime de sanctions administratives
Élaboration d'une feuille de route de conformité

Legal Risk Management : anticiper, évaluer et maitriser les risques liés aux technologies

Alain Bensoussan – Anthony Coquer

En coanimation par Anthony Coquer , expert cybersécurité et IA et Alain Bensoussan, Président fondateur du cabinet d'avocats Lexing.

Objectifs

- Identifier et cartographier les risques liés aux projets technologiques et numériques ;
- Construire une cartographie des risques et définir des stratégies de traitement adapté ;
- Intégrer une approche « Legal by Design » dans les processus de l'entreprise.

Outils

- Support de formation
- Dossier pédagogique

Participants

- Juristes d'entreprise
- Responsables juridiques
- Délégué à la protection des données
- Juristes conformité

PROGRAMME DE LA FORMATION

APPROCHE GÉNÉRALE

Préambule
Risque juridique amplifié par la digitalisation
Cycle de gestion de risque : identification, évaluation, traitement et suivi
Rôle du juriste
Prise en compte des enjeux de vitesse, dématérialisation et d'internationalisation

CARTOGRAPHIE DES RISQUES TECHNOLOGIQUES

Déploiement d'une démarche structurée et cartographie des risques
Implication des métiers
Risques liés aux données : conformité, RGPD et cybersécurité
Risques contractuels : cloud, développement logiciel et licences
Risque de pro
Risque de propriété intellectuelle : code source, bases de données et innovation
Risques des interfaces numériques : contenus, CGV, cookies et responsabilité

TRAITEMENT DU RISQUE

Évaluation selon probabilité et impact
Reduction du risque par le contrat ou l'organisation interne
Transfert du risque via assurance cyber ou sous-traitance
Décision d'accepter ou d'éviter le risque résiduel

INNOVATION ET CONFORMITE CONTINUE

Intégration du « Legal by design » dans les projets
Analyse des enjeux juridiques de l'intelligence artificielle et de la blockchain
Usage d'outils numériques pour le pilotage de la conformité