

## Prévenir et gérer des risques juridiques et mettre en oeuvre des procédures de mise en conformité – Parcours 4 jours

Cette formation vise le bloc 3 de la certification RNCP39587 enregistrée auprès de France Compétence par HEAD.

Code  
**703028**

Durée  
**4**  
jours

Tarif Inter\*  
**3 990 €**  
HT

*\*Repas inclus (en présentiel)*

### PUBLIC

Compliance officers en fonction ou en devenir – Directeurs juridiques – Responsables juridiques – Juristes – Risk managers

### PRÉ-REQUIS

Etre titulaire d'une certification de niveau 6 minimum – Sélection sur dossier et test d'admission

### LES POINTS FORTS

Parcours Eligible CPF.

Nos parcours sont composés de formations cohérentes et complémentaires dispensées par des experts et praticiens d'entreprise pour découvrir, approfondir et valider savoir-faire et compétences. Nous vous accompagnons dès le début en veillant à ce que les objectifs du parcours soient en adéquation avec vos attentes puis tout au long de votre formation avec des échanges personnalisés

### MOYENS PÉDAGOGIQUES

- Dispositif de formation structuré autour du transfert des compétences
- Acquisition des compétences opérationnelles par la pratique et l'expérimentation
- Apprentissage collaboratif lors des moments synchrones
- Parcours d'apprentissage en plusieurs temps pour permettre engagement, apprentissage et transfert
- Formation favorisant l'engagement du participant pour un meilleur ancrage des enseignements

### SATISFACTION ET EVALUATION

- Le parcours fera l'objet d'une évaluation des compétences portant sur l'élaboration d'un dossier écrit de synthèse juridique et d'analyse des risques sur la base des pratiques juridiques d'une entreprise réelle.
- Le dossier de synthèse juridique et d'analyse des risques contient :

## Objectifs pédagogiques

- Décrire l'évolution du cadre juridique et le champ d'application du devoir de vigilance
- Déployer un programme de compliance au sein de sa structure
- Déterminer les obligations techniques et organisationnelles des entités concernées par le RGPD

## Programme de la formation

### Engagement

Vous vous engagez dans votre formation. Connectez-vous sur votre espace participant et complétez votre questionnaire préparatoire. Votre formateur reçoit vos objectifs de progrès.

Devoir de vigilance : les nouvelles exigences de la CS3 (1 jour)

### Décrire l'évolution du cadre juridique et le champ d'application du devoir de vigilance

Expliquer l'évolution du cadre juridique du devoir de vigilance en France et en Europe

- Genèse du devoir de vigilance (Rana Plaza, UNGPs, principes directeurs de l'OCDE)
- Processus d'adoption et rappel du cadre réglementaire européen (Green Deal)
- Distinction des autres normes de durabilité (CSRD, SFDR, Taxinomie)
- Différences et articulation avec la loi française
- Mur d'images : Lien entre vigilance, reporting, « duty of care » et autres notions juridiquesEtat des lieux des contentieux français et à l'étranger

Définir le champ d'application du devoir de vigilance européen

- Sociétés concernées
- Portée extraterritoriale : sociétés étrangères avec seuil de CA
- Application sur une base consolidée, filiales et exonération, cas des holdings non opérationnelles

- ▶ La synthèse de l'audit et la cartographie de pratiques à risque de l'entreprise (comme les comme les non-conformités RSE et RGPD),
- ▶ La présentation et l'analyse des documents afférents (le règlement intérieur, la charte informatique, la politique de protection des données personnelles, les procédures d'alertes, les chartes éthiques, guides de bonnes pratiques, clauses contractuelles...) comportant des propositions de modification ou d'adaptations des documents.
- Taux de réussite global à la certification : 100%
- La réussite à l'épreuve certificative permet la validation du bloc 3 de la Certification RNCP39587 "Juriste d'Affaires". Attention un bloc ne constitue pas une certification. Pour obtenir la certification du titre RNCP39587 "Juriste d'Affaires", il faut valider ses 5 blocs

### ACCOMPAGNEMENT FORMATION À DISTANCE

En cas de nécessité, une assistance technique et pédagogique est joignable entre 8h30 et 18h (jours ouvrés):

- par téléphone : 01 83 10 10 10
- par mail : [care-formation@lefebvre-dalloz.fr](mailto:care-formation@lefebvre-dalloz.fr)

Une réponse immédiate est apportée ; si besoin, le demandeur est mis en relation avec un expert dans un délai maximum de 48h.

- Périmètre de la vigilance : activités et secteurs concernés, définition et périmètre des chaînes d'activités, partenaires commerciaux directs et indirects
- Calendrier progressif de mise en application

## Analyser l'approche de la vigilance de la CS3D

- Une approche centrée sur les risques
- Caractéristiques des atteintes et dommages : potentiels et actuels, atteintes graves
- Définition des atteintes aux droits humains, environnementaux et sociaux par référence au droit international
- Inclusion des manquements directs aux droits protégés lorsqu'ils sont prévisibles au regard des activités, du secteur économique, géographique et opérationnel de l'entreprise
- Dispositions spécifiques relatives aux atteintes aux droits des personnes vulnérables, droits des peuples autochtones, aux droits à un salaire décent, santé environnementale, droit à un environnement sain
- Cas des conflits armés : due diligence renforcée (convention de Genève et conventions internationales), exonération pour l'export autorisé par les Etats
- Quiz de synthèse sur le cadre réglementaire et le champ d'application de la directive CS3D

## Expliquer la méthodologie de la démarche de vigilance

### Distinguer les 8 étapes essentielles de la procédure

- Intégration dans la stratégie et la politique de gestion des risques de l'entreprise
- Identification et cartographie des risques : évaluation et priorisation des risques potentiels et actuels
- Matrice de priorités
- Prévention et remédiation
- Obligation de mettre un terme aux risques potentiels et actuels
- Obligation de réparer les conséquences des atteintes avérées
- Consultation des parties prenantes à tous les stades du process de vigilance
- Suivi du caractère approprié et de l'efficacité des mesures
- Obligation de publicité annuelle, déclaration de vigilance et lien avec la CSRD

### Analyser la nature des obligations

- Obligation de moyen ou de résultat
- Charge de la preuve : des obligations progressives selon le caractère des dommages
- Intégration des principes de due diligence des UNGPs et OCDE
- Prise en compte du pouvoir d'influence de l'entreprise
- Distinction des mesures entre dommages potentiels et dommages actuels ou avérés
- Définition des mesures de prévention et de limitation des atteintes graves potentielles
- Etude comparative de plans de vigilance

## Inscrire le devoir de vigilance dans la stratégie et la gouvernance de l'entreprise

### Plan de transition climatique conforme à l'Accord de Paris

- Objectifs climatiques court et moyen terme : neutralité carbone en 2050, « Loi climat européenne »
- Calculer et reporter les émissions de GHG : scopes 1, 2 et émissions indirectes (scope 3)
- Obligation d'adoption et de conception d'un plan de transition ; nature de l'obligation « through best efforts »
- Obligation de mise en œuvre : quel contrôle et quelles sanctions ?
- Lien avec le plan de transition climatique de la CSRD
- Cas pratique : Elaborer son plan de transition climatique / analyse des objectifs et trajectoires compatibles avec la limitation du réchauffement à 1,5°visée par la CSRD

### Devoir de vigilance, stratégie et gouvernance de l'entreprise

- Codes de conduite et engagements contractuels : effets sur la stratégie et la gouvernance de l'entreprise
- Intégration de la due diligence au sein des organes de direction et d'administration
- Conséquences de la CS3D sur l'organisation interne des directions de l'entreprise

### Autorité administrative de supervision : risques juridiques et sanctions

- Autorité compétente en France, réseau de superviseurs et coopération européenne
- Saisine et procédure devant l'autorité de supervision
- Pouvoir d'investigation et de contrôle sur place, auditions de parties prenantes
- Pouvoir d'injonction administrative et mesures provisoires
- Pouvoir d'amende
- Principe de responsabilité civile
- Possibilité de cumul des recours judiciaires et administratifs
- Voies de recours et compétence des juridictions françaises pour les entreprises ayant leur siège en France
- Les risques d'autres sanctions
- Retour d'expérience : analyse de contentieux ESG et information de durabilité
- Débat : la responsabilité des dirigeants et des administrateurs en matière d'information de durabilité et de vigilance

### Devoir de vigilance et réglementations sectorielles européennes

- Déforestation importée : principales dispositions du règlement européen
- Autres réglementations sectorielles (minerais, bois, batteries, travail forcé)
- Règle de conflits entre CS3D et réglementations sectorielles

## Mesurer l'opportunité d'adopter une démarche compliance

### Situer le contexte de la compliance

- Distinction des notions de compliance, conformité et risque de non-conformité
- Définition de la fonction-clé de Chief compliance officer
- Standards et normes de conformité
- Interactions entre compliance et fonctions juridiques
- Brainstorming : la compliance, c'est quoi ?

### Intégrer les enjeux et bénéfices d'une démarche de compliance

- La compliance pour qui : des grands groupes aux PME, les secteurs et entreprises les plus concernés
- Les acteurs majeurs d'une démarche de compliance
- La compliance pour quoi : des principes généraux au ROI
- Partage d'expériences : les facteurs clés de succès indispensables pour une démarche de compliance réussie

## Déployer un programme de compliance au sein de sa structure

### Délimiter le périmètre d'intervention de la compliance

- Le spectre commun d'intervention de la compliance
- La sécurité financière : lutte anti blanchiment et financement du terrorisme, lutte contre la fraude, etc
- La protection des intérêts de la clientèle et le devoir de conseil L'éthique et la déontologie
- Les prestations essentielles externalisées : gestion des sous-traitances importantes ou critiques
- La réglementation informatique et libertés et la gestion des données personnelles
- Le droit de la concurrence
- Les reporting extra-financiers
- Atelier « Délimiter le périmètre d'intervention de la compliance » :
- Études de cas : analyser en groupe les outils relatifs à la sécurité financière (lignes directrices, guides de bonne conduite...), un plan de vigilance, un rapport de gestion d'entreprises données et un exemple de lettre d'engagement dans le cadre d'un reporting extra-financier
- Autodiagnostic : autoévaluer le risque de corruption au sein de son entreprise grâce au questionnaire AFA

### Appliquer la méthodologie de déploiement d'un programme de compliance

- Positionnement de la compliance dans la gouvernance et la maîtrise des risques (composantes fonctionnelles et organisationnelles)
- Délimitation du cadre et des principes du programme



- Définition d'une stratégie globale de conformité grâce aux méthodes existantes (ISO 19600:2014 méthodologie opérationnelle, taxonomie des risques) Cartographier et évaluer les risques de non-conformité
- Élaboration d'un programme de conformité : appétence au risque, plan de conformité
- Suivi des actions correctives
- Atelier « Appliquer la méthodologie de déploiement d'un programme de conformité » :
- Études de cas : analyser les trois livrables indispensables (un exemple de cartographie du risque de corruption, programmes de conformité et politiques de conformité)
- Débriefing : faire une revue des différents organigrammes possibles

## Manager le dispositif de conformité déployé

### Mettre en place les mécanismes de suivi nécessaires

- Indicateurs de conformité (KPI, KRI, KCI)
- Reportings
- Tableau des risques opérationnels
- Cas pratique : faire une lecture critique des tableaux de bord présentés

### Sélectionner les outils de conformité adéquats

- GRC
- « Comitologie »
- Référentiel des obligations réglementaires
- Base incidents
- Relais conformité
- Registre des conflits d'intérêts
- Veille interne et externe
- Brainstorming : quels outils privilégieriez-vous dans la mise en œuvre de votre futur programme de conformité ?

### Diffuser une culture de conformité et de gestion du changement

- États des lieux et statistiques
- Outils de diffusion
- Formation des opérationnels : FPC, documents internes, newsletters...
- Débriefing : comment mettre en œuvre la conformité au quotidien et se positionner en tant que Compliance officer ?

Protection des données personnelles : mise en conformité (1 jour)

## Déterminer les obligations techniques et organisationnelles des entités concernées par le RGPD

### Rappeler le champ d'application, les objectifs et les enjeux du RGPD

- Origine de la directive 95-46 et de la loi Informatique et Libertés et philosophie du RGPD

- Critères d'application territoriale et personnelle
- Acteurs et responsabilités : coresponsabilité des clients et prestataires
- Débat : quelle impact de la suppression des formalités et autorisations par la création du "Guichet unique"

### Définir les concepts et principes

- Notions de donnée, traitement, finalité, base légale, responsable de traitement, sous-traitant, destinataire, profilage, etc.
- Comment qualifier les protagonistes (responsables de traitement, sous-traitants...) ?
- Principes de licéité/loyauté de la collecte, limitation des finalités, minimisation/exactitude et conservation limitée des données, confidentialité, proportionnalité, responsabilité, transparence, et sécurité des traitements...
- Focus sur le consentement
- Eprivacy : spécificités des données de communications électroniques, cookie consent
- Etude de cas : l'exploitation de données à des fins de prospection marketing ou commerciale

### Identifier les contraintes techniques et organisationnelles

- Cartographie des traitements, des finalités, des bases légales et des durées de conservation
- Protection structurelle des données, les exigences « Privacy by Design »
- Sécurité des données : mesures de sécurité logicielle/physique (pseudonymisation, certifications, plan d'assurance sécurité)
- Gestion d'une violation de données personnelles
- Analyses d'impact préalable
- Adoption d'une gouvernance interne et sensibilisation des équipes
- Procédures de conformité : gestion des demandes des droits, des violations de données et des AIDP et communiquer auprès des personnes concernées
- Cas pratique : adopter une démarche projet pour instruire et déployer la conformité RGPD

## Définir le rôle pour le délégué à la protection des données (DPD/DPO)

### Repérer les raisons de nommer un DPO

- Prévenir les risques et sanctions : amendes/CA, actions des personnes concernées, condamnation et préjudices
- Fonction quasi-obligatoire dans l'entreprise
- Débat : quel intérêt de nommer un DPO ?

### Mesurer les fonctions du DPO dans l'entreprise

- Tenir le registre
- Limiter les mises en cause de responsabilité
- Expliquer ses missions
- Partage d'expériences : le rôle du DPO

## Cerner les obligations juridiques

### Informez les personnes concernées et gérez leurs droits

- Conception des mentions d'information
- Déploiement des mentions d'information et modalités de recueil des consentements des personnes
- Cas pratique : comment instruire des demandes d'exercice des droits des personnes concernées ?

### Gérer la conformité RGPD sur le plan contractuel

- Thématiques contractuelles
- Clauses et annexes du RGPD
- Exercice pratique : qualifier les protagonistes des relations complexes et en cerner les conséquences

## Caractériser les spécificités du traitement des données et les risques

### Analyser les flux transfrontaliers de données

- Encadrement des transferts internationaux de données : « BCR », clauses contractuelles types
- Conventions de flux complémentaires
- Débat : Privacy Shield et conséquences du nouvel accord pour le transfert de données entre l'Union européenne et les États-Unis

### Déterminer les sanctions liées au RGPD

- Sanctions et responsabilités
- Responsabilités contractuelles
- Amendes et sanctions de la CNIL
- Cas pratique: quelle sanction ?  
Modalités d'évaluation du bloc certifiant
- Le parcours fera l'objet d'une évaluation des compétences portant sur l'élaboration d'un dossier écrit de synthèse juridique et d'analyse des risques sur la base des pratiques juridiques d'une entreprise réelle.
- Le dossier de synthèse juridique et d'analyse des risques contient :
- La synthèse de l'audit et la cartographie de pratiques à risque de l'entreprise (comme les non-conformités RSE et RGPD),
- La présentation et l'analyse des documents afférents (le règlement intérieur, la charte informatique, la politique de protection des données personnelles, les procédures d'alertes, les chartes éthiques, guides de bonnes pratiques, clauses contractuelles...) comportant des propositions de modification ou d'adaptations des documents.

### Transfert

Votre parcours de formation se poursuit dans votre espace participant. Connectez-vous pour accéder aux ressources et faciliter la mise en œuvre de vos engagements dans votre contexte professionnel.

## A noter

...

En amont et en aval de la formation, le positionnement pédagogique sera effectué à l'aide d'un questionnaire d'auto-positionnement.

## Prochaines sessions

...

### A DISTANCE, PARIS

- 3 Sep. au 4 Nov. 2026
- 18 Nov. au 18 Déc. 2026

