

## 🔴 Cybersécurité et traitement de données personnelles – Blended learning

Garantir la sécurité des données face au risque numérique à l'ère de l'IA

Code  
**600578**

Durée  
**1 jour / 7 heures**

Tarif Inter\*  
**1247 € HT**

*\*Repas inclus (en présentiel)*

### PUBLIC

Délégués à la protection des données (DPO/DPD) – Directeurs des services informatiques (DSI) – Avocats – Toute personne s'intéressant à l'économie de la data et/ou en charge de la conformité de traitements de données personnelles

### PRÉ-REQUIS

Aucun prérequis nécessaire

### NIVEAU D'EXPERTISE

Perfectionnement

### LES POINTS FORTS

Accès en amont de votre formation au E-learning : Que faire en cas de cyber-attaque ? – Durée 45 minutes – Réf.701076.

### 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

- L'évaluation des compétences sera réalisée tout au long de la formation par le participant lui-même (auto-évaluation) et/ou le formateur selon les modalités de la formation.
- Evaluation de l'action de formation en ligne sur votre espace participant :
  - ▶ A chaud, dès la fin de la formation, pour mesurer votre satisfaction et votre perception de l'évolution de vos compétences par rapport aux

## Objectifs pédagogiques

- Définir une politique de protection des données personnelles
- Évaluer les risques numériques à l'ère de l'IA
- Développer des actions de traitement des risques

## Programme de la formation

### Engagement

Connectez-vous sur votre espace participant pour compléter les ressources pédagogiques indispensables au lancement de votre formation. Votre formateur recevra vos objectifs de progrès. Auto-évaluez vos compétences pour suivre vos progrès à l'issue de votre formation..Accès en amont de votre formation au E-learning : Que faire en cas de cyber-attaque ? – Durée 45 minutes

## Définir une politique de protection des données personnelles

### Repérer les données à caractère personnel

- IA générative et protection des données personnelles (RIA/IA Act)
- Identification, modélisation des traitements et flux de données métiers
- Localisation des données à caractère personnel dans le SI et/ou dans le cloud
- Cas pratique : repérer les vulnérabilités pouvant impacter les biens supports

### Prévenir les violations de données

- Panorama des cybermenaces et des acteurs de la cybersécurité
- Recensement des mesures de sécurité existantes
- Repérage des vulnérabilités pouvant impacter les biens supports
- Mise en situation : les réflexes pour garantir la violation de données

## Évaluer les risques numériques à l'ère de l'IA

### Analyser les risques numériques

- Listing des scénarios d'attaque convoitant les données sensibles et les données à caractère personnel

objectifs de la formation. Avec votre accord, votre note globale et vos verbatims seront publiés sur notre site au travers d'Avis Vérifiés, solution Certifiée NF Service

- ▶ A froid, 60 jours après la formation pour valider le transfert de vos acquis en situation de travail
- Suivi des présences et remise d'une attestation individuelle de formation ou d'un certificat de réalisation

#### 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.

- Quantification des risques numériques en termes de probabilité d'occurrence et d'impacts induits
- Mise en situation : élaborer des scénarios d'attaque

#### Être acteur de la conformité

- Sensibilisation des décideurs sur les risques pour leur donner les moyens d'évaluation des risques
- Comment devenir force de proposition sur la stratégie à élaborer ?
- Jeux de rôle : convaincre les décideurs

### Développer des actions de traitement des risques

#### Agir sur les risques identifiés

- Pilotage des actions : réduction, transfert, acceptation, annulation
- Sélection, implémentation, test et optimisation des mesures de sécurité à même de réduire les risques identifiés
- Plan d'actions : renforcer le système d'information de son entreprise en appliquant les 42 règles du guide d'hygiène de l'ANSSI

#### Échafauder des stratégies

- Définition d'une stratégie de réalisation des analyses d'impact
- Outil PIA de la CNIL pour protéger les données personnelles
- Mise en situation : utilisation de l'outil PIA

#### Transfert

Votre parcours de formation se poursuit dans votre espace participant. Connectez-vous pour accéder aux ressources, auto-évaluer vos compétences acquises pendant votre formation 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

...

### PARIS

- 24 Sep. 2026 – Session Garantie
- 3 Nov. 2026 – Session Garantie

