LES FORMATIONS PRIVALORA

Dans un monde où la donnée est au cœur de l'activité, la conformité RGPD, la cybersécurité et l'usage responsable de l'IA générative sont devenus des enjeux stratégiques. Il s'agit d'opportunités de renforcer vos équipes et votre organisation.

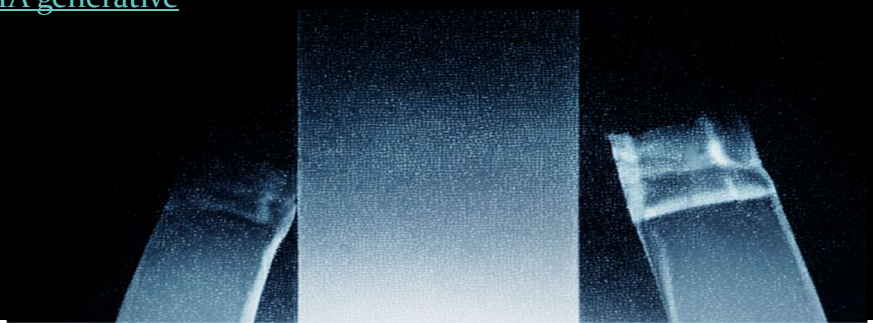
NOS FORMATIONS VOUS PERMETTENT DE :

- **Sécuriser vos données et votre activité** pour rester résilient face aux menaces numériques
- **Protéger vos clients et vos collaborateurs** et bâtir une relation de confiance durable
- **Optimiser vos processus internes** en rendant l'application des règles simple et efficace
- **Développer une véritable culture de la donnée** pour transformer une contrainte en avantage compétitif

*En complément, nous pouvons construire des programmes **sur mesure** en fonction de vos besoins et objectifs, tels que des ateliers pratiques (utilisation optimisée de l'IA générative, Privacy by design, etc.) ou des accompagnements autour des nouvelles réglementations (DGA, DORA, NIS2, IA Act, etc.).*

NOS DIFFERENTES FORMATIONS :

- Sensibilisation aux enjeux stratégiques du RGPD
- Formation des équipes à la conformité RGPD et à la protection des données
- Sensibilisation à la cybersécurité et à l'hygiène numérique
- Encadrement de l'utilisation de l'IA générative



Sensibilisation aux enjeux stratégiques du RGPD

Durée du module : 1 heure

OBJECTIFS :

Comprendre l'importance de :

- **Transformer la conformité en opportunité stratégique** : moteur de différenciation et de confiance
- **Renforcer la gouvernance des données** : réduire les risques opérationnels, juridiques et réputationnels
- **Valoriser le patrimoine informationnel** : améliorer la qualité et l'usage des données
- **Donner une vision claire pour le pilotage** : intégrer la conformité dans les décisions stratégiques

SUJETS ABORDES :

- **Optimisation des processus internes** : réduction des erreurs, gain de temps, meilleure adhésion des collaborateurs
- **Image et réputation** : pratiques éthiques, transparence, amélioration de l'expérience client/utilisateur
- **Gouvernance** : clarification des responsabilités, maîtrise des risques juridiques et réputationnels, enjeux de sécurité numérique
- **Outils et pratiques de conformité** : registres, AIPD, *Privacy by design*, dossier d'accountability
- **Opportunités** : amélioration continue, mesure du ROI, différenciation concurrentielle

PUBLIC CIBLE :

- Membres du comité de direction
- Directions générales et opérationnelles
- Responsables métiers stratégiques (RH, IT, marketing, juridique, etc.)

Formation des équipes à la protection des données

Durée du module : 2 heures

OBJECTIFS :

Comprendre l'importance de :

- **Maîtriser les fondamentaux du RGPD** : concepts clés, principes généraux, données sensibles, consentement et droits des personnes
- **Identifier les obligations de l'organisation :** traitements, registres, sous-traitance, sécurité, transferts de données hors UE, etc.
- **Comprendre la démarche de mise en conformité** et le rôle des différents acteurs (internes et externes)
- **Adopter une culture de la conformité** pour protéger les données, réduire les risques et renforcer la confiance

SUJETS ABORDES :

- **Cadre juridique**, notions essentielles et principes fondamentaux
- **Obligations** des organisations et droits des personnes concernées
- **Encadrement des traitements** : fondements juridiques, données sensibles
- **Gouvernance et responsabilité** (registre, DPO, analyses d'impact, Privacy by design, accountability)
- **Sécurité des données**, gestion des incidents, violations de données, transferts internationaux, etc.
- **Conservation des données**, archivage et hygiène numérique

PUBLIC CIBLE :

- Collaborateurs de tous services et prestataires externes manipulant des données personnelles
- Managers opérationnels
- Nouveaux arrivants (on-boarding)

Sensibilisation à la cybersécurité et à l'hygiène numérique

Durée **du module : 2** heures

OBJECTIFS :

- **Comprendre le rôle central de l'humain** dans la cybersécurité et savoir adopter les bons réflexes
- **Acquérir les notions fondamentales :** authentification, chiffrement, sauvegardes, mises-à-jour
- **Identifier les menaces courantes :** principaux types et vecteurs d'attaques, ingénierie sociale
- **Re forcer la culture de la sécurité** au quotidien pour réduire les risques et protéger l'organisation

SUJETS ABORDES :

- Pourquoi les collaborateurs sont le premier rempart … mais aussi la première cible
- **Hygiène numérique et bonnes pratiques** : mots de passe, utilisation des outils professionnels et personnels, journalisation, shadow IT, etc.
- **Concepts de base** de la cybersécurité et de la gestion de crise cyber
- **Panorama des différents types d'attaques** : phishing, ransomware, arnaques, deep fakes, etc.
- **Méthodes et pratiques** des cyberattaquants : comment ils ciblent et exploitent les failles humaines

PUBLIC CIBLE :

- Collaborateurs de tous services manipulant des données personnelles (RH, Marketing, Commercial, IT, Support, etc.)
- Managers opérationnels
- Nouveaux arrivants (onboarding)

En complément de cette formation, il est recommandé de déployer des campagnes de sensibilisation continue (mails pédagogiques, rappels réguliers, affichages internes, etc.) afin de renforcer l'attention des collaborateurs sur les sujets de cyber sécurité et maintenir leur adhésion sur le long terme.

Encadrement de l'utilisation de l'IA générative

Durée **du module : 2** heures

OBJECTIFS :

- **Comprendre les opportunités et limites** de l'IA générative pour mieux en tirer parti
- **Identifier les risques juridiques et opérationnels** liés à son utilisation (confidentialité, biais, propriété intellectuelle, sécurité numérique, etc.)
- **Définir un cadre clair :** charte, bonnes pratiques, règles pour un usage responsable
- **Préparer l'organisation aux évolutions réglementaires** : IA Act, normes sectorielles, exigences des clients/partenaires, etc.

SUJETS ABORDES :

- **Fonctionnement et cas d'usage** de l'IA générative en entreprise
- **Risques associés** : qualité des données, biais, confidentialité, dépendance technologique, hallucinations
- **Enjeux juridiques** : protection des données, droits d'auteur, propriété intellectuelle, obligations réglementaires
- **Gouvernance et pilotage** : chartes internes, politiques d'usage, validation des cas d'utilisation, outils professionnels vs. outils personnels
- **Anticipation et évolutions légales** : IA Act, initiatives européennes et internationales
- **Bonnes pratiques** pour une utilisation responsable et sécurisée

PUBLIC CIBLE :

- Membres de direction et managers opérationnels
- Responsables innovation, transformation digitale, IT et juridique, etc.
- Ensemble des collaborateurs, tous étant susceptibles d'utiliser l'IA de manière plus ou moins contrôlée