

## Présentation de la formation

La CNIL a publié en octobre 2018, le référentiel permettant la certification des compétences du DPO.

Le DPO doit disposer de compétences juridiques, informatiques et organisationnelles en matière de protection des données personnelles.

L'obtention du certificat délivré par des organismes accrédités par la CNIL, apportera au DPO un gage de confiance et de sérieux.

Pour pouvoir se présenter à la certification, **la CNIL exige** notamment **d'avoir suivi une formation de 35 heures** sur la protection des données.

## Les + de cette formation

- Gestion de la conformité RGPD comme un véritable **projet interne**
- **Formation labellisée par la CNIL** pour le **module DPO** (3 jours)
- Formation dispensée par des **Juristes spécialisés** en protection des données personnelles (Master en Droit) et des **DPO opérationnels**.
- Intervention d'un expert en sécurité informatique (1 jour)
- Des cas pratiques tirés des expériences de terrain des intervenants



## Profil stagiaire

DPO déjà désigné ou amené à être désigné au sein de son organisme

## Prérequis

- Avoir une culture en matière de protection des données
- Être sensibilisé à la sécurité des systèmes d'information
- Disposer d'une connaissance approfondie du secteur d'activité de son organisme
- Disposer d'aptitudes relationnelles nécessaires à l'exercice de la fonction de DPO

## Format

Présentiel  
Groupe de 6 participants maximum

## Durée : 35 heures

**Module 1** : 3 jours  
**Module 2** : 2 jours

## Lieu

2, rue de l'industrie  
38760 VARCES-ALLIERES-ET-RISSET

## Objectifs de la formation

Connaitre et acquérir les compétences et savoir-faire obligatoires listés dans le référentiel de la CNIL

- Comprendre et maîtriser les principes du RGPD (licéité, minimisation, exactitude, conservation limitée, intégrité et confidentialité)
- Identifier la base juridique d'un traitement
- Etablir des procédures pour recevoir et gérer des demandes d'exercice des droits des personnes
- Connaître le cadre juridique relatif à la sous-traitance
- Identifier l'existence de transferts de données hors Union européenne
- Elaborer et mettre en œuvre une politique et des règles internes en matière de protection des données
- Organiser et participer à des audits en matière de protection des données
- Connaitre le contenu du registre d'activités de traitement, du registre des sous-traitants et la documentation relative aux violations de données
- Identifier des mesures de protection de données dès la conception et par défaut
- Participer à l'identification des mesures de sécurité
- Identifier les violations de données personnelles nécessitant une notification à la CNIL et celles nécessitant une notification aux personnes concernées
- Déterminer la nécessité d'effectuer une analyse d'impact (AIPD)
- Gérer les relations avec les autorités de contrôle (CNIL)
- Elaborer et dispenser des programmes de formation et de sensibilisation du personnel
- Assurer la traçabilité de ses activités à l'aide d'outils de gouvernance

## Prix

Selon le nombre de participants et le format de formation choisi (intra ou inter-entreprise)

Possibilité de prise en charge par un OPCA



**Référencé Datadock**

**Programme de formation - Module 1 :**  
Maîtriser les exigences du RGPD  
et de la Loi Informatique et Libertés



**Labellisée CNIL**

## **1. Le RGPD et la mise en conformité**

- Introduction générale à la protection des données
- Les définitions
- Les acteurs de la protection des données (responsables du traitement, responsables conjoints du traitement, sous-traitants)
- Les principes du RGPD
- La validité du traitement
- Le consentement
- La protection des données dès la conception et par défaut
- Les droits des personnes
- L'*accountability* et les process internes
- Le registre des activités de traitement (responsable de traitement) et registre des catégories d'activités de traitement (sous-traitant)
- Les transferts de données hors de l'Union européenne
- Les autorités de contrôle (CNIL)

## **2. La gestion des risques**

- L'analyse d'impact relative à la protection des données (AIPD)
- Les violations de données à caractère personnel, la notification des violations et la communication aux personnes concernées

## **3. – Le Délégué à la protection des données (DPO)**

- La désignation du DPO
- Les fonctions du DPO
- Les missions du DPO

## **Programme de formation – Module 2** Gestion de la sécurité des systèmes d'information

### **1. Introduction aux systèmes d'information**

- Présentation et concepts généraux
- Périmètre du Responsable Informatique
- Les infrastructures réseau, serveur, utilisateur / poste de travail

### **2. La sécurité des systèmes d'information**

- La sécurité des réseaux internes et externes
- La sécurité des postes de travail
- La sécurité des appareils mobiles et connexion à distance
- La sécurité des sites internet
- La sécurité des serveurs et applicatifs métier

### **3. Protéger les systèmes d'information**

- Gestion des risques, des incidents et des événements
- Détection et analyse des risques, des incidents et des événements
- Solutions de cryptographie, d'anonymisation et de signatures numériques
- Continuation des activités (PRC, PCA)

### **4. Documenter la sécurité des systèmes d'information**

- Identifier et décrire les mesures de sécurité (CNIL, ANSSI)
- Les politiques et chartes informatiques
- La méthodologie et les procédures de surveillance et suivi des incidents et des événements

### **5. Cas pratique**

## **Programme de formation – Module 2** Ateliers pratiques

- 1. Doctrine et jurisprudence**
- 2. Gouvernance RGPD**
- 3. Réseaux**
- 4. Cas pratiques**
- 5. Echanges d'expérience**



**Référencé Datadock**