Ref : DNDADPO	**Durée :** 5 Jours	**Tarif :** 3 625 €HT

Formation DPO Data Protection Officer

Objectifs de la formation DPO Data Protection Officer:

- Connaître les missions du Data Protection Officer (DPO) ;
- Acquérir les compétences nécessaires à l'exercice de ces fonctions ;
- S'approprier les démarches et outils nécessaires au maniement des règles en matière de protection des données ;
- Apprendre à gérer l'organisation pour accompagner la mise à niveau et le maintien de performance de l'organisation en matière de respect de la vie privée ;
- Mettre en place un programme de mise en conformité et priorisation des actions par les risques.

Programme de la formation DPO Data Protection Officer:

1. Vision globale : les principes de la protection des données à caractère personnel

1.1 **Les sources**

Histoire, évolution et mise en perspective du droit de la protection des données personnelles ;
Directive « Police » et données relatives aux condamnations pénales et aux infractions ;
Lignes directrices du G29, avis, lignes directrices et recommandations du comité européen de protection des données ;
Jurisprudence française et européenne ;
Changement de paradigme :
du contrôle a priori au contrôle a posteriori ;
exception : la survivance de formalités préalables dans le domaine de la santé, dans certains cas.

1.2 **Les définitions essentielles**

Définitions et notions :
donnée à caractère personnel ;
traitement ;
fichier ;
personne concernées, responsable de traitement, sous-traitant, destinataire, tiers ;
catégories particulières de données ;
profilage et prise de décision automatisée.
Champs d’application du RGPD et organismes concernés.

1.3 **Les grands principes L’architecture complexe du RGPD ;**

Les principes essentiels du RGPD :
finalités du traitement ;
principe de minimisation des données ;
notion d’exactitude des données ;
notion de conservation limitée des données ;

notion de base légale du traitement ;
notion de consentement ;
notion de catégories particulières de données à caractère personnel.
L'accountability et la traçabilité : le changement de paradigme ;
La sécurité.

1.4 Les droits des personnes concernées

Droits et limites ;

Transparence et information ;
Accès, rectification et effacement (droit à l'oubli) ;
Limitation du traitement ;
Décisions individuelles automatisées et profilage ;
Opposition ;
Portabilité.

1.5 Les acteurs DPO :

Du CIL au DPO ;
Désignation et fin de mission ;
Qualités professionnelles, connaissances spécialisées, capacité à accomplir ses missions, profil ;
Qualités personnelles, travail en équipe, management, communication, pédagogie ;
Fonction du DPO (moyens, ressources, positionnement, indépendance, confidentialité, absence de conflit d'intérêts, formation) ;
Missions du DPO et rôle du DPO en matière d'audits ;
Relations du DPO avec les personnes concernées, l'autorité de contrôle et les collaborateurs.
Autorités de contrôle :
La CNIL ;
Statut ;
Fonctionnement ;
Missions ;
Pouvoirs ;
Régime de sanction.
Comité européen de protection des données (CEPD) ;
Organismes de certification ;
Recours juridictionnels.

1.6 Les transferts de données :

Les traitements transfrontaliers ;
Les transferts de données hors UE :
Décision d'adéquation ;
Garanties appropriées ;
Règles d'entreprise contraignantes ;
Dérogations ;
Autorisation de l'autorité de contrôle ;
Suspension temporaire ;
Clauses contractuelles.

2 Vision opérationnelle : mettre en œuvre la conformité

2.1 Nommer un DPO dans l'entreprise

Mettre en place une organisation de gestion de projet :
Constituer un comité de pilotage ;
Nommer un chef de projet (le DPO ou non) ;
Planifier des workshops avec les Services ;
Désigner un sponsor dans l'organisation.
Gérer et faire évoluer les organisations existantes ;
Lui confier ou non la tenue des registres de traitement.

2.2 **Mettre en place et/ou gérer la Gouvernance de protection des données**

Etre nommé DPO ;

Faire un état des lieux de la situation.

2.3 **Recenser parallèlement les outils et livrables de gouvernance**

Recenser les outils d'aide à la conformité déjà disponibles

Prendre note des mises à jour et modifications éventuellement nécessaires

Constituer ou mettre à jour un dossier des outils d'aide à la conformité

Modèles de document, formulaire, outil PIA, référentiels, guides, forum, etc.

Établir une liste des livrables attendus

S'informer : mettre en place des outils et une méthodologie de veille (CEPD, lignes-directrices, actualités de la CNIL, etc.) ;

établir des relations avec d'autres professionnels du domaine (associations de DPO, AFCDP, etc.).

Recenser les codes de conduite, labels et certifications obtenus par l'entreprise ou intéressants, ainsi que les formations en place et les compétences déjà acquises dans la société

2.4 **Connaître son environnement et son écosystème**

État des lieux plus poussé des livrables passés

Études d'impact précédentes, conformité avec les formalités CNIL pré-RGPD, etc.

Cartographier les données avec l'aide du RSSI et des Services

cartographier les systèmes d'informations (repérer les DACP), établir une matrice des flux, cartographier les acteurs (lister les contrats)

éclaircir les imprécisions sur les conséquences juridiques du fonctionnement des systèmes d'information (flux de données non connus, lieu d'hébergement des données et des back up)

Etablir le registre des activités de traitement (responsable de traitement) et registre des catégories d'activités de traitement (sous-traitant)

2.5 **Prioriser les actions sur la base de l'état des lieux**

Tirer les conséquences des qualifications juridiques établies

apprécier l'impact des éventuelles modifications de fondement juridique des traitements ;

apprécier la qualification donnée par les opérationnels des données traitées / collectées.

Clarifier la situation contractuelle de l'entreprise

renégocier les contrats ;

entrer en contact avec les prestataires, les clients, etc. ;

mettre à jour les documents et mentions d'information ;

sensibiliser / informer les personnels.

2.6 **Réaliser les analyses d'impact relatives à la protection des données (AIPD)**

Piloter les traitements par le risque :

identifier les traitements les plus à risque ;

identifier les traitements imposant la réalisation d'une étude d'impact.

Réaliser les analyses de risque sur la sécurité des données ;

Anticiper les violations de données à caractère personnel, la notification des violations et la communication avec les personnes concernées :

mettre en place des mécanismes de remontées d'alertes, des référentiels de quantification des risques, des procédures de notification des violations de données ;

coordonner cette notification avec les autres mécanismes de notification des incidents de sécurité ;

prendre des mesures en vue de rétablir la disponibilité des données et l'accès aux données en cas d'incident physique ou technique.

2.7 **Constituer son dossier de conformité (Accountability) et déployer une culture de « Protection des données » dans l'organisation**

Constituer son dossier de conformité (Accountability) :

lancer la création d'un SI /dossier dédié à la conformité pour la documentation ;

mettre en place de processus d’alimentation de ce dossier.
Prendre des mesures techniques et organisationnelles pour la sécurité des données au regard des risques :
mettre en place la protection des données dès la conception (Privacy by design) et par défaut (Privacy by default) ;
garantir la confidentialité, l’intégrité et la résilience des systèmes et des services de traitement.
Déployer une culture de « Protection des données » dans l’entreprise :
sensibiliser le personnel ;
créer un processus de réponse aux réclamations ;
organiser des exercices pour anticiper d’éventuelles violations de sécurité.

2.8 **Se préparer à un contrôle de la CNIL et intégrer les risques juridiques**
Se préparer à un contrôle de la CNIL ;
Intégrer les risques juridiques (voies de recours, moyens de défense, sanctions).

Public

DPO (Délégué à la Protection des Données) ou futurs DPO, anciens CIL ; Personnes ayant à prendre en charge ou à mettre en œuvre la conformité de traitements de données personnelles à tous les niveaux, du management à l'opérationnel en passant par la conformité : Personnes responsables de services opérationnels ; DSI et leurs équipes ; Responsables conformité, responsables des risques ; Juristes et responsables juridiques. Consultants accompagnant à la mise en conformité RGPD ou assistant le DPO.

Pré-requis

Aucun pré-requis n'est demandé pour la formation. Ne pourront passer l’examen que les candidats justifiant de deux ans d’expérience professionnelle, soit en lien avec la protection des données, soit dans tout domaine si le candidat a également suivi une formation de 35h minimum en matière de protection des données.

Méthodes pédagogiques

La méthode pédagogique se fonde sur les quatre axes suivants : Un cours magistral sur le sujet, construit en partant des textes et documents officiels mais adapté de façon à rendre la matière compréhensible en langage courant, pour aboutir à des recommandations opérationnelles ; Enrichi de cas pratiques et d’exemples concrets illustrant les notions explicitées profitant du partage d'expérience des instructeurs HS2 tous avocats spécialistes reconnus de ces questions ou implémenteurs des normes ; Un cours construit pour favoriser l’interactivité entre les participants, qui peuvent à tout moment poser des questions, et les intervenants ; Des exercices pratiques individuels effectués par les stagiaires, basés sur des études de cas, permettant de se confronter à des cas réels et de se préparer aux questions de l'examen.