Formation « DPO »

Réf : DPO

La formation certifiante par excellence pour obtenir la certification de Data Protection Officer (DPO) et confirmer l'étendue de vos connaissances en matière de protection des données. **Notre formation est entièrement dédiée à l'obtention de cette certification !**
Notre formation est enregistrée par AFNOR Certification comme prérequis à la certification de compétences des DPO.
AFNOR Certification est historiquement le 1er organisme certificateur agréé par la CNIL pour certifier les compétences des délégués à la protection des données / Data Protection Officer (DPO), sur la base des référentiels du 20 septembre 2018 adoptés par la CNIL.

ATTENTION : Pour une formation permettant de s'approprier les démarches et les outils dédiés à la protection des données, approfondir ses connaissances du métier du DPO et apprendre à gérer la conformité RGPD de son organisation, nous vous recommandons plutôt la formation « Métier du DPO » qui répondra à toutes ces attentes.

Objectifs

- **Acquérir les connaissances juridiques, techniques et organisationnelles nécessaires à la réussite à l'examen de certification.**

Durée & horaires

- **5 jours, soit 37h heures réparties en 35h00 de cours (dont 2h de travail personnel) et 2h d'examen.**
- **Du lundi au jeudi : de 9h30 à 12h00 et de 13h30 à 17h30/18h00.**
- **Le vendredi : de 09h30 à 12h00 et de 13h30/14h00 à 16h00/16h30.**

Nombre de participant

- **Minimum 6 participants – Maximum 16 participants.**

Public visé

- **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 et souhaitant disposer de la certification DPO :**
  - **DPO, DRPO**
  - **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

- **Avoir au minimum relu :**
  - **Les principales lignes directives du CEPD**
  - **Les principales recommandations de la CNIL**
- **Avoir passé les MOOCs de la CNIL et de l'ANSSI**
- **Avoir des bases informatiques ou juridiques est un vrai plus.**

Méthode pédagogique

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 appréhender au mieux les questions de l'examen**
- **Enrichi de cas pratiques et d'exemples concrets illustrant les notions explicitées profitant du partage d'expérience des instructeurs HS2 tous avocats et consultants spécialistes reconnus de ces questions ou implémenteurs des normes ayant tous passés récemment l'examen**
- **Des quizz à chaque étape des points importants de la formation pour évaluer le niveau de compréhension et de connaissance, ainsi qu'un examen blanc dans les conditions de l'examen final**
- **Un cahier d'exercices et un cahier de révisions de notions de cours à travailler le soir permettant de se préparer aux questions de l'examen.**

Supports

- **Support de cours en français ;**
- **Cahier d'exercices et corrections des exercices ;**
- **Tous les documents nécessaires à la formation en français ou anglais ;**
- **Feuilles d'émargement par demi-journée de formation et certificat individuel de formation attestant de la participation à l'ensemble de la formation.**

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration.**

Certification

- **Cette formation prépare à l'examen de certification "Délégué à la protection des données" (DPO). Formation enregistrée par AFNOR Certification comme prérequis à la certification de compétences des DPO.**
- **A l'issue de cette formation, le stagiaire passe l'examen d'une durée de 2h en français. L'examen est constitué d'un QCM. Cet exercice valide les compétences et les savoir-faire présentés dans la catégorie 2 de la délibération n°2018-318 du 20 septembre 2018. Les questions couvrent tous les domaines du programme figurant en annexe de la délibération n°2018-317 du 20 septembre 2018.**

Programme

1 - Les principes de la protection des données à caractère personnel

- **1.1 Les sources**
  - Evolution et mise en perspective des principes généraux applicables (loi informatique et Libertés, textes européens, genèse RGPD, droit comparé US)
  - Qu'est-ce que la CNIL ? Qu'est-ce que le CEPD ?

- **1.2 Les définitions essentielles**
  - De quoi parle-t-on ? Notions de donnée à caractère personnel, traitement, responsable de traitement/sous-traitant, etc.

- **1.3 Le champ d'application**
  - Champ d'application matériel du RGPD (la Directive 2016/680 dite Directive « Police », le secteur des télécom/commerce électronique)
  - Champ d'application territorial (l'autorité de contrôle « chef de file », les transferts de données hors UE/EEE, certifications/codes de conduite)

- **1.4 Les grands principes**
  - L'architecture complexe du RGPD
  - Les principes essentiels du RGPD (licéité, loyauté, transparence, limitation des finalités, minimisation des données, exactitude, etc.)
  - Conformité de l'écosystème (la qualification de responsable de traitement/sous-traitant ; accords contractuels)
  - Le registre de traitements

- **1.5 Les régimes spéciaux**
  - Les données à caractère hautement personnel, les données relatives aux condamnations pénales ou infractions, catégories particulières de données, etc.
  - Le profilage
  - Les référentiels de la CNIL

- **1.6 Les droits des personnes**
  - Droit à l'information, droit d'accès, droit de rectification, droit à l'effacement, droit d'opposition, etc.

2 - L'approche par les risques

- **2.1 Intégrer les principes de Privacy by design et by default**
  - Les 7 piliers du Privacy by design
  - A quoi servent ces principes ?
  - Les outils de mise en œuvre

- **2.2 Se donner les moyens d'assurer la sécurité**
  - Les violations de données personnelles : notion d'intégrité, de disponibilité, de confidentialité… et d'accountability
  - Les sanctions en cas de manquement à la sécurité
  - Notions de mesures de sécurité et d'adéquation aux risques
  - Exemples de mesures de sécurité et de contre-mesures pour chaque type de violation
  - Les bonnes pratiques, etc.

- **2.3 Evaluer les risques et analyser l'impact de vos traitements sur les droits et libertés fondamentales (AIPD)**
  - Qu'est-ce qu'une analyse d'impact ? Position de la CNIL
  - Contenu de l'AIPD
  - Appréciation du risque
  - Notion d'AIPD flash

- **2.4 Savoir notifier les violations de données personnelles**
  - Genèse de l'obligation de notification
  - Modalités de la notification (qui, quand, comment ?)
  - Modalités de la communication aux personnes concernées

- **2.5 Anticiper les recours et préparer un contrôle par les autorités**
  - Réclamations, recours, responsabilités
  - L'action collective, le droit à réparation
  - Se préparer à un contrôle de la CNIL (modalités, pouvoirs de la CNIL, sanctions)

3 - Mettre en œuvre la conformité

- **3.1 Nommer un DPO dans l'entreprise**
  - Qualités, profil, statut
- **3.2 Mettre en place et/ou gérer la gouvernance de protection des données**
  - DPO, contrôleur ou faiseur ?
  - Comité de pilotage, groupe de travail, etc.

- **3.3 Déployer une culture « Protection des données » dans l'entreprise**
  - Notion, intérêt et structuration du Dossier de conformité
  - Sensibilisation des personnels

- **3.4 Recenser parallèlement les outils et livrables de gouvernance**
  - Analyse de l'existant, veille globale
  - Accountability

- **3.5 Connaître son environnement et son écosystème**
  - Cartographies