DROIT DE LA GESTION DES DONNEES

FICHE PROGRAMMATION

PARCOURS BE+ : DEVENIR DELEGUE(E) A LA PROTECTION DES DONNEES A CARACTERE PERSONNEL - DPO

Public

DPO - Délégué(e) à la protection des données ou personne suceptible de le devenir

Prérequis

- Avoir suivi le MOOC de l'ANSII intitulé "secnum", ou une formation équivalente.
- Et avoir une expérience de deux ans en lien avec la protection de données : CIL, RSSI, service juridique…

Objectifs pédagogiques

- Garantir la conformité à la réglementation "informatique et libertés" en interne et vis à vis des autorités publiques (CNIL, régulateurs sectoriels).
- Gérer et améliorer les processus de la conformité.
- Diffuser la culture de la protection des données.
- Sensibiliser les acteurs à la protection des données.

Contenu

Depuis le 01er juin 2019 en Nouvelle-Calédonie, les Délégués à la protection des données sont formellement désignés par les responsables de traitement auprès des autorités de contrôle (la CNIL en France), soit obligatoirement, soit volontairement. Leurs fonctions sont définies réglementairement.

L'objectif principal de cette formation est de les doter des compétences nécessaires afin d'assurer cette mission, soit pour:
- informer et sensibiliser, diffuser une culture « Informatique et Libertés »,
- veiller au respect du cadre légal,
- informer et responsabiliser, alerter si besoin, son responsable de traitement,
- d'analyser, investiguer, auditer, contrôler,
- établir et maintenir une documentation au titre de « l'Accountability »,
- assurer la médiation avec les personnes concernées,
- présenter un rapport annuel à son responsable de traitement,
- interagir avec l'autorité de contrôle.

Chaque Module est suivi d'une période au cours de laquelle les participants devront réaliser des travaux attachés au contenu abordé et feront l'objet d'un suivi de formation individualisé en entretien de 4 heures pour obtenir l'attestation de réussite BE+.
La formation s'échelonne sur plusieurs semaines pour permettre une appropriation des savoirs et savoir-faire.

Module 1 : Organiser/bâtir le processus de mise en conformité – Désigner un pilote – Associer la direction de la structure

- Mettre en place une gouvernance des données (définir les rôles et responsabilités, les process de traitement des données, etc.)
- Se former aux nouvelles technologies, outils de communication ou aspects juridiques spécifiques à l'organisation en fonction de l'évolution des traitements.

Travail personnel à produire : identification et définition des rôles des parties prenantes « qui fait quoi ? » et entretien de remédiation avec le formateur sur les difficultés rencontrées.

Module 2: Le contrôle

- Etablir une cartographie des traitements de données à caractère personnel et des flux de données
- Tenir un registre des traitements comportant les actions préventives et correctives
- Diagnostiquer la conformité notamment par la réalisation d'audits
- Procéder à des analyses d'impact en matière de protection des données (Privacy Impact Assessment).
- Anticiper et réagir aux demandes de droits d'accès et en cas de violation des données à caractère personnel / faire face à des situations de crise
- Organiser le contrôle en interne et lors de la sous-traitance
- Évaluer régulièrement l'amélioration de la mise en œuvre des procédures de conformité
- Assurer une veille juridique sur le thème de la protection des données personnelles
- Gagner du temps dans la mise en conformité : exposé des process permettant une mise en conformité allégée par l'autorité de tutelle elle-même
- Mise en place du Guide Pratique du RGPD au sein des organisations.
- Utiliser les outils disponibles pour gagner du temps en gardant une exigence de contrôle

Travail personnel à produire : Cartographie d'un méta traitement, et réalisation d'une analyse d'impact (étude de cas fictive), puis entretien de remédiation avec le formateur sur les difficultés rencontrées.

Module 3: La communication

- Dialoguer avec les régulateurs (dont la CNIL) afin d'améliorer la conformité de l'organisme avec les formalités déclaratives (déclarations et demandes d'autorisations)
- Élaborer sa politique de gestion des données
- Rédiger les procédures, les chartes, les clauses
- Échanger avec les responsables des activités qui traitent des données à caractère personnel
- Alerter sur les risques de non-conformité et de sécurité informatique
  - Connaître les bonnes pratiques d'hygiène informatique (la notion de sécurité by design, la gestion des mots de passe, la gestion des mises à jour de logiciels et la sauvegarde régulière des données)
  - Reconnaître les différentes formes de cyberattaques et leurs vecteurs
  - Savoir réagir en cas d'incident de sécurité et mettre en place un plan de réponse
- Former les collaborateurs directement concernés par les traitements
- Conseiller l'ensemble des parties prenantes de l'entreprise afin que la protection des données devienne un réflexe
- Informer sur la loi Informatique et Libertés afin de faire prendre conscience aux acteurs de son importance dans la mise en pratique quotidienne de leurs activités
- Communiquer auprès du public sur la politique de l'organisme en matière de protection des données
- Assurer le recueil du consentement
- Résoudre les difficultés concrètes et matérielles de mise en place de la règlementation au sein des organisations
- Transformer la mise en place de la réglementation en un avantage concurrentiel : RGPD et droit de la concurrence

Travail personnel à produire : Réaliser un inventaire de la documentation existante (si possible en lien avec le méta-traitement cartographié), puis entretien de remédiation avec le formateur sur les difficultés rencontrées.

Module 4: Identifier les cas d'applications existant

  - Exposé des principales condamnations en Europe
  - Résumé rapide de la remise en cause du PRIVACY SHIELD et conséquences directes sur le Territoire.
  - Quel avenir pour la protection des données personnelles au regard des défis technologiques des prochaines décennies ?
  - Le RGPD et l'intelligence artificielle (Chat GPT et autres)
  - Faire vivre le processus de conformité dynamique et général.
  - Présentation de travaux réalisés.

Cette formation et son contenu répondent à l'exigence de 35h de formation (en plus d'une expérience professionnelle de 2 ans tous domaines au minimum) pour passer la **certification des compétences du DPO**conformément au référentiel de certification de la CNIL. Les modalités de test sont disponibles sur le site de la CNIL.

Le passage de l'examen n'est pas n'est pas compris dans le tarif de ce parcours.