Formation RGPD
DPO : Data Protection Officer

Devenir délégué à la protection des données
Préparer la certification CNIL

Thématique

L'Union européenne a officialisé en 2016 un nouveau règlement sur la protection des données à caractère personnel, qui est applicable depuis le 25 mai 2018 sur tout le territoire européen.

Ce règlement introduit de nouveaux droits pour les citoyens européens en matière de protection de la vie privée et donc de nouvelles obligations pour les organisations et entreprises. Il implique une évolution profonde des pratiques liées à la collecte, la conservation et l'exploitation des données à caractère personnel.

Ce règlement a créé un nouveau rôle clé, le DPO (Data Protection Officer), qui est au cœur du dispositif de « Responsabilité » (principe d'*accountabiliy* du RGPD). Le DPO est :

- En charge de mettre en œuvre et de faciliter la mise en conformité au RGPD de la structure ;
- Le conseiller du responsable de traitement ou du sous-traitant ;
- Un intermédiaire entre les parties prenantes, en interne et externe ; et
- Le correspondant de l'Autorité de Contrôle (en France, la CNIL).

Dans certains cas, la nomination d'un délégué à la protection des données est obligatoire (organismes publics, traitements systématiques à grande échelle, traitement de données sensibles, etc.), quel que soit la taille de la structure, et aussi bien pour les responsables de traitement que les sous-traitants.

Cependant, en dehors de ces situations, il est tout de même fortement recommandé par le Groupe de travail de l'article 29 du RGPD (dit « G29 ») – désormais Comité européen de la protection des données (dit « EDPB ») – de confier à un référent la mise en œuvre de la conformité au RGPD de l'organisation afin de prévenir les risques liées aux données personnelles. En effet, en cas de non-respect du RGPD, la CNIL peut prononcer une amende pouvant aller jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires mondial (le montant le plus élevé étant retenu).

La conformité d'une entité au RGPD constitue donc un enjeu majeur, c'est pourquoi les entreprises cherchent à recruter des DPO, et l'offre d'emploi a sans nul doute vocation à croitre de façon exponentielle dans les années à venir.

Formateurs

Alexandre Diehl - Cabinet d'Avocats Lawint – Professeur à l'Université Paris 1 Panthéon Sorbonne
Aziz Ben Ammar – Cabinet d'Avocats Lawint – Professeur à l'INSEEC
Jean-Baptiste ARTIGNAN – DPO certifié AFNOR – Auditeur cybersécurité certifié ISO 27001 – Associé chez BlueSecure – Professeur à l'ESIEE IT

Ils parlent de nous

Objectifs

A l'issue de cette formation *DPO*, vous serez à même de :

- Maîtriser les enjeux et les principes clés de la réglementation relative aux données personnelles ;
- Appliquer les bonnes pratiques au sein d'une organisation pour garantir le respect du cadre légal au quotidien ;
- Appréhender le rôle, les missions et les responsabilités du DPO ;
- Réaliser un état des lieux de la conformité au RGPD d'une structure ;
- Mettre en œuvre un projet de mise en conformité des traitements ;
- Tenir un registre des activités de traitement ;
- Négocier un cadre contractuel adapté avec les différents acteurs ;
- Mettre en œuvre les droits de personnes concernées par les traitements ;
- Gérer les transferts de données en dehors de l'Union européenne ;
- Participer à une analyse de risques ;
- Identifier les mesures de sécurité minimales et appropriées aux risques propres à votre structure ;
- Maîtriser les mécanismes techniques de pseudonymisation, d'anonymisation et de chiffrement de données ;
- Réaliser une analyse d'impact sur la protection des données ;
- Gérer un incident de sécurité lié aux données personnelles ainsi que l'éventuelle procédure de notification qui s'en suit ;
- Préparer l'examen de certification DPO.

Public concerné

Toute personne au sein d'une organisation (entreprise, association, groupement d'intérêt économique, etc.) amené à prendre le rôle de DPO ou souhaitant devenir référent RGPD.

Prérequis

La formation est construite de manière à être accessible à tous, sans connaissances préalables dans le domaine juridique ou informatique.

Durée

35 heures.

Matériel de formation

Formation 100% en ligne à suivre à son rythme : Vidéos, cas pratiques, tests de validation des acquis par chapitre, documents annexes et liens utiles.

- Etude de cas : Négociation contractuelle DPA – Data Processing Agreement
- Etude de cas : Réalisation d'un registre des traitements
- Etude de cas : Sécurité SI – Vulnérabilités des sites web
- Exercice pratique + corrigé : Réalisation d'une Analyse d'Impact PIA

Programme de la formation

Partie 1- Comprendre le Règlement

- Les enjeux de la protection des données
- Définitions et champ d'application
- Les fondamentaux et principes du RGPD : Droits des personnes et principes clés
- 40 ans de construction de la protection de la vie privée
- Le positionnement du RGPD dans le cadre légal
- L'Autorité de Contrôle : la CNIL en France
- Sanctions et recours
- Les autres acteurs du RGPD : G29, EDPB, CJUE…

Partie 2 - Appliquer le Règlement

- Les obligations générales des organisations
- Les procédures écrites
- La conservation, l'aonymisation et la purge des données
- Formation des employés et audits
- Code de conduite
- Certification et politique de protection des données
- L'encadrement juridique des relations avec les salariés
- La mise en conformité des sites internet
- La détermination de la validité d'un traitement : focus sur toutes les bases juridiques
- L'information des personnes et le recueil du consentement
- La contractualisation

Étude de cas : Négociation contractuelle d'un Data Processing Agreement (DPA)

- Les mentions légales obligatoires
- Les transferts internationaux
- L'obligation de transparence
- Déterminer les droits des personnes : Accès, rectification, oubli, limitation, opposition, portabilité, post-mortem.
- Mettre en œuvre les droits des personnes

Partie 3 – La sécurité des données

- Les fondamentaux de la sécurité des données
- Introduction à l'analyse de risques
- Focus sur les 12 mesures élémentaires de sécurité de l'information

Étude de cas : La sécurité des sites web

- Disponibilité, intégrité et résilience des données
- Pseudonymisation, anonymisation, signature et chiffrement des données personnelles
- Audits en matière de protection des données personnelles

Partie 4 – Responsabilité

- La responsabilité de la structure
- La responsabilité du DPO
- Tenir un registre des traitements ou un registre sous-traitant

Étude de cas : Registre de traitement d'un hôtel

- Gestion et notifications des violations de données à l'autorité de contrôle et aux personnes concernées
- *Privacy by design* et *privacy by default*
- Focus sur l'analyse d'impact : Principes et réalisation

Cas pratique : Réalisation de l'analyse d'impact d'une société de crédit en ligne

Partie 5 - Le Délégué à la Protection des Données (DPO)

- Qu'est-ce qu'un DPO ?
- Désignation obligatoire d'un DPO
- Désignation volontaire d'un DPO
- Absence de désignation
- Missions et fonctions
- Profil du DPO
- Nomination et révocation du DPO
- Le positionnement du DPO
- La déontologie du DPO

Partie 6 - DPO Au quotidien

- Le marché du DPO
- Prise de poste du DPO
- Réaliser un état des lieux de la conformité de l'organisme
- Plan de mise en conformité et gestion du changement
- Piloter la conformité au quotidien
- Documenter la conformité
- Les aspects contractuels pratiques
- Le rapport annuel du DPO et relations avec la direction
- Comment gérer un contrôle CNIL ?
- Le départ du DPO

Partie 7 – La certification DPO

- Présentation du processus de certification de personnes
- Notions importantes pour la certification
- Préparation à la certification

Examen blanc de certification DPO (100 questions)

Bonus inclus dans la formation

• Sélection des lignes directrices G29/EDPB incontournables ;
• Modèle de registre des traitements ;
• Outil analyse d'impact PIA et exemple de d'analyse d'impact complétée ;
• Clauses contractuelles types pour les transferts de données ;
• Clauses contractuelles types pour la sous-traitance ;
• Procédure de contractualisation avec détermination du positionnement du partenaire ;
• Modèle de charte et mentions RGPD pour un site web ou un formulaire ;
• Modèle de charte informatique et d'engagement de confidentialité;
• Recommandations et Auto-questionnaire relatif à la Privacy by design ;
• Guide des bonnes pratiques et des mesures de sécurité à adopter ;
• Check-list de diagnostic des pratiques de sécurité informatique ;
• Guide pratique relatif à la gestion des habilitations ;
• Guide des recommandations pour la journalisation ;
• Guide sécurité du télétravail et de la mobilité ;
• Guide sécurité du réseau internet et du Wi-Fi ;
• Guide pour réaliser un Plan de Continuité d'Activité ;
• Guide des meilleures pratiques de Pseudonymisation.

Prix de la formation

1290€ HT, soit 258 € HT la journée.
TVA applicable 20%.

Pour commander en ligne, nous contacter ou obtenir davantage d'informations :

https://bluelearning.fr/formation/dpo-data-protection-officer-rgpd/