

Réglementation en cybersécurité : RGPD & DPO

Durée : 4 jours (28 heures)

CONNAISSANCES PREALABLES

- Connaissances générales du fonctionnement d'une organisation et des systèmes d'information.
- Connaissances de base en cybersécurité ou en gestion des risques recommandées.
- Aucun prérequis juridique spécifique n'est nécessaire.

PROFIL DES STAGIAIRES

- Délégués à la Protection des Données (DPO)
- RSSI et responsables cybersécurité
- Responsables conformité et gestion des risques
- DSI et responsables informatiques
- Responsables juridiques
- Responsables RH
- Chefs de projets SI et métiers
- Toute personne impliquée dans la gestion ou la protection des données personnelles.

OBJECTIFS

À l'issue de la formation, les participants seront capables de :

- Comprendre les principes fondamentaux du RGPD et de la protection des données personnelles.
- Identifier les obligations réglementaires applicables à leur organisation.
- Comprendre le rôle, les missions et les responsabilités du DPO.
- Mettre en œuvre une démarche de conformité RGPD.
- Réaliser une cartographie des traitements de données.
- Conduire une analyse d'impact relative à la protection des données (AIPD/DPIA).
- Gérer les violations de données personnelles.
- Articuler les exigences du RGPD avec les enjeux de cybersécurité.
- Construire un plan d'action de mise en conformité.

CERTIFICATION PREPAREE

Aucune

METHODES PEDAGOGIQUES

- Alternance d'apports réglementaires, juridiques et opérationnels.
- Études de cas inspirées de situations réelles et de sanctions prononcées par les autorités de contrôle.
- Ateliers collaboratifs de cartographie des traitements et d'analyse de conformité.
- Exercices pratiques de gestion des violations de données.
- Simulations de prise de décision et de gestion des risques.

- Cas fil rouge permettant de construire une démarche de conformité complète.

FORMATEUR

- Consultant expert en protection des données personnelles, conformité réglementaire et cybersécurité disposant d'une expérience significative dans l'accompagnement des organisations sur les sujets RGPD, gouvernance des données, gestion des risques et mise en conformité réglementaire.

METHODE D'EVALUATION DES ACQUIS

- Questionnaire de positionnement en début de formation.
- Évaluation continue à travers les ateliers et exercices pratiques.
- Quiz intermédiaires de validation des connaissances.
- Études de cas individuelles et collectives.
- Cas pratique fil rouge de mise en conformité RGPD.
- Questionnaire d'évaluation des acquis en fin de formation.

CONTENU DU COURS

Jour 1 : Comprendre le RGPD et le rôle du DPO (7h)

Module 1 : Fondamentaux de la protection des données personnelles (2h)

Objectifs

- Comprendre les enjeux de la protection des données.
- Identifier les grands principes du RGPD.

Contenu

- Historique et objectifs du RGPD.
- Définitions clés.
- Données personnelles et données sensibles.
- Acteurs du traitement.
- Principes fondamentaux du RGPD.
- Droits des personnes concernées.

Mise en pratique

Brainstorming collectif :

- Identification des données personnelles manipulées dans différents contextes métiers.

Module 2 : Les obligations des organisations (2h)

Objectifs

- Identifier les obligations réglementaires applicables.
- Comprendre les responsabilités des acteurs.

Contenu

- Licéité des traitements.
- Information et transparence.
- Consentement.
- Durées de conservation.
- Sous-traitance.
- Documentation de conformité.
- Accountability.

Mise en pratique

Atelier :

- Analyse de conformité d'un traitement de données.

Module 3 : Le rôle et les missions du DPO (2h)

Objectifs

- Comprendre les missions du DPO.
- Définir son positionnement dans l'organisation.

Contenu

- Désignation du DPO.
- Missions et responsabilités.
- Relations avec les métiers.
- Relations avec les autorités de contrôle.
- Gouvernance de la conformité.

Mise en pratique

Étude de cas :

- Construction d'une feuille de route DPO pour une organisation.

Module 4 : Atelier de synthèse RGPD (1h)

Objectifs

- Consolider les notions fondamentales.

Mise en pratique

Cas pratique :

- Identification des obligations RGPD applicables à une entreprise fictive.

Jour 2 : Cartographier les traitements et piloter la conformité (7h)

Module 5 : Réaliser une cartographie des traitements (2h)

Objectifs

- Identifier les traitements de données personnelles.
- Construire un registre conforme.

Contenu

- Inventaire des traitements.
- Registre des traitements.
- Identification des finalités.
- Catégories de données.
- Catégories de personnes concernées.
- Flux de données.

Mise en pratique

Atelier :

- Construction d'un registre des traitements.

Module 6 : Gérer les droits des personnes concernées (2h)

Objectifs

- Organiser la gestion des demandes des personnes.

Contenu

- Droit d'accès.
- Droit de rectification.
- Droit à l'effacement.
- Droit à la limitation.
- Droit à la portabilité.
- Gestion des demandes et délais.

Mise en pratique

Jeu de rôle :

- Traitement de demandes d'exercice des droits.

Module 7 : Documentation et gouvernance de la conformité (2h)**Objectifs**

- Structurer la démarche de conformité.

Contenu

- Politique de protection des données.
- Procédures internes.
- Sensibilisation des collaborateurs.
- Audits internes.
- Contrôles de conformité.

Mise en pratique**Atelier :**

- Élaboration d'un plan de gouvernance RGPD.

Module 8 : Atelier de conformité (1h)**Objectifs**

- Appliquer les notions étudiées.

Mise en pratique**Étude de cas :**

- Audit simplifié de conformité RGPD.

Jour 3 : Analyse des risques et gestion des violations de données (7h)**Module 9 : Analyse des risques liés aux données personnelles (2h)****Objectifs**

- Identifier les risques pour les personnes concernées.

Contenu

- Notion de risque RGPD.
- Menaces et vulnérabilités.
- Impacts sur les droits et libertés.
- Évaluation des risques.

Mise en pratique**Atelier :**

- Analyse de risques sur un traitement de données.

Module 10 : Réaliser une AIPD / DPIA (3h)**Objectifs**

- Conduire une analyse d'impact conforme aux exigences du RGPD.

Contenu

- Critères nécessitant une AIPD.
- Méthodologie CNIL.
- Description du traitement.
- Évaluation des risques.
- Mesures de réduction.

Mise en pratique**Travaux pratiques :**

- Réalisation guidée d'une AIPD sur un cas concret.

Module 11 : Gérer une violation de données personnelles (1h)

Objectifs

- Réagir efficacement à un incident impliquant des données personnelles.

Contenu

- Détection des violations.
- Évaluation de la gravité.
- Notification à la CNIL.
- Communication aux personnes concernées.
- Documentation de l'incident.

Mise en pratique

Étude de cas :

- Gestion d'une fuite de données personnelles.

Module 12 : Atelier de gestion d'incident RGPD (1h)

Objectifs

- Mettre en œuvre les procédures de gestion des violations.

Mise en pratique

Simulation :

- Qualification et traitement d'un incident de protection des données.

Jour 4 : RGPD, cybersécurité et mise en conformité opérationnelle (7h)

Module 13 : Articuler RGPD et cybersécurité (2h)

Objectifs

- Comprendre le lien entre conformité et sécurité.

Contenu

- Exigences de sécurité du RGPD.
- Mesures techniques et organisationnelles.
- Gestion des accès.
- Chiffrement.
- Journalisation.
- Sauvegarde et résilience.

Mise en pratique

Atelier :

- Évaluation des mesures de sécurité d'un traitement sensible.

Module 14 : Auditer et maintenir la conformité (2h)

Objectifs

- Pérenniser la conformité dans le temps.

Contenu

- Audit RGPD.
- Contrôles périodiques.
- Gestion des écarts.
- Amélioration continue.
- Veille réglementaire.

Mise en pratique

Étude de cas :

- Préparation d'un audit de conformité.

Module 15 : Cas fil rouge : Construire un plan de conformité RGPD (2h)

Objectifs

- Mettre en œuvre l'ensemble des acquis de la formation.

Mise en pratique

Exercice de synthèse :

- Cartographie des traitements.
- Analyse des risques.
- Réalisation d'une AIPD.
- Gestion d'un incident.
- Définition d'un plan d'actions de conformité.

Module 16 : Restitution et débriefing (1h)

Objectifs

- Présenter une démarche de conformité structurée.
- Défendre les choix réalisés.

Mise en pratique

Présentation orale :

- Restitution devant un comité de direction fictif.
- Débriefing collectif.
- Retour d'expérience.

Notre référent handicap se tient à votre disposition au [01.71.19.70.30](tel:01.71.19.70.30) ou par mail à <mailto:referent.handicap@edugroupe.com> pour recueillir vos éventuels besoins d'aménagements, afin de vous offrir la meilleure expérience possible.