

# Programme de formation RGPD et Sécurité

## 1 OBJECTIFS DU DOCUMENT

---

L'objectif de ce document est de présenter le sommaire de la journée de formation RGPD & sécurité

## 2 DESCRIPTIF

---

### 2.1 Objectifs pédagogiques

Consolider les fondamentaux du RGPD :

- Rappel des principes de base du RGPD
- Connaître le cadre juridique et le champ d'application
- Connaître les principes de la mise en conformité
- Sensibiliser les salariés aux bonnes pratiques de la sécurisation des données

Acquérir les fondamentaux de la sécurité :

- Comprendre la notion d'identité numérique
- Savoir gérer ses mots de passe
- Sécuriser l'utilisation de la messagerie
- Comprendre comment réagir face aux menaces d'aujourd'hui

### 2.2 Méthode

- Echanges à la fin de chaque point abordé
- Questions réponses
- Quizz/étude de cas
- Modalité pédagogique : Présentiel & Distanciel

### 2.3 Participants

- Salariés de l'entreprise
- Pré-requis : aucune connaissance particulière
- Durée : 1 journée
- 9 participants maximum par session

### 2.4 Prérequis

Avant de suivre cette formation, les stagiaires devront avoir été sensibilisés au RGPD (voir programme de formation « Initiation au RGPD »).

## 3 DEROULE DE LA FORMATION RGPD/SECURISATION DES DONNEES

---

### 1. Le champ d'application du RGPD

- 1.1. Quoi
- 1.2. Qui
- 1.3. Où
- 1.4. Quand
- 1.5. Pourquoi

## **2. Les principes**

- 2.1. Les fondements juridiques
  - 2.1.1. Mission d'intérêt public
  - 2.1.2. Obligation légale
  - 2.1.3. Contrat
  - 2.1.4. Consentement
  - 2.1.5. Intérêt légitime
- 2.2. Les droits des personnes
  - 2.2.1. Le droit d'information
  - 2.2.2. Le droit d'accès
  - 2.2.3. Le droit d'opposition
  - 2.2.4. Le droit de rectification
  - 2.2.5. Le droit à la limitation
  - 2.2.6. Le droit de s'opposer au profilage
  - 2.2.7. Le droit à l'effacement
  - 2.2.8. Le droit à la portabilité
- 2.3. Les obligations du Responsable de Traitement
- 2.4. Les obligations du Sous-Traitant
- 2.5. Les sanctions

## **3. La mise en conformité**

- 3.1. Le DPO
  - 3.1.1. Définition
  - 3.1.2. Les missions
- 3.2. La cartographie des traitements
- 3.3. Les actions de mise en conformité
- 3.4. La gouvernance
  - 3.4.1. Le registre des failles de sécurité

## **4. L'identité numérique**

- 4.1. Identifier
- 4.2. Authentifier
- 4.3. Contrôler les accès

## **5. La gestion des mots de passe**

- 5.1. Le cycle de vie
- 5.2. Constituer un mot de passe
- 5.3. Choix des mots de passe
- 5.4. D'autres méthodes d'authentification

## **6. La gestion de la messagerie**

- 6.1. Description d'un email
- 6.2. Utilisation de la messagerie

## **7. Comment éviter les menaces**

- 7.1. La cyber délinquance (quelques exemples)
- 7.2. Comment procède un attaquant
- 7.3. Quelques bonnes pratiques