

FORMATION « Sécurité des données personnelles » : Formation des employés

La sécurité des données personnelles dont vous êtes responsable face au **RGPD** au sein de votre entreprise dépend des moyens que vous avez mis en œuvre pour vous mettre en conformité avec le RGPD.

Parmi tous ces moyens, nombreux sont ceux qui dépendent des solutions informatiques dont vous avez équipé le système d'information de votre entreprise. Mais **les solutions électroniques de sécurité des données personnelles ne suffisent pas**, il faut **former votre équipe** afin que la gestion et la sécurité des données à caractère personnel dans votre entreprise soient un **réflexe naturel quotidien de la part de toutes vos ressources humaines**.

Sécurité des données personnelles : L'erreur humaine

L'**erreur humaine** est tellement présente au quotidien que le système d'information le plus performant en matière de sécurité ne suffit pas.



formation des employés à la gestion quotidienne des données à caractère personnel de l'entreprise pour leur sécurité

L'**ignorance décuple cette erreur humaine** et la rend incontrôlable et **inattaquable**.

En cas d'incident sur les données à caractère personnel dont vous êtes responsable issu d'une erreur de vos collaborateurs, vous n'aurez plus qu'à vous acquitter le l'amende de 4% de votre chiffre d'affaires affligée par la CNIL.

Former vos employés fait parti de vos responsabilités et fait partie à part entière de votre mise en conformité au RGPD. De plus, la vérification de votre conformité par vos clients, pour pouvoir continuer à travailler avec vous, **vous engage à avoir former votre personnel** sur la gestion et la sécurisation au quotidien des données à caractère personnel qu'ils manipulent tous les jours.

Enfin, **un employé formé** peut se voir soumettre un avenant à son contrat de travail qui **le rend pénalement responsable des erreurs** qu'il pourrait effectuer sur des données à caractères

personnel qui lui sont confiées dans le cadre de ses attributions. Cela pourra vous permettre de vous retourner contre lui en cas de manquement ayant des conséquences financières graves.

Dans le cadre de votre mise en conformité, je vous propose une formation de base de gestion et de sécurisation des données à caractère personnel au quotidien dans l'entreprise.

But de la formation :

Former les employés, en contact avec des données à caractère personnel au quotidien, à les gérer et les sécuriser.

Lieu :

Dans vos locaux sur votre vidéo projecteur

Ou salle Raymond Tache à COLLERET selon les besoins

Taille des groupes :

Jusqu'à 10 personnes par demi-journée

Programme de la formation :

1. Les données personnelles

1. Définition d'une donnée à caractère personnel
2. Définition d'un **traitement** de données à caractère personnel
3. Définition d'une violation de données à caractère personnel
4. La sécurisation des données à caractère personnel
5. Les conséquences d'une fuite de données à caractère personnel
6. Les engagements des salariés exigés par les employeurs
 - 6.1. Signatures d'engagements de confidentialité
 - 6.2. Conséquences du non respect des engagements de confidentialités

2. Méthodes de sécurisation des données à caractère personnel

1. Au bureau
2. Accueil clients en face à face
3. Au téléphone
 - 3.1. L'environnement
 - 3.2. Enregistrement des données à caractère personnel

4. La navigation sur internet
5. La réception d'email
 - 5.1. Déceler un hameçonnage
 - 5.2. Ne jamais faire
6. Les envois d'email
 - 6.1. Ne jamais utiliser son adresse personnelle à des fins professionnelles.
 - 6.2. Vérifier la sécurité de l'adresse du destinataire
 - 6.3. Relecture des destinataires
 - 6.4. Vérification des pièces jointes
 - 6.5. Chiffrage des pièces jointes sensibles
7. Les mots de passe et identifiants
 - 7.1. Définition
 - 7.2. Confidentialité
 - 7.3. Méthode de saisie
 - 7.4. Comment construire un mot de passe facile à retenir ?
 - 7.5. Ce qu'il ne faut pas faire
 - 7.6. Les gestionnaires de mot de passe
8. En déplacement
 - 8.1. Avant de partir
 - 8.2. Pendant le voyage
 - 8.3. Après le voyage
9. Les postes informatiques de travail
 - 9.1. Séparer les usages personnels de vos usages professionnels
 - 9.2. Le poste fixe de l'entreprise
 - 9.3. L'ordinateur portable fourni par l'entreprise
 - 9.4. L'utilisation du scanner pour la numérisation de documents
 - 9.5. L'impression de documents au sein de l'entreprise

3. Les violations de données à caractère personnel

1. Comment reconnaître une violation de données à caractère personnel
2. Comment réagir face à une violation de données à caractère personnel
 - 2.1. Identifier les dossiers et fichiers concernés
 - 2.2. Alerter votre supérieur.