RGPD POUR LES COLLABORATEURS

Durée
3.50 heures (0.5 jour)

Profils des apprenants
- Collaborateurs administratifs, commerciaux, RH, managers, agents d'accueil, équipes support ou opérationnelles.
- Toute personne amenée à manipuler des données personnelles dans son activité professionnelle.
- Salariés utilisant des outils numériques, fichiers clients, dossiers salariés, bases de données, CRM, logiciels métiers ou plateformes internes.
- Collaborateurs devant appliquer les consignes internes relatives à la confidentialité, à la sécurité des informations et à la protection des données.

Prérequis
- Aucun prérequis juridique ou technique.
- Une utilisation courante des outils numériques professionnels est recommandée.

Processus :
Recueil de besoin, validation prérequis, devis/convention, convocation. Pour toute inscription contacter notre service commercial sur contact@axio-protech.com. Délai d'accès: 3 semaines. Personnalisation via DUERP/consignes site.

Modalités d'accès aux personnes en situation de handicap :
Pour les personnes en situation de handicap, nous étudions les actions que nous pouvons mettre en place pour favoriser leur apprentissage à travers un questionnaire avant formation. Nous nous appuyons également sur un réseau de partenaires locaux.
Contact référent handicap: maud.hoffmann@axio-formation.com.

Qualité et indicateurs de résultats :
Taux de présence VS taux d'abandon, taux de satisfaction à chaud et à froid, taux de réussite à l'évaluation finale.

OBJECTIFS PÉDAGOGIQUES.

- Comprendre les principes fondamentaux du RGPD.
- Identifier les données personnelles et les données sensibles dans leur activité professionnelle.
- Reconnaître les principaux traitements de données réalisés au quotidien.
- Appliquer les bons réflexes de confidentialité, de sécurité et de limitation des données.
- Réagir correctement face à une demande d'exercice de droits ou à un incident de sécurité.
- Contribuer à la conformité RGPD de l'entreprise dans leur périmètre d'action.

CONTENU DE LA FORMATION.

1. Comprendre le RGPD et ses enjeux

- Origine et objectifs du RGPD.
- Pourquoi les entreprises doivent protéger les données personnelles.
- Les risques pour l'entreprise : sanctions, perte de confiance, atteinte à l'image, incidents de sécurité.
- Les risques pour les personnes concernées : usurpation d'identité, discrimination, divulgation d'informations confidentielles.
- Le rôle des collaborateurs dans la protection des données.
- Différence entre sensibilisation RGPD, conformité juridique et mission du DPO.

2. Identifier les données personnelles dans son activité

- Définition d'une donnée personnelle.
- Exemples de données personnelles : nom, prénom, email, téléphone, adresse, numéro client, matricule, photo, adresse IP, données de connexion.
- Définition des données sensibles : santé, origine, opinions, données biométriques, données syndicales, etc.
- Identification des données personnelles dans les outils professionnels.
- Comprendre la notion de traitement de données.
- Exemples de traitements quotidiens : envoyer un email client, gérer une candidature, tenir un fichier salarié, partager une liste de contacts, créer un compte utilisateur.

3. Connaître les grands principes du RGPD

- Licéité, loyauté et transparence.
- Finalité du traitement : utiliser les données uniquement pour un objectif défini.
- Minimisation des données : ne collecter que les informations nécessaires.
- Exactitude des données : veiller à la fiabilité des informations utilisées.
- Limitation de la durée de conservation.
- Intégrité et confidentialité des données.
- Responsabilité de l'entreprise et traçabilité des actions.
- Notion de base légale : consentement, contrat, obligation légale, intérêt légitime, mission d'intérêt public, sauvegarde des intérêts vitaux.
- Ce qu'un collaborateur peut faire ou ne doit pas faire avec une donnée personnelle.

4. Appliquer les bons réflexes au quotidien

- Vérifier les destinataires avant l'envoi d'un email contenant des données personnelles.
- Éviter les envois groupés visibles lorsque cela n'est pas justifié.
- Utiliser les outils validés par l'entreprise.
- Ne pas transférer de données professionnelles vers une messagerie personnelle.
- Limiter les exports inutiles de fichiers clients, RH, apprenants ou fournisseurs.
- Protéger les documents papier contenant des données personnelles.
- Verrouiller sa session en cas d'absence.
- Utiliser des mots de passe robustes et respecter les consignes internes.
- Ne pas partager ses identifiants.
- Classer, archiver ou supprimer les documents selon les règles internes.
- Respecter la confidentialité des données consultées dans le cadre de son poste.
- Demander conseil en cas de doute avant de transmettre ou réutiliser une donnée.

5. Comprendre les droits des personnes

- Droit d'accès, de rectification, d'effacement, d'opposition.
- Droit à la limitation du traitement et à la portabilité.
- Droit de retirer son consentement lorsque le traitement repose sur le consentement.
- Les bons réflexes lorsqu'un client, salarié, candidat, fournisseur ou usager exerce un droit.
- Pourquoi le collaborateur ne doit pas répondre seul à une demande complexe.
- Transmission de la demande au bon interlocuteur : manager, service juridique, DPO ou référent interne.

6. Réagir face à un incident ou une situation à risque

- Définition simple d'une violation de données.
- Exemples d'incidents fréquents : email envoyé à la mauvaise personne ; fichier partagé publiquement par erreur ; ordinateur ou clé USB perdu ; phishing visant des données clients ou salariés.
- Les bons réflexes à adopter.
- Comprendre l'importance du délai de 72 heures en cas de notification à la CNIL lorsque la violation présente un risque pour les personnes.
- Savoir distinguer une erreur mineure d'une situation à signaler rapidement.

ÉQUIPE PÉDAGOGIQUE.

Notre équipe pédagogique maîtrise l'ensemble des sujets proposés à la formation. Nous construisons nos programmes en identifiant les besoins en compétences des futurs apprenants et en collaboration avec nos experts métiers.

Pour tout besoin lié à la pédagogie, notre référente est Maud : maud.hoffmann@axio-formation.com (également référente handicap)
Pour tout besoin d'ordre administratif ou logistique, notre référente est Emilie : emilie.vannieuwenborg@axio-formation.com

Moyens pédagogiques et techniques

- **En présentiel :** - Accueil des participants dans une salle dédiée à la formation ou en entreprise - Documents supports de formation projetés - Analyse d'exemples d'incidents de violation de données - Etudes de cas concrets - Quizz et activités collectives en salle - Mise à disposition en ligne de documents supports à la suite de la formation
- **En distanciel :** - Classes virtuelles via l'interface Digiforma - Support de formation partagé - Activités d'entrainement en synchrone - Etudes de cas concrets - Messagerie instantanée permettant de dialoguer avec le formateur et les autres apprenants (si collectif)
- **En intra-entreprise**, les exemples et exercices peuvent être adaptés à l'environnement réel de l'entreprise : quais, zones d'attente, entrepôts, flux piétons/engins, organisation interne, protocole de sécurité et consignes spécifiques.

Dispositif de suivi de l'exécution de l'évaluation des résultats de la formation

- Feuilles d'émargement.
- Autoévaluation de positionnement en début et fin de formation.
- Exercices d'application tout au long de la formation.
- Questionnaire de satisfaction à chaud et à froid.
- Remise d'une attestation de formation à l'issue du parcours.
- Évaluation finale des acquis réalisée le jour de la formation, en fin de session, permettant de vérifier la capacité du participant à identifier les données personnelles, appliquer les bons réflexes de sécurité et réagir correctement face à une demande ou un incident.
- L'évaluation finale comprend : - Un QCM de validation des acquis portant sur les principes du RGPD, les droits des personnes, la confidentialité, la sécurité des données et les situations à risque. - Une étude de cas courte : erreur d'envoi d'un email, fichier partagé par erreur, demande d'accès d'un client ou perte d'un document contenant des données personnelles.
- Cette formation ne prépare pas à la fonction de DPO et ne constitue pas un audit de conformité RGPD. Elle vise à sensibiliser les collaborateurs et à vérifier l'acquisition des bons réflexes professionnels dans leur périmètre d'activité.
- L'organisme Axio PROTECH forme et évalue les participants dans le cadre de mises en situation pédagogiques. L'employeur reste responsable de l'application des procédures internes, des autorisations nécessaires et des conditions de sécurité sur le site.