

Formation : Protection des données personnelles, les bonnes pratiques à appliquer au quotidien

Cours de synthèse - 3h30 - Réf. 9DP

Prix : 350 € H.T.

L'article 32 du Règlement général sur la protection des données (RGPD) impose aux entreprises la mise en œuvre de moyens de sécurité défensifs. Découvrez quels sont les enjeux et les bonnes pratiques à mettre en place au quotidien.

Objectifs pédagogiques

À l'issue de la formation, le participant sera en mesure de :

- ✓ Comprendre ce qu'est l'identité numérique et les risques liés
- ✓ Connaître les bonnes pratiques au quotidien, dans sa vie personnelle et professionnelle, pour protéger ses données
- ✓ Connaître les gestes essentiels en cas de fuite de données

Public concerné

Toute personne souhaitant comprendre les enjeux de la protection des données personnelles.

Prérequis

Aucune connaissance particulière.

Méthodes et moyens pédagogiques

Méthodes pédagogiques

Conférence avec temps d'échange avec les participants.

Modalités d'évaluation

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques...

Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

Programme de la formation

PARTICIPANTS

Toute personne souhaitant comprendre les enjeux de la protection des données personnelles.

PRÉREQUIS

Aucune connaissance particulière.

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques...

Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

1 Comprendre le contexte

- Qu'est-ce qu'une identité numérique ?
- Pourquoi le RGPD ?
- Rappel du rôle de la CNIL.
- Que sont les données à caractère personnel et les données sensibles selon la CNIL ?

2 Les bonnes pratiques au quotidien

- Le risque en cybersécurité : vulnérabilités/menace/impacts. L'ingénierie sociale.
- Reconnaître un phishing/vishing vous demandant des données personnelles.
- La gestion des mots de passe.
- La veille sur votre identité numérique.
- Autres recommandations dans la vie professionnelle : conservation des données, cloisonnement...

3 Fuite de donnée, que faire ?

- Je suis victime d'une fuite ou d'une attaque sur mon identité numérique : porter plainte, déclaration à la CNIL...
- Mon entreprise est victime d'une fuite de données : les premiers gestes.
- Gestion des cyber-crisis (cellule de crise, plan de communication).
- Que dit la loi ?

MOYENS PÉDAGOGIQUES ET TECHNIQUES

- Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les formations pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
- À l'issue de chaque formation ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.
- Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le participant a bien assisté à la totalité de la session.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Pour toute question ou besoin relatif à l'accessibilité, vous pouvez joindre notre équipe PSH par e-mail à l'adresse psh-accueil@orsys.fr.