Exposées à des attaques virtuelles permanentes, les entreprises ont fort à faire pour protéger efficacement les données de leurs utilisateurs. Comprendre la cybercriminalité et ses risques est la meilleure manière de mieux se protéger. Avec Expertisme, découvrez comment mettre en place les bonnes actions et respecter les réglementations en vigueur.

## *Les enjeux d'une protection des données efficace*

La cybercriminalité est permanente dans la plupart des secteurs d'activité. Elle vise aujourd'hui de nombreuses entreprises sans distinction de taille. La cible des attaques : les données personnelles, qui représentent une importante source de valeur. Pour respecter la sensibilité de ces données, mais aussi les traiter en accord avec les souhaits des utilisateurs, les mesures adaptées doivent être connues et mises en place. Entre cadre réglementaire, habilitations et pratiques internes, le **bon traitement des données** est gage de plus de sérénité et de satisfaction utilisateur.

## *Les éléments clés d'une bonne protection des données*

Bien protéger ses données signifie à la fois connaître ses dispositifs déjà en place et le contexte réglementaire en vigueur. On pourra ainsi définir la **responsabilité de l'entreprise** sur les données et développer un dispositif adapté pour faire face aux potentielles menaces virtuelles.

### Connaître les exigences du RGPD pour ses données

Entré en application en 2018, le Règlement Général sur la Protection des Données impose un cadre au traitement de la data et donne davantage de contrôle aux utilisateurs sur leurs informations personnelles. C'est aujourd'hui lui qui guide la plupart des décisions prises en matière de sécurité des données. Comprendre **les notions clés du RGPD**, avec par exemple les questions de portabilité, de protection à la conception ou encore le rôle de la CNIL, est essentiel pour bien protéger les données et respecter les dispositions légales.

### Évaluer le niveau de protection déjà en place

Une fois les règles connues, mieux vaut s'assurer de les respecter. Au préalable, on procèdera bien sûr à une évaluation complète du niveau de sécurité en interne avant d'établir un plan d'action. Bonnes pratiques, **mode de recueil du consentement** selon votre organisation, situations de mobilité et gestion de crise sont autant de points clés pour savoir comment agir et réagir dans un contexte de cyberattaques fréquentes.

***« La sécurité des données est le grand sujet du moment. Le traiter correctement, c'est écarter les cybermenaces et pérenniser son organisation. »*** Laurent Rignault – fondateur et CEO d'Expertisme.

## *Faire de la cybersécurité une philosophie d'entreprise*

Au-delà des mesures technologiques, la cybersécurité s'appuie souvent sur des failles humaines et des mauvaises pratiques en interne. La manipulation – ou ingénierie sociale – est elle aussi à connaître pour ne pas se laisser surprendre.
Apprenez à **former et sensibiliser le personnel** pour que les mesures de sécurité soient appliquées en permanence. La définition de rôles et habilitation clairs pour tous les utilisateurs seront eux aussi importants pour protéger efficacement les données.

## *L'avis des experts d'Expertisme*

La **protection des données** se joue sur plusieurs fronts, et c'est justement ce qui la rend complexe. Le respect des lois doit guider les mesures prises sur le plan technologique, mais les bonnes pratiques quotidiennes doivent également intégrer la culture d'entreprise. Une connaissance pointue du RGPD et des procédures seront les meilleurs alliés des organisations pour bien se préparer.
Les formations en cybersécurité dispensées par Expertisme couvrent aussi bien les aspects techniques qu'humains de la protection des données. De l'audit de votre organisation à la création d'un plan d'action et au suivi durant 12 mois, assurez-vous de ne rien manquer des mesures clés de protection de vos données.

**N'hésitez-pas à nous contacter pour nous faire part de vos besoins en formations digitales.**