Protection des données – RGPD

La RGPD est le règlement général sur la protection des données, elle a pour but de renforcer la protection des données personnelles et à harmoniser les règles en Europe. Elle agit sur toutes les entreprises travaillant ou passant par l'Europe.

// La protection des données personnelles est un enjeu majeur pour les entreprises, qui doivent garantir leur sécurité tout en respectant la réglementation le RGPD. Un manquement peut entraîner des risques juridiques, financiers et réputationnels.

Les données personnelles sont des données personnelles et sensibles permettant de vous identifier, de près ou de loin. Les données personnelles comprennent les données de types médicales, d'identification, financières, biométriques, géolocalisation et numériques. Les données sensibles comprennent le genre, la religion et le parti politique. Par ailleurs, il faut savoir que les risques encourus sont le vol d'identité, le piratage et la cyberattaque, la fraude financière, l'atteinte à la vie privée, l'usurpation et chantage, et l'exploitation par des entreprises ou gouvernements. De plus, il faut savoir que toutes données servent à des fins commerciales. Afin de pouvoir s'en protéger de ces attaques, on peut mettre en place un chiffrement des données avec BitLocker, une gestion sécurisée des mots de passe avec un coffre-fort ou double authentification, en utilisant un pare-feu et une protection des réseau en le segmentant, en faisant des sauvegardes des données avec un stockage sécurisé, se protéger contre les cyberattaques avec une détection des intrusions ou antivirus, et en faisant une gestion des accès et surveillance avec un audit de sécurité. De plus, il faut mettre ne place une politique de confidentialité qui permet de comprendre et respecter les politiques internes, de sécuriser les données et les communications, de contrôler l'accès aux informations sensibles, de protéger les équipements et les infrastructures, de respecter les réglementations en vigueur, et de réagir en cas de violation de données.

La RGPD est établit avec ces grandes lois : la licéité, la loyauté et la transparence de l'information, la limitation des finalités, la minimisation des données, l'exactitude des données, la limitation de la conservation, et la sécurité et confidentialité. En tant qu'utilisateur, la RGPD nous donne accès à ces droits : droit d'accès, droit de rectification, droit d'effacement, droit de portabilité, droit d'opposition.

//

Chiffrement des données sensibles → Utiliser des outils comme **BitLocker** pour protéger les fichiers et disques durs contre l'accès non autorisé.

Gestion sécurisée des mots de passe → Employer un **gestionnaire de mots de passe** et activer la **double authentification** pour les accès critiques.

Protection réseau et pare-feu → Segmenter le réseau et configurer un **pare-feu** pour prévenir les intrusions et limiter les accès non autorisés.

Sauvegarde régulière des données → Mettre en place une stratégie de sauvegarde avec un **stockage sécurisé** pour éviter la perte définitive en cas de cyberattaque.

Audit et surveillance de la sécurité → Effectuer des **contrôles réguliers**, analyser les journaux d'accès et détecter les intrusions avec des outils spécialisés.

Navigation internet / usage pro-perso

De nos jours, utiliser une connexion wifi public en entreprise crée une ouverture pour les malwares, phishing, vols de données sensibles, et des failles de sécurités. Même en allant sur un site malveillant sans faire attention à l'url suspecte, l'absence de HTTPS, et contenu ou design incohérent.

// Suite à une mauvaise utilisation de l'équipement informatique, l'entreprise s'expose à des risques de sécurité, pouvant entraîner la perte de données, des cyberattaques ou des failles compromettant son activité.

Pour s'en prémunir, il a l'installation d'antivirus et de maintenir son matériel à jour, cela permet d'avoir une protection contre les logiciels malveillants et corrige les failles de sécurités.

Lorsqu'on est amené à faire un déplacement professionnel, il faut faire attention aux Wi-Fi publics qui sont non sécurisés, car on peut ouvrir une brèche pour le vol de données, également faire attention à son matériel pour éviter le vol ou la parte de l'appareil contenant des données sensibles.

Pour s'en prémunir, il faut utiliser un VPN afin de sécuriser la connexion réseau, puis d'éviter le plus possible de s'y connecter sans protection, et activer l'authentification à double facteurs sur les comptes professionnels.

//

Vérifier la sécurité des sites web → Toujours s'assurer de la présence du **HTTPS** dans l'URL et éviter les sites au design incohérent.

Installer un antivirus et effectuer des mises à jour régulières → Protection efficace contre les **logiciels malveillants** et correction des failles de sécurité.

Éviter les connexions sur les Wi-Fi publics non sécurisés → Risque de vol de données et d'interception des informations sensibles.

Utiliser un VPN en déplacement → Sécurisation des échanges réseau et protection des données transmises.

Activer l'authentification à double facteur (2FA) → Renforcement de la sécurité des comptes professionnels pour éviter les accès frauduleux.