Parcours TAI – Module Cybersécurité et RGPD

Activité 1 – La RGPD et la protection des données en entreprise

Partie 1 : Protéger les données personnelles, pourquoi et comment ?

-Pourquoi les données personnelles sont-elles considérées comme précieuses ? Donnez des exemples concrets de données sensibles.

Les données personnelles sont considérées comme précieuses car elles contiennent les données de type :

-Médicales (dossiers de santé, résultats d'examens) ;
-Identification (nom, prénom, adresse, numéro de téléphone) ;
-Financières (numéro de CB, relevés bancaires) ;
-Biométriques (empreintes digitales, reconnaissance faciale) ;
-Géolocalisation (suivi GPS, historique de déplacements) ;
-Numériques (historique de navigation, publications sur les réseaux sociaux).

Elles peuvent identifier une personne et exploitées à des fins commerciales, politiques, ou malveillantes.

-Quels risques encourt-on en cas de mauvaise gestion ou divulgation des données personnelles ?

Les risques encourus sont :

-Vol d'identité : usurpation d'identité pour des fraudes financières ;
-Piratage et cyberattaque : accès non autorisé aux comptes et fichiers ;
-Fraude financière : utilisation abusive des données bancaires ;
-Atteinte à la vie privée : exploitation des données sans consentement ;
-Usurpation et chantage : utilisation des données pour manipuler ou nuire ;
-Exploitation par des entreprises ou gouvernements : profilage et surveillance.

-En tant que TAI, quelles bonnes pratiques dois-tu adopter pour protéger les données stockées sur un poste ou un réseau ?

Les bonnes pratiques à adopter sont :

-Sécurisation du système et des accès (mots de passe forts, authentification à 2 facteurs)
-Protection contre les cyberattaques (antivirus, pare-feu, mises à jour régulières)
-Sauvegarde et récupération des données (stockage sécurisé, tests de restauration)
-Protection contre les accès physiques non autorisés (verrouillage automatique, chiffrement des disques)
-Surveillance et gestion des incidents (journalisation, détection des intrusions)

-Quels outils ou configurations techniques peux-tu mettre en place pour assurer la confidentialité et la sécurité des données (sauvegarde, chiffrement, mot de passe, pare-feu, etc…) ?

Les outils et configuration techniques pouvant être mis en place sont :

-Chiffrement des données (BitLocker, VeraCrypt, SSL/TLS)
-Gestion sécurisée des mots de passe (Gestionnaires de mots de passe, 2FA)
-Pare-feu et protection réseau (firewall matériel et logiciel, segmentation réseau)
-Sauvegarde des données (règles des 3-2-1, stockage sécurisé)
-Protection contre les cyberattaques (antivirus, SIEM, détection des intrusions)
-Gestion des accès et surveillance (RBAC, ACL, audits de sécurité)

-Pourquoi faut-il éviter de partager certaines données en ligne, même sur des plateformes dites « sûres » ?

Il faut éviter de partager des données en ligne sur n'importe quel site même « sûr » car :

-Risque de fuite de données : aucune plateforme n'est totalement sécurisée
-Exploitation commerciale et suivi : profilage publicitaire et revente des données
-Perte de contrôle sur les informations : données difficiles à supprimer une fois publiées
-Risques de piratage et d'usurpation d'identité : accès frauduleux aux comptes
-Risques liés aux réseaux sociaux et vie privée. : surveillance et manipulation

-Comment t'assurer que tu respectes les politiques de confidentialité mises en place dans une entreprise ?

Pour m'assurer le respect des politiques de confidentialités dans l'entreprise :

-Comprendre et respecter les politiques internes,
-Sécuriser les données et les communications,
-Contrôler l'accès aux informations sensibles,
-Protéger les équipements et les infrastructures,
-Respecter les réglementations en vigueur,
-Réagir en cas de violation de données.

Partie 2 : Comprendre le RGPD et son rôle

-A quoi sert le RGPD ? Présente le contexte de sa création et les objectifs visés

Légalement, la loi Informatique et Liberté (janvier 1978) étant obsolète, le RGPD est adopté en 2018. Il vise à renforcer la protection des données personnelles et à harmoniser les règles en Europe.

Objectifs :

-Renforcer le contrôle des citoyens sur leurs données
-Responsabiliser les entreprises qui collectent des données
-Harmoniser la législation au sein de l'UE

-Améliorer la transparence sur l'utilisation des données
-Imposer des sanctions en cas de non-respect (jusqu'à 20M€ ou 4% du CA)

-Quels sont les 6 grands principes du RGPD ? Donne une explication concrète pour chacun

1er grand principe : Licéité, loyauté et transparence : collecte légale et transparente des données

2ième grand principe : Limitation des finalités : utilisation des données uniquement pour un objectif précis

3ième grand principe : Minimisation des données : collecte uniquement des informations nécessaires

4ième grand principe : Exactitude des données : données à jour et correctes

5ième grand principe : Limitation de la conservation : suppression des données après la durée nécessaire

6ième grand principe : Sécurité et confidentialité : protection contre les accès non autorisés et les cyberattaques

-Quels droits le RGPD garantit-il aux personnes dont les données sont collectées ?
Uniquement sur consentement explicite entre l'entreprise et le client :
Droit de/d'/à : -Accès : consulter ses données

-Rectification : modifier ses informations

-L'effacement (oubli) : suppression des données

-La portabilité : transfert des données vers un autre service

-Opposition : refus de l'utilisation des données

-En tant que TAI, dans quelles situations peux-tu être amené à appliquer les règles du RGPD ?

En tant que TAI, je peux être dans ces situations pour appliquer les règles du RGPD :

-Gestion des demandes d'accès et de suppression des données
-Sécurisation des données et des systèmes
-Mise en conformité des logiciels et outils
-Gestion des incidents liés aux données personnelles
-Encadrement du transfert de données hors de l'Union Européenne
-Sensibilisation des employés et utilisateurs
-Vérification des politiques de confidentialité
-S'appuyer sur le DPO

-Quelles responsabilités as-tu vis-à-vis du traitement des données des utilisateurs ? Et que risques-tu en cas de non-respect ?

Responsabilités du TAI	Risques en cas de non-respect
Respect des principes du RGPD	Sanctions financières (jusqu'à 20M€ ou 4% du CA)
Sécuriser les données et les accès	Atteinte à la réputation et perte de confiance
Assurer la transparence et l'information	Actions en justice et plaintes des utilisateurs
Limiter la conservation des données	Obligation de correction immédiate
Gérer les demandes des utilisateurs	Violation de données -> Notification sous 72h
Encadrer le transfert des données	Amende et interdiction de traitement des données
Devoir d'alerte	

-Comment une entreprise peut-elle prouver qu'elle respecte le RGPD (notion de « traçabilité » ou « accountability ») ?

Pour prouver qu'elle respecte le RGPD, il existe :

-la documentation et politique de confidentialité,
-le registre des traitements,
-la gestion des violations de données,
-les droits des utilisateurs,
-la sensibilisation et formation des employés,
-les audits et contrôles réguliers.