RGPD

Équipe de travail :

Amandine Satin (Méthodes à appliquer, questions 1 et 2)
Dylan Capron (Règlement RGPD, questions 3 et 4)
Laurent Fauveau (Présentation RGPD, questions 5 et 6)

Introduction

C’est quoi le RGPD?

R = Règlement
G = Général
P = Protection
D= Données

Le **RGPD** (Règlement Général sur la Protection des Données) est une réglementation européenne adoptée en 2016 et appliquée depuis 2018.
Elle vise à renforcer et unifier la protection des données personnelles des individus au sein de l'Union Européenne.

Le **RGPD** impose des obligations strictes aux entreprises concernant la collecte, le traitement et la conservation des données personnelles, tout en garantissant aux individus des droits accrus sur leurs données (comme le droit d'accès, de rectification et d'effacement).

Les entreprises doivent également assurer la sécurité des données et signaler rapidement les violations de données.

I - Les règles

1. Champ d'Application

- Le RGPD s'applique à toute organisation traitant des données personnelles de résidents de l'UE, indépendamment du lieu où l'organisation est basée.

2. Consentement

- Les données personnelles ne peuvent être collectées et traitées qu'avec le consentement explicite des individus. Ce consentement doit être libre, spécifique, informé et sans ambiguïté.

3. Droits des Personnes

- **Droit à l'information**: Les individus doivent être informés sur la collecte et l'utilisation de leurs données personnelles.
- **Droit d'accès**: Les individus ont le droit d'accéder à leurs données personnelles et de savoir comment elles sont traitées.
- **Droit de rectification**: Les individus peuvent demander la correction de données inexactes ou incomplètes.
- **Droit à l'effacement**: Les individus peuvent demander la suppression de leurs données dans certaines circonstances.
- **Droit à la limitation du traitement**: Les individus peuvent demander la restriction du traitement de leurs données.
- **Droit à la portabilité des données**: Les individus peuvent demander que leurs données soient transférées à une autre organisation.
- **Droit d'opposition**: Les individus peuvent s'opposer au traitement de leurs données dans certaines conditions, notamment en ce qui concerne le marketing direct.
- **Droit de ne pas être soumis à une décision automatisée**: Les individus ont le droit de ne pas être soumis à des décisions automatisées sans intervention humaine.

4. Obligations des Responsables du Traitement et des Sous-Traitants

- Les organisations doivent mettre en place des mesures techniques et organisationnelles pour protéger les données personnelles.
- Elles doivent tenir un registre des activités de traitement.
- En cas de violation de données, les autorités compétentes doivent être notifiées dans les 72 heures.
- La désignation d'un Délégué à la Protection des Données (DPD) est obligatoire dans certains cas.

5. Transferts Internationaux de Données

- Les transferts de données personnelles en dehors de l'UE sont strictement réglementés et ne peuvent avoir lieu que si des garanties appropriées sont en place.

II/ Les méthodes

1. Audit des Données

Objectif : Identifier et documenter les données personnelles collectées, les méthodes de collecte, les processus de traitement, et les flux de données.

Étapes :

- **Identification des données collectées :** Créer un inventaire des données personnelles traitées par l'organisation (nom, adresse, email, etc.).
- **Cartographie des flux de données :** Visualiser le parcours des données depuis leur collecte jusqu'à leur suppression.
- **Analyse des processus de traitement :** Examiner comment les données sont utilisées, par qui, et à quelles fins.
- **Évaluation des risques :** Identifier les points de vulnérabilité et les risques potentiels pour la sécurité des données.

2. Nommer un Délégué à la Protection des Données (DPO)

Objectif : Assurer la conformité continue et servir de point de contact avec les autorités et les individus concernés.

Rôles du DPO :

- **Supervision de la conformité :** Veiller à ce que les politiques et les procédures soient conformes au RGPD.
- **Formation et sensibilisation :** Informer et former le personnel sur les obligations légales et les bonnes pratiques en matière de protection des données.
- **Conseil sur les DPIA :** Aider à la réalisation des analyses d'impact sur la protection des données.
- **Contact avec les autorités :** Servir de liaison avec les autorités de protection des données.

3. Mise en Œuvre de Politiques et Procédures

Objectif : Formaliser les pratiques de gestion des données pour garantir la protection des données personnelles.

Actions à Entreprendre :

- **Rédaction de politiques de confidentialité :** Élaborer des politiques claires expliquant comment les données sont collectées, utilisées, et protégées.
- **Procédures de gestion des données :** Mettre en place des procédures pour l'accès, la modification, et la suppression des données personnelles.
- **Plan de réponse aux incidents :** Développer un plan pour gérer et notifier les violations de données.

4. Formation et Sensibilisation

Objectif : Assurer que tous les employés comprennent l'importance de la protection des données et connaissent leurs responsabilités.

Programme de Formation :

- **Sensibilisation générale :** Informer sur les principes de base du RGPD et les droits des individus.
- **Formation spécifique :** Former les employés ayant des rôles spécifiques (IT, marketing, RH) sur les pratiques de protection des données pertinentes pour leurs tâches.
- **Mises à jour régulières :** Offrir des sessions de formation continue pour maintenir le niveau de connaissance et de vigilance élevé.

5. Contrats avec les Sous-Traitants

Objectif : S'assurer que les sous-traitants respectent également les exigences du RGPD.

Mesures à Prendre :

- **Clauses contractuelles :** Inclure des clauses spécifiques sur la protection des données dans les contrats avec les sous-traitants.
- **Vérifications régulières :** Effectuer des audits et des évaluations régulières des pratiques des sous-traitants.
- **Accords de traitement des données :** Signer des accords de traitement des données pour clarifier les responsabilités et les obligations.

6. Analyse d'Impact sur la Protection des Données (DPIA)

Objectif : Évaluer les risques pour les droits et libertés des personnes concernées avant de lancer de nouveaux projets ou systèmes.

Processus de DPIA :

- **Description du traitement :** Détailler la nature, la portée, le contexte, et les finalités du traitement des données.
- **Évaluation des risques :** Identifier les risques pour les droits et libertés des individus.
- **Mesures d'atténuation :** Proposer des mesures pour atténuer les risques identifiés.
- **Documentation :** Documenter les résultats et les décisions prises.

7. Technologies de Sécurité

Objectif : Protéger les données personnelles contre les accès non autorisés, les altérations, et les pertes.

Technologies à Utiliser :

- **Chiffrement :** Utiliser le chiffrement pour protéger les données en transit et au repos.
- **Pare-feux et antivirus :** Mettre en place des pare-feux et des logiciels antivirus pour prévenir les attaques.
- **Contrôle d'accès :** Implémenter des systèmes de contrôle d'accès pour limiter l'accès aux données aux seules personnes autorisées.
- **Systèmes de détection d'intrusion :** Utiliser des IDS pour détecter les activités suspectes et prévenir les violations de données.

8. Révision Régulière

Objectif : S'assurer que les mesures de protection des données restent efficaces et conformes aux exigences du RGPD.

Activités de Révision :

- **Audits internes :** Réaliser des audits internes réguliers pour vérifier la conformité.
- **Mises à jour des politiques :** Réviser et mettre à jour les politiques de confidentialité et de protection des données en fonction des changements réglementaires et technologiques.
- **Tests de sécurité :** Effectuer des tests de pénétration et des évaluations de vulnérabilité pour identifier et corriger les failles de sécurité.

En suivant ces méthodes pratiques, les entreprises peuvent assurer une mise en œuvre efficace et continue du RGPD, garantissant ainsi la protection des données personnelles des individus et la conformité avec la réglementation européenne.

III/ Les Questions

1. À quelle réglementation est soumise la base de données d'un site d'e-commerce ? Et notamment la table d'utilisateurs ?

Pour un site d'e-commerce, la gestion de la base de données des utilisateurs doit se conformer à diverses réglementations pour protéger les données personnelles. Cela inclut l'obtention de consentement, la sécurisation des données, la garantie des droits des utilisateurs et la transparence des pratiques de traitement des données.

Règlement Général sur la Protection des Données (RGPD)

- **Applicabilité :** Toutes les entreprises traitant des données personnelles des résidents de l'UE.
- **Obligations :**
    - Consentement explicite des utilisateurs.
    - Droits d'accès, d'effacement, et de portabilité des données.
    - Sécurité des données et notification des violations.

Directives sur la Confidentialité et les Communications Électroniques (ePrivacy)

- **Applicabilité :** Complément au RGPD, se concentrant sur les communications électroniques et les cookies.
- **Obligations :**
    - Consentement pour les cookies.
    - Confidentialité des communications électroniques.

Loi Informatique et Libertés (France)

- **Applicabilité :** Alignée sur le RGPD avec des spécificités locales.
- **Obligations :**
    - Notification à la CNIL pour les traitements à haut risque.
    - Nomination d'un Délégué à la Protection des Données (DPO) si nécessaire.

CAN-SPAM Act (USA)

- **Applicabilité :** Régule les messages commerciaux non sollicités aux États-Unis.
- **Obligations :**
    - Possibilité de se désinscrire des communications commerciales.
    - Identification claire des messages commerciaux.

California Consumer Privacy Act (CCPA)

- **Applicabilité :** Entreprises traitant les données des résidents de Californie.
- **Obligations :**
    - Droits d'accès, de suppression, et de non-discrimination pour les consommateurs.
    - Notification des catégories de données collectées et de leurs fins.

2.Comment devez-vous stocker et sécuriser ces données ?

Pour protéger efficacement les données des utilisateurs d'un site d'e-commerce, il est crucial de combiner des mesures techniques et organisationnelles. Le chiffrement, les contrôles d'accès, les sauvegardes, et les mises à jour régulières sont des aspects techniques essentiels, tandis que la sensibilisation du personnel, la gestion des risques, et les audits des sous-traitants complètent la stratégie de sécurité globale. En suivant ces pratiques, les entreprises peuvent se conformer aux réglementations comme le RGPD et assurer la sécurité et la confidentialité des données personnelles.

<u>Mesures Techniques</u>

Chiffrement des Données

- **En Transit :** Utiliser le protocole HTTPS pour sécuriser les communications entre les utilisateurs et le serveur.
- **Au Repos :** Chiffrer les données stockées dans la base de données pour protéger les informations même si une personne non autorisée accède physiquement aux serveurs.

Contrôle d'Accès

- **Authentification Forte :** Utiliser l'authentification à deux facteurs (2FA) pour les accès administratifs.
- **Gestion des Droits :** Mettre en place des contrôles stricts pour garantir que seuls les employés autorisés peuvent accéder aux données sensibles.

Pare-feux et Systèmes de Détection d'Intrusion (IDS)

- **Pare-feux :** Utiliser des pare-feux pour protéger le réseau contre les accès non autorisés.
- **IDS :** Mettre en place des systèmes de détection d'intrusion pour identifier et réagir rapidement aux activités suspectes.

Sauvegardes Régulières

- **Plan de Sauvegarde :** Réaliser des sauvegardes régulières des données et les stocker dans des lieux sécurisés et distincts (par exemple, dans des centres de données différents).
- **Chiffrement des sauvegardes :** Chiffrer les sauvegardes pour protéger les données en cas de compromission des supports de sauvegarde.

Mises à Jour et Patches

- **Logiciels à jour :** Maintenir les logiciels et les systèmes à jour avec les derniers correctifs de sécurité pour éviter les vulnérabilités.

Mesures Organisationnelles

Politique de Sécurité de l'Information

- **Documentation :** Rédiger et maintenir une politique de sécurité de l'information détaillant les mesures de protection des données.
- **Sensibilisation :** Former les employés sur les bonnes pratiques de sécurité et la confidentialité des données.

Gestion des Risques

- **Évaluation des risques :** Réaliser régulièrement des évaluations des risques pour identifier les menaces potentielles et les faiblesses.
- **Plan de Réponse aux Incidents :** Mettre en place un plan de réponse aux incidents pour réagir rapidement et efficacement en cas de violation de données.

Analyses d'Impact sur la Protection des Données (DPIA)

- **DPIA :** Effectuer des DPIA pour les nouveaux projets ou les changements majeurs qui impliquent le traitement des données personnelles, afin d'identifier et de minimiser les risques pour les individus.

Contrats avec les Sous-Traitants

- **Clauses de Sécurité :** Inclure des clauses spécifiques de sécurité des données dans les contrats avec les sous-traitants.
- **Audits des Sous-Traitants :** Réaliser des audits réguliers des sous-traitants pour s'assurer qu'ils respectent les normes de sécurité.

3. Sont-elles publiques ?

Non, les données personnelles des utilisateurs ne sont pas publiques. Elles doivent être traitées de manière confidentielle et sécurisée, et ne peuvent être accessibles qu'aux personnes autorisées.

4. Pouvez-vous les vendre/distribuer à une entreprise partenaire ?

Non, la vente ou la distribution des données personnelles des utilisateurs à des entreprises partenaires n'est pas autorisée sans le consentement explicite des utilisateurs. Le RGPD exige que les utilisateurs soient informés et donnent leur consentement libre et éclairé avant que leurs données ne soient partagées avec des tiers.

5. Les données de la table de connexions sont-elles sensibles ? [laurent]

Oui, les données de la table de connexions peuvent être sensibles car elles peuvent inclure des informations personnelles comme les adresses IP, les horodatages, et les identifiants d'utilisateur, permettant d'identifier et de suivre les individus.

6. Devez-vous pouvoir les effacer ? [laurent]

Oui, selon le RGPD, vous devez pouvoir effacer les données de la table de connexions si elles contiennent des informations personnelles et si l'utilisateur en fait la demande (droit à l'effacement ou "droit à l'oubli").