Gaci Hanafi
Derri Tara

RGPD

INTRODUCTION

Aujourd'hui, la question des données personnelles et de leur protection est cruciale, même si beaucoup d'entre nous ne s'en rendent pas compte. Nos informations personnelles sont extrêmement précieuses pour de nombreuses entreprises, qui les utilisent pour mieux nous segmenter, cibler, et analyser nos comportements afin de mieux nous atteindre.

Mais alors, que change concrètement le RGPD dans notre vie ? Cette question mérite d'être posée.

Le RGPD transforme radicalement la situation en établissant des règles précises et en mettant l'accent sur le consentement et la transparence des traitements de données comme nous allons le voir dans cette documentation.

INTRODUCTION AU RGPD

Le Règlement Général sur la Protection des Données entré en vigueur le 25 mai 2018, est la loi de l'Union Européenne qui protège les données personnelles des citoyens. Il s'applique à toutes les organisations, qu'elles soient publiques ou privées, dès qu'elles traitent des données de résidents européens.

Le RGPD est directement applicable dans tous les pays de l'UE depuis 2018. Il encadre le traitement des données personnelles, incluant la collecte, l'organisation et l'utilisation de ces données. Se conformer au RGPD est une obligation légale pour toutes les entreprises.

En résumé, le RGPD est un cadre légal de l'UE pour protéger les données personnelles des citoyens. Il régit la collecte, le traitement et le stockage des données, exige le consentement des individus et impose des sanctions en cas de non-conformité.

PRINCIPES FONDAMENTAUX DU RGPD

Licéité, Loyauté et Transparence : Les données doivent être traitées de manière légale, loyale et transparente.

Limitation des Finalités : Les données doivent être collectées pour des finalités déterminées, explicites et légitimes.

Minimisation des Données : Les données collectées doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées.

Exactitude : Les données doivent être exactes et tenues à jour.

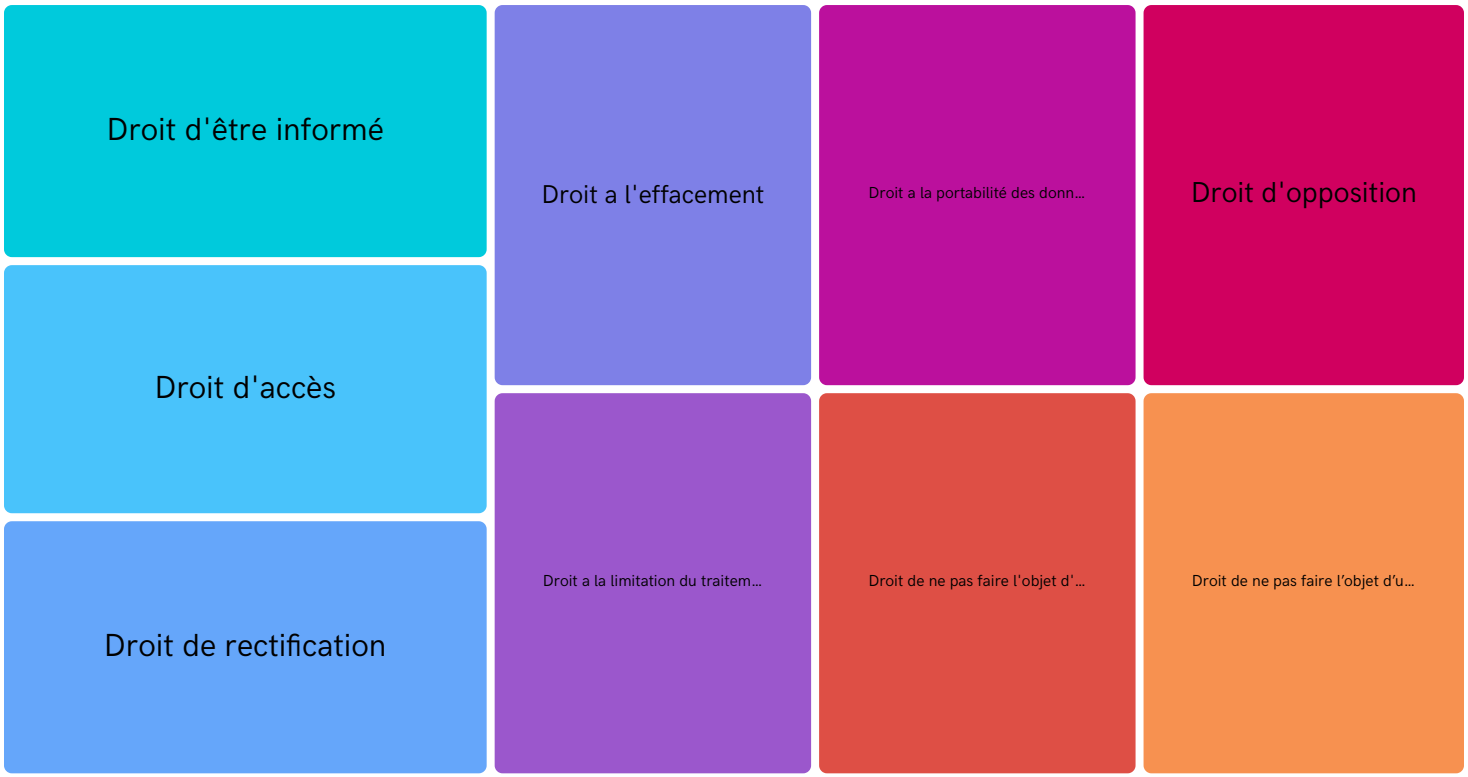
Limitation de la Conservation : Les données doivent être conservées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont traitées.

Intégrité et Confidentialité : Les données doivent être traitées de manière à garantir leur sécurité.

Responsabilité : Les responsables de traitement doivent être capables de démontrer la conformité au RGPD.

DROIT DES PERSONNES CONCERNÉES

Le RGPD prévoit les droits suivants aux personnes concernées, c'est-à-dire aux individus dont les données sont traitées :



PRINCIPALES REGLES DU RGPD

Principes Fondamentaux : Le RGPD impose des principes clés tels que la licéité, la loyauté et la transparence dans le traitement des données, la limitation des finalités, la minimisation des données collectées, l'exactitude, la limitation de la conservation, ainsi que l'intégrité et la confidentialité des données.

Droits des Personnes Concernées : Les individus bénéficient de droits forts, notamment le droit à l'information, d'accès, de rectification, d'effacement, de limitation du traitement, de portabilité des données, d'opposition et de protection contre les décisions automatisées.

Obligations des Responsables du Traitement et des Sous-Traitants : Les responsables du traitement doivent tenir un registre des activités, intégrer la protection des données dès la conception (Privacy by Design) et par défaut (Privacy by Default), mettre en place des mesures de sécurité appropriées, et être capables de démontrer la conformité au RGPD. Les sous-traitants doivent respecter les instructions des responsables de traitement et notifier les violations de données.

Évaluation et Gestion des Risques : L'Analyse d'Impact relative à la Protection des Données (AIPD) est nécessaire pour évaluer et atténuer les risques liés au traitement des données.

MÉTHODES PRATIQUES POUR ASSURER LA CONFORMITÉ AU RGPD

- **Documentation :** Tenir à jour un registre des activités de traitement et réaliser une AIPD lorsque nécessaire.
- **Gestion des Droits des Personnes Concernées :** Mettre en place des procédures pour répondre aux demandes d'exercice des droits des individus.
- **Sécurité des Données :** Appliquer des mesures techniques et organisationnelles appropriées pour protéger les données contre tout accès non autorisé, perte ou destruction.
- **Formation et Sensibilisation :** Sensibiliser le personnel aux obligations en matière de protection des données et à la sécurité de l'information.
- **Gestion des Sous-Traitants :** S'assurer que les contrats avec les sous-traitants incluent des clauses de protection des données conformes au RGPD.

NORMES ET REGLEMENTS ASSOCIÉS

ISO 27001

L'ISO/IEC 27001 est une norme internationale pour la gestion de la sécurité de l'information, fournissant un cadre pour protéger les informations sensibles. Voici ses points clés :

- **Système de Gestion de la Sécurité de l'Information (SGSI)** : ISO 27001 aide les organisations à établir, mettre en œuvre, entretenir et améliorer continuellement un SGSI. Elle impose une évaluation des risques de sécurité de l'information et la mise en place de mesures appropriées pour traiter ces risques.
- **Conformité et Sécurité** : L'ISO 27001 soutient la conformité au RGPD en renforçant la sécurité des données personnelles grâce à des mesures techniques et organisationnelles telles que le chiffrement, les contrôles d'accès, et la formation du personnel.

ANSSI

L'ANSSI est l'autorité nationale française en matière de sécurité des systèmes d'information. Elle joue un rôle crucial dans la protection des données et des infrastructures critiques :

- **Prévention et Réponse aux Incidents** : L'ANSSI coordonne la réponse aux cyberattaques et incidents de sécurité informatique, assurant une protection proactive des systèmes d'information.
- **Promotion des Bonnes Pratiques et Coopération Internationale** : Elle élabore des guides et recommandations, certifie des produits et services de sécurité, et collabore avec des agences internationales pour renforcer la cybersécurité globale

QUESTIONS:

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

La base de données d'un site d'e-commerce, incluant la table des utilisateurs, est soumise au RGPD si elle traite les données personnelles de résidents européens. Le RGPD impose des règles strictes sur la collecte, le traitement et la conservation de ces données pour garantir leur protection. Les entreprises doivent s'assurer que les données sont traitées conformément aux principes de licéité, loyauté et transparence, limitation des finalités, minimisation des données, exactitude, limitation de la conservation, et intégrité et confidentialité.

- [ ] **Comment devez-vous stocker et sécuriser ces données ?**

Les données doivent être stockées et sécurisées de manière à protéger leur confidentialité, intégrité et disponibilité. Cela inclut :

- **Chiffrement des données** : Utiliser des techniques de chiffrement pour protéger les données stockées et en transit.
- **Contrôle d'accès** : Restreindre l'accès aux données aux seules personnes autorisées et mettre en place des systèmes d'authentification robustes.
- **Sécurité des infrastructures** : Assurer que les serveurs et systèmes de stockage sont protégés contre les cyberattaques par des pare-feu, des logiciels antivirus et des mises à jour régulières.
- **Surveillance et audit** : Mettre en place des systèmes de surveillance pour détecter toute activité suspecte et effectuer des audits réguliers pour s'assurer de la conformité.

- [ ] **Sont-elles publiques ?**

Les données personnelles des utilisateurs ne sont pas publiques et doivent être protégées contre tout accès non autorisé. Le RGPD stipule que les données doivent être traitées de manière confidentielle et ne doivent être accessibles qu'aux personnes ayant une nécessité professionnelle d'y accéder. Toute

divulgation de données personnelles à des tiers nécessite le consentement explicite des individus concernés ou une autre base légale justifiée.

- [ ] **Pouvez-vous les vendre/distribuer à une entreprise partenaire ?**

La vente ou la distribution des données personnelles à des entreprises partenaires est soumise à des conditions strictes sous le RGPD. Cela nécessite généralement :

- **Consentement explicite** : Les utilisateurs doivent donner leur consentement explicite pour que leurs données soient partagées avec des partenaires.
- **Information et transparence** : Les utilisateurs doivent être informés de l'identité des partenaires et des finalités du partage des données.
- **Contrats de sous-traitance** : Les entreprises doivent s'assurer que les partenaires respectent également les obligations du RGPD par le biais de contrats de sous-traitance conformes.

- [ ] **Les données de la table de connexions sont-elles sensibles ?**

Les données de la table de connexions peuvent être considérées comme sensibles, notamment si elles incluent des identifiants uniques, des adresses IP, des horodatages de connexion, et d'autres informations susceptibles de permettre l'identification d'utilisateurs spécifiques ou d'exposer leurs habitudes de connexion. Ces données doivent donc être protégées de manière appropriée, conformément aux exigences du RGPD.

- [ ] **Devez-vous pouvoir les effacer ?**

Oui, les individus ont le droit de demander l'effacement de leurs données personnelles, en vertu du droit à l'effacement (droit à l'oubli) prévu par le RGPD. Les entreprises doivent mettre en place des procédures pour répondre à ces demandes dans les délais prescrits et s'assurer que les données sont complètement et définitivement supprimées, sauf si leur conservation est nécessaire pour respecter une obligation légale ou pour l'exercice ou la défense de droits en justice.