RGPD

RGPD - Enjeux de sécurité

Introduction du sujet

Ce projet est une recherche documentaire qui sert d'introduction à la sécurité des données, aux normes et règlements associées ; en gros à la DPO et au RGPD.

Projet

INTRODUCTION AU RGPD

Le Règlement Général sur la Protection des Données (RGPD) est né du besoin de moderniser les lois sur la protection des données dans l'Union européenne. Comparé aux anciennes lois, le RGPD vise à renforcer les droits des individus et à harmoniser les règles à travers l'UE. Ses principaux objectifs sont de protéger les données personnelles des citoyens européens et de responsabiliser les organisations qui les traitent.

PRINCIPES FONDAMENTAUX DU RGPD

Les principes du RGPD incluent :
- 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.
- 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.

DROITS DES PERSONNES CONCERNÉES

Le RGPD confère plusieurs droits aux individus :
- Droit à l'Information : Les individus doivent être informés de l'utilisation de leurs données.
- Droit d'Accès : Les individus ont le droit d'accéder à leurs données personnelles.
- Droit de Rectification : Les individus peuvent demander la correction de leurs données inexactes.
- Droit à l'Effacement (Droit à l'Oubli) : Les individus peuvent demander la

suppression de leurs données.
- Droit à la Limitation du Traitement : Les individus peuvent demander de limiter le traitement de leurs données.
- Droit à la Portabilité des Données : Les individus peuvent obtenir et réutiliser leurs données pour leurs propres besoins.
- Droit d'Opposition : Les individus peuvent s'opposer au traitement de leurs données dans certaines conditions.
- Droits Relatifs à la Prise de Décision Automatisée et au Profilage : Les individus ont le droit de ne pas être soumis à des décisions automatisées produisant des effets juridiques.

OBLIGATIONS DES RESPONSABLES DU TRAITEMENT ET DES SOUS-TRAITANTS

Les responsables du traitement doivent :
- Tenir un registre des activités de traitement.
- Intégrer les principes de "Privacy by Design" et "Privacy by Default".
- Mettre en place des mesures techniques et organisationnelles pour protéger les données.

Les sous-traitants doivent :
- Respecter les instructions des responsables de traitement.
- Mettre en œuvre des mesures de sécurité appropriées.
- Notifier les violations de données sans délai.

ÉVALUATION ET GESTION DES RISQUES

L'Analyse d'Impact Relative à la Protection des Données (AIPD) est nécessaire pour évaluer les risques liés aux traitements de données. Elle doit inclure :
- Une description des traitements et des finalités.
- Une évaluation de la nécessité et de la proportionnalité des traitements.
- Une évaluation des risques pour les droits et libertés des individus.
- Les mesures envisagées pour traiter ces risques.

IMPACT ET FUTUR DU RGPD

Le RGPD a un impact significatif sur les entreprises, les forçant à revoir leurs pratiques de gestion des données et à investir dans des mesures de conformité. Pour les consommateurs, le RGPD renforce leur contrôle sur leurs données personnelles, influençant positivement leur confiance envers les entreprises. Avec l'évolution technologique, notamment l'IA et le Big Data, la protection des données continuera d'évoluer, posant de nouveaux défis et opportunités pour la réglementation.

DOCUMENTATION FINALE

La documentation finale à produire doit résumer de manière professionnelle le RGPD, ses principales règles, ainsi que les méthodes pratiques pour assurer sa mise en œuvre efficace.

Puis pour finir, vous devez répondre aux questions qui sont ci-dessous.

Questions :

● À quelle réglementation est soumise la base de données d’un site d'e-commerce ? Et notamment la table d’utilisateurs ?
● Comment devez-vous stocker et sécuriser ces données ?
● Sont-elles publiques ?
● Pouvez-vous les vendre/distribuer à une entreprise partenaire ?
● Les données de la table de connexions sont-elles sensibles ?
● Devez-vous pouvoir les effacer ?

Rendu

Vous partagerez avec l’équipe pédagogique votre document de recherche et de réponse aux questions sur le drive.

Base de connaissances

➔ RGPD de quoi parle-t-on ?
➔ Le règlement général sur la protection des données - RGPD
➔ CNIL
➔ Hébergement de données de santé
➔ Certification HDS
➔ Règlement Général sur la Protection des Données (RGPD)
➔ Guide de la CNIL sur le RGPD
➔ Études de cas sur les violations du RGPD

Le RGPD, ou Règlement Général sur la Protection des Données (en anglais, GDPR pour General Data Protection Regulation), est une réglementation de l'Union européenne adoptée en avril 2016 et entrée en vigueur le 25 mai 2018. Il a pour objectif de renforcer et d'harmoniser la protection des données personnelles des individus au sein de l'Union européenne (UE).

Objectifs du RGPD

1. **Renforcement des droits des personnes** :
    - Droit d'accès : Les individus ont le droit de savoir quelles données sont collectées sur eux et comment elles sont utilisées.
    - Droit de rectification : Les individus peuvent demander la correction de leurs données personnelles si elles sont inexactes.
    - Droit à l'effacement (ou droit à l'oubli) : Les individus peuvent demander la suppression de leurs données personnelles sous certaines conditions.
    - Droit à la portabilité des données : Les individus peuvent demander à recevoir leurs données personnelles dans un format structuré, couramment utilisé et lisible par machine, et peuvent également demander que ces données soient transférées directement à un autre responsable de traitement.
    - Droit d'opposition : Les individus peuvent s'opposer au traitement de leurs données personnelles dans certains cas, notamment en ce qui concerne le marketing direct.
2. **Obligations des entreprises** :
    - Consentement : Les entreprises doivent obtenir le consentement explicite et éclairé des individus avant de collecter et de traiter leurs données personnelles.
    - Transparence : Les entreprises doivent informer les individus de manière claire et compréhensible sur la collecte et l'utilisation de leurs données.
    - Sécurité des données : Les entreprises doivent mettre en place des mesures techniques et organisationnelles appropriées pour protéger les données personnelles.

- Notification des violations de données : En cas de violation de données, les entreprises doivent notifier les autorités compétentes dans les 72 heures et, dans certains cas, informer les individus concernés.

3. **Sanctions** :
    - Le RGPD prévoit des sanctions sévères pour les entreprises qui ne se conforment pas à ses règles, avec des amendes pouvant atteindre 20 millions d'euros ou 4 % du chiffre d'affaires annuel mondial, selon le montant le plus élevé.

Champ d'application

Le RGPD s'applique à toutes les entreprises, organisations et entités, indépendamment de leur emplacement géographique, qui traitent des données personnelles de résidents de l'UE. Cela signifie que même des entreprises situées en dehors de l'UE doivent se conformer au RGPD si elles offrent des biens ou des services aux résidents de l'UE ou surveillent leur comportement.

Impacts

Le RGPD a eu un impact significatif sur la manière dont les entreprises et organisations gèrent les données personnelles. Il a conduit à une prise de conscience accrue de l'importance de la protection des données et a encouragé le développement de meilleures pratiques en matière de gestion des données personnelles. Les entreprises ont dû revoir et ajuster leurs politiques de confidentialité, mettre en place des mesures de sécurité renforcées, et souvent désigner un délégué à la protection des données (DPO).

En résumé, le RGPD vise à protéger les droits des individus en matière de données personnelles tout en imposant des obligations strictes aux entreprises et organisations qui collectent, traitent et stockent ces données.

Mise en place de protocoles RGPD :

Constituer un registre des traitements de données :

- Identifier les activités principales utilisant des données personnelles.
- Créer des fiches pour chaque activité en précisant l’objectif, les catégories de données, les accès et la durée de conservation.
- Le registre doit être maintenu à jour par le dirigeant en collaboration avec les différents responsables de traitement.

2. **Faire le tri dans les données** :
    - Vérifier que seules les données nécessaires sont collectées et éviter les données sensibles sans autorisation.
    - Limiter l’accès aux données aux personnes habilitées et définir des règles d’effacement ou d’archivage.

3. **Respecter les droits des personnes** :

- Informer les personnes sur la collecte de leurs données, les finalités, les accès et les durées de conservation.
- Faciliter l'exercice des droits des personnes (accès, rectification, opposition, etc.) via des formulaires ou des contacts spécifiques.

4. **Sécuriser les données** :
    - Mettre en place des mesures de sécurité adaptées à la sensibilité des données (mises à jour, mots de passe, chiffrement, sauvegardes).
    - Évaluer régulièrement le niveau de sécurité des données et préparer des procédures en cas d'incident.

5. **Signaler les violations de données** :
    - En cas de violation de données, la signaler à la CNIL dans les 72 heures et informer les personnes concernées si les risques sont élevés.

6. **Accompagnement spécifique des têtes de réseaux** :
    - La CNIL assiste les TPE et PME via des partenariats pour les aider à se conformer à la RGPD.

Les données Personnelles :

1. **Définition** :
    - Toute information se rapportant à une personne physique identifiée ou identifiable.
    - Identification possible directement (nom, prénom) ou indirectement (identifiant, numéro de téléphone, données biométriques).

2. **Exemples d'identification** :
    - Une seule donnée (numéro de sécurité sociale, ADN).
    - Croisement de plusieurs données (adresse, date de naissance, abonnements, activités).

3. **Traitement de données personnelles** :
    - Toute opération sur des données personnelles (collecte, enregistrement, organisation, etc.).
    - Chaque traitement doit avoir un objectif légal et légitime.

Exemples de traitement

1. **Opérations courantes** :
    - Gestion de clientèle (collecte d’informations pour livraison, facturation, fidélisation).
    - Tenue de fichiers clients, collecte de coordonnées via questionnaires, mise à jour de fichiers fournisseurs.
2. **Exclusions** :
    - Fichiers contenant uniquement des coordonnées d’entreprises ne sont pas des traitements de données personnelles.
    - Les fichiers papier sont également concernés et doivent être protégés de la même manière que les fichiers informatisés.

En résumé, les données personnelles englobent toute information permettant d'identifier une personne, directement ou indirectement, et leur traitement inclut diverses opérations qui doivent toujours avoir une finalité précise et légitime.

➔ RGPD de quoi parle-t-on ?
➔ Le règlement général sur la protection des données - RGPD
➔ CNIL
➔ Hébergement de données de santé
➔ Certification HDS
➔ Règlement Général sur la Protection des Données (RGPD)
➔ Guide de la CNIL sur le RGPD
➔ Études de cas sur les violations du RGPD

RGPD de quoi parle-t-on ?

Le RGPD (Règlement Général sur la Protection des Données) est un règlement de l'Union européenne visant à renforcer et unifier la protection des données pour les individus au sein de l'UE. Il établit des obligations pour les entreprises et organisations sur la manière de collecter, traiter et protéger les données personnelles.

Le règlement général sur la protection des données - RGPD

Le RGPD est une législation européenne entrée en vigueur le 25 mai 2018. Il remplace la directive de 1995 sur la protection des données et vise à donner aux citoyens plus de contrôle sur leurs données personnelles. Il impose également des obligations strictes aux entreprises sur la gestion et la sécurité des données personnelles.

CNIL

La CNIL (Commission Nationale de l'Informatique et des Libertés) est l'autorité française chargée de veiller à la protection des données personnelles et de la vie privée. Elle accompagne les professionnels dans la mise en conformité avec le RGPD et dispose de pouvoirs de sanction en cas de non-respect de la réglementation.

Hébergement de données de santé

L’hébergement de données de santé concerne la conservation et le traitement des données relatives à la santé des individus. En France, cet hébergement doit être réalisé par des prestataires certifiés HDS (Hébergement de Données de Santé), garantissant la sécurité et la confidentialité des informations médicales.

Certification HDS

La certification HDS (Hébergement de Données de Santé) est une certification française obligatoire pour les prestataires qui hébergent des données de santé. Elle garantit que le prestataire respecte des normes strictes de sécurité et de protection des données.

Règlement Général sur la Protection des Données (RGPD)

Comme mentionné précédemment, le RGPD est la réglementation européenne qui encadre la protection des données personnelles des citoyens de l'UE. Il établit des droits pour les individus (comme le droit d'accès, de rectification, et d'effacement de leurs données) et des obligations pour les organisations (comme la nécessité d'obtenir un consentement explicite pour le traitement des données).

Guide de la CNIL sur le RGPD

La CNIL propose des guides pour aider les organisations à se conformer au RGPD. Ces guides fournissent des conseils pratiques sur la mise en œuvre des obligations du RGPD, la gestion des données personnelles, et les bonnes pratiques pour assurer la sécurité des informations.

Études de cas sur les violations du RGPD

Les études de cas sur les violations du RGPD illustrent les situations où des entreprises ou organisations ont manqué à leurs obligations en matière de protection des données. Ces cas sont souvent utilisés pour éduquer et sensibiliser les autres entreprises sur l'importance de la conformité et les conséquences potentielles des violations, qui peuvent inclure des amendes significatives.

● À quelle réglementation est soumise la base de données d’un site d'e-commerce ? Et notamment la table d’utilisateurs ?
● Comment devez-vous stocker et sécuriser ces données ?
● Sont-elles publiques ?
● Pouvez-vous les vendre/distribuer à une entreprise partenaire ?
● Les données de la table de connexions sont-elles sensibles ?
● Devez-vous pouvoir les effacer ?

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, y compris la table d'utilisateurs, est soumise au Règlement Général sur la Protection des Données (RGPD). Cette réglementation impose des obligations strictes concernant la collecte, le traitement, la conservation et la protection des données personnelles des utilisateurs.

Comment devez-vous stocker et sécuriser ces données ?

Pour stocker et sécuriser les données, vous devez :

1. **Utiliser des mesures de sécurité techniques** telles que le chiffrement des données, les pare-feu, les antivirus et les mises à jour régulières des logiciels.
2. **Appliquer des mesures organisationnelles** comme des politiques de confidentialité, des contrôles d'accès stricts, et la formation des employés sur la protection des données.
3. **Assurer des sauvegardes régulières** des données pour éviter la perte de données en cas d'incident.
4. **Mettre en place des procédures de gestion des incidents** pour répondre rapidement en cas de violation des données.

Sont-elles publiques ?

Non, les données de la table d'utilisateurs ne sont pas publiques. Elles doivent être protégées et ne peuvent être accessibles qu'aux personnes autorisées dans le cadre de leur travail.

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

Vous ne pouvez vendre ou distribuer les données personnelles des utilisateurs à une entreprise partenaire que si vous avez obtenu un consentement explicite et éclairé des utilisateurs concernés. Sans ce consentement, la vente ou la distribution des données personnelles serait une violation du RGPD.

Les données de la table de connexions sont-elles sensibles ?

Les données de la table de connexions, qui peuvent inclure des informations telles que les adresses IP, les horaires de connexion, et les journaux d'activité, sont considérées comme sensibles. Elles peuvent révéler des informations sur les habitudes et les comportements des utilisateurs, et doivent donc être protégées de manière appropriée.

Devez-vous pouvoir les effacer ?

Oui, vous devez être en mesure d'effacer les données personnelles si les utilisateurs en font la demande, conformément au droit à l'effacement prévu par le RGPD. Vous devez mettre en place des procédures pour traiter les demandes de suppression et assurer que les données sont supprimées de manière sécurisée et complète.