

Recommandations RGPD

Dans le cadre de la mise en conformité RGPD de notre organisation, il est essentiel d'identifier et de remédier aux problématiques liées à la gestion des données personnelles. Les violations identifiées, comme la conservation excessive, l'absence de processus de suppression ou l'utilisation inappropriée des données, exposent l'entreprise à des sanctions et nuisent à la confiance des clients.

Ce document présente six recommandations clés visant à répondre aux enjeux soulevés par la CNIL et à renforcer notre gouvernance des données. Chaque recommandation s'appuie sur les principes fondamentaux du RGPD, notamment la limitation de conservation, la minimisation des données et le droit à l'oubli. Ces actions permettront de lever les sanctions actuelles tout en garantissant une gestion éthique et sécurisée des données personnelles.

1. Conservation excessive des données

- **Phrase** : "Il est persuadé que nous avons collecté et conservé illégalement son relevé d'information avec son Bonus/Malus qu'il nous avait fait parvenir il y a 7 ans lorsqu'il était jeune conducteur."
- **Problème** : La conservation des données personnelles pendant une durée excessive constitue une violation du principe de limitation de la conservation (Article 5 du RGPD). Ce client n'a pas été assuré pendant plusieurs années et

les données auraient dû être supprimées ou anonymisées après un certain délai.

- **Recommandation** : Mettre en place une politique de gestion des durées de conservation des données en fonction des finalités de chaque traitement. Les données des anciens clients ou prospects devraient être supprimées ou archivées de manière sécurisée après une période définie, par exemple trois ans après la fin de la relation commerciale.

2. Absence de processus de suppression des données

- **Phrase** : "Nous n'avons pas de vrai processus ni pour supprimer les données de notre logiciel de CRM que nous ne devrions pas garder aussi longtemps, ni pour gérer ce type de demandes de client, personne ne savait qui devait la traiter !"
- **Problème** : Le manque de processus de suppression constitue une violation du RGPD, car il empêche l'organisation de garantir le droit à l'oubli des personnes (Article 17 du RGPD) et de respecter le principe de minimisation des données (Article 5 du RGPD).
- **Recommandation** : Mettre en place des procédures automatisées dans le CRM pour la suppression régulière des données non utilisées ou obsolètes. Assigner des responsabilités claires pour gérer les demandes de suppression des données clients.

3. Utilisation injustifiée de données anciennes

- **Phrase** : "Malheureusement, nous avons conservé ses anciennes données de prospection commerciale et lui avons appliqué un malus de 25% sur le devis !"
- **Problème** : L'utilisation de données anciennes (et potentiellement incorrectes) pour appliquer un malus constitue une utilisation non conforme et va à l'encontre du principe de finalité du traitement (Article 5 du RGPD). La collecte et l'utilisation de données doivent être spécifiquement liées à une finalité actuelle et légitime.
- **Recommandation** : Éviter l'utilisation de données qui ne sont plus pertinentes. Pour les nouveaux devis, ne prendre en compte que les informations fournies récemment par le client ou les données strictement nécessaires aux finalités en cours.

4. Usage des données pour la performance commerciale sans garantie de conformité

- **Phrase** : "Nous manipulons ces données pour piloter la performance commerciale de nos équipes, ça commence à devenir très compliqué !"
- **Problème** : L'utilisation de données personnelles à des fins de performance commerciale sans vérification de la conformité RGPD peut enfreindre le principe de transparence et de limitation de la finalité. Les clients doivent être informés de la façon dont leurs données sont utilisées, y compris à des fins d'analyses commerciales.
- **Recommandation** : Informer les clients de l'usage de leurs données à des fins de performance commerciale et obtenir leur consentement si nécessaire.

Mettre en place un cadre de gouvernance des données pour limiter les traitements aux seules informations nécessaires à des fins commerciales.

5. Absence de procédure d'accès aux données personnelles pour le client

- **Phrase** : "Un de nos clients a contacté le service dédié il y a plusieurs mois pour avoir accès à ses données personnelles."
- **Problème** : Il semble que l'entreprise n'ait pas de procédure efficace pour répondre aux demandes d'accès aux données personnelles, ce qui est en violation du droit d'accès (Article 15 du RGPD).
- **Recommandation** : Mettre en place une procédure standardisée et documentée pour traiter les demandes d'accès rapidement, en informant les clients de leurs données disponibles et de la manière dont elles sont traitées.

6. Absence de formation ou d'un responsable chez les employés

- **Phrase** : "Personne ne savait qui devait la traiter !"
- **Problème** : Un manque de formation RGPD des employés ou d'un responsable est mis en évidence, ce qui pourrait entraîner des erreurs dans la gestion des données personnelles et des demandes clients.
- **Recommandation** : Former les employés sur les principes de base du RGPD, attribuer ou recruter un DPO (délégué à la protection des données) pour les questions liées aux données.

