Comment tenir un registre des violations de données conforme au RGPD

Guide pratique pour PME

La protection des données personnelles est un enjeu majeur pour toutes les entreprises, y compris les PME. Le **Règlement Général sur la Protection des Données (RGPD)** impose aux organisations de tenir un registre des violations de données. Ce document vous explique comment créer et maintenir ce registre de manière conforme et pratique.

1. Qu'est-ce qu'une violation de données personnelles ?

Une **violation de données personnelles** désigne tout incident de sécurité entraînant, de manière accidentelle ou illicite :

- La destruction, la perte ou l'altération de données,
- La divulgation non autorisée de données à des tiers,
- L'accès non autorisé à des données personnelles.

Exemple :
Un employé envoie par erreur une liste de clients à une adresse email externe non autorisée. C'est une violation de données qui doit être consignée.

2. Pourquoi tenir un registre des violations ?

Le **registre des violations** permet à votre entreprise de :

- Respecter les obligations légales du RGPD (Articles 33 et 34),
- Démontrer votre conformité en cas de contrôle par la CNIL,
- Identifier les risques et améliorer votre sécurité des données,
- Réagir rapidement en cas de violation (notification aux autorités et aux personnes concernées).

3. Que doit contenir le registre ?

Selon le RGPD, le registre doit inclure **toutes les informations nécessaires pour documenter chaque violation** :

1. **Date et heure de la violation**
2. **Description de la violation**
   Exemple : « Envoi accidentel de 150 emails clients à un destinataire externe non autorisé. »
3. **Catégorie et nombre de personnes concernées**
4. **Type de données affectées**
   Exemple : noms, emails, numéros de téléphone
5. **Conséquences probables de la violation**
6. **Mesures prises pour remédier à la violation**
7. **Mesures pour prévenir de futures violations**
8. **Notification aux autorités compétentes (CNIL)**
   Si nécessaire, la date et le contenu de la notification.

9. **Notification aux personnes concernées**
   Si applicable, le détail de la communication.

4. Comment tenir le registre concrètement ?

a) Format du registre

Le registre peut être **papier** ou **numérique**, mais un format numérique est recommandé pour faciliter les mises à jour et les exports.

Exemple de tableau pour PME :

Date	Description de la violation	Catégorie de données	Nombre de personnes concernées	Conséquences probables	Mesures correctives	Notification CNIL	Notification personnes concernées
15/02/2025	Email client envoyé à un destinataire externe	Emails et noms	150	Divulgation limitée, faible impact	Formation employé et vérification emails	Oui, 16/02/2025	Oui, 17/02/2025

b) Les étapes de gestion d'une violation

1. **Identifier la violation** dès qu'elle est détectée.
2. **Contenir l'incident** pour limiter l'impact.
3. **Évaluer les risques** pour les personnes concernées.
4. **Notifier la CNIL** dans les 72 heures si nécessaire.
5. **Informer les personnes concernées** si le risque est élevé.
6. **Consigner toutes les informations** dans le registre.
7. **Mettre en place des mesures correctives** pour éviter que cela ne se reproduise.

5. Bonnes pratiques pour les PME

- Former vos employés à la sécurité des données et aux procédures de notification.
- Nommer un **responsable de la protection des données** (DPO) ou un référent RGPD, même à temps partiel.
- Auditer régulièrement le registre et vos procédures.
- Utiliser des outils numériques simples (Excel, Google Sheet sécurisé, ou logiciels spécialisés).
- Garder un **historique détaillé** : chaque violation doit rester dans le registre, même après correction.

6. Exemples concrets

Exemple 1 : PME BtoC (services en ligne)

Situation : Une PME vend des services en ligne et utilise un CRM. Un salarié supprime par erreur une base de données contenant les informations clients.

Date	Description	Catégorie de données	Nombre de personnes	Conséquences	Mesures correctives	CNIL	Clients
22/03/2025	Suppression accidentelle de la base CRM	Noms, emails, téléphones	300	Perte temporaire d'accès aux contacts	Restauration à partir d'une sauvegarde, formation employé	Non (impact limité)	Non

Exemple 2 : PME BtoB (fournisseur de solutions informatiques)

Situation : Un fichier Excel contenant les contacts et identifiants de plusieurs clients professionnels est partagé accidentellement sur un serveur accessible à d'autres

Date	Description	Catégorie de données	Nombre de personnes	Conséquences	Mesures correctives	CNIL	Clients
10/05/2025	Partage accidentel d'un fichier clients BtoB sur serveur interne	Noms, emails, identifiants de connexion	50 entreprises	Risque de divulgation d'informations professionnelles	Retrait immédiat du fichier, mise à jour des accès, formation employés	Oui, 12/05/2025	Non (risque limité)

Exemple 3 : PME manufacturière / concession automobile

Situation : Une concession automobile enregistre les données personnelles des clients pour les ventes et les services. Un employé laisse un ordinateur portable contenant ces informations dans un véhicule non sécurisé. L'appareil est retrouvé par un tiers

Date	Description	Catégorie de données	Nombre de personnes	Conséquences	Mesures correctives	CNIL	Clients
01/07/2025	Perte d'un ordinateur portable contenant données clients	Noms, adresses, numéros de téléphone, historiques de vente	120	Risque d'accès non autorisé aux informations clients	Chiffrement des appareils, politique stricte de sécurité des postes mobiles, formation employés	Oui, 03/07/2025	Oui, 04/07/2025

Tenir un registre des violations conforme au RGPD n'est pas seulement une obligation légale : c'est aussi un moyen de **protéger vos clients, vos salariés et votre entreprise**. Avec un registre clair, détaillé et mis à jour, votre PME pourra réagir rapidement et efficacement à toute violation de données.

Besoin d'aide pour mettre en place votre registre des violations ou pour être sûr de votre conformité RGPD ? Contactez-moi dès maintenant !