GESTION DES VIOLATIONS RGPD

Identification d'une violation de données personnelles

Lorsqu'une violation de données personnelles est suspectée ou détectée, les étapes suivantes doivent être suivies pour l'identification et l'évaluation initiale de la violation :

- **Notification interne :**
- Toute personne suspectant une violation de données personnelles doit immédiatement en informer son responsable direct et le Délégué à la Protection des Données (DPD) ou responsable RGPD.
- **Vérification initiale :**
- Le DPD doit évaluer la situation en collectant des informations sur la nature de l'incident, les données concernées, le nombre de personnes affectées, et l'impact potentiel sur les droits des personnes concernées.

Évaluation de la gravité de la violation

- **Évaluation rapide de l'impact :**
- Le DPD doit évaluer si la violation présente un risque pour les droits et libertés des personnes concernées (par exemple, risque de discrimination, d'usurpation d'identité, de fraude financière, etc.).
- **Documentation de l'incident :**
- L'incident doit être documenté dans un registre des violations de données personnelles, avec un résumé de la violation, les mesures prises, et les conclusions de l'évaluation.
-

Notification de la violation à la CNIL

Si la violation présente un risque élevé pour les droits et libertés des personnes concernées, la CNIL doit être informée dans un délai de 72 heures suivant la détection de l'incident.

- **Contenu de la notification à la CNIL :**
- La notification doit inclure les informations suivantes :
  - La nature de la violation.
  - Les catégories et le nombre approximatif de personnes concernées.
  - Les catégories et le nombre approximatif de données personnelles concernées.
  - Les conséquences probables de la violation.
  - Les mesures prises ou proposées pour remédier à la violation (par exemple, verrouillage des systèmes, alerte aux personnes concernées, etc.).

- **Modèle de notification à la CNIL :**
- Utiliser le formulaire de notification disponible sur le site de la CNIL ou contacter directement la CNIL via l'interface de gestion en ligne.

Notification des personnes concernées

Si la violation est susceptible d'entraîner un risque élevé pour les droits et libertés des personnes concernées, celles-ci doivent être informées dans les meilleurs délais.

- **Contenu de la notification aux personnes concernées :**
- La notification doit comporter les informations suivantes :
  - Description de la violation de données personnelles.
  - Les conséquences possibles de la violation.
  - Les mesures prises pour remédier à la violation.
  - Les recommandations pour minimiser les effets négatifs (par exemple, changement de mots de passe, suivi de compte bancaire, etc.).

GESTION DES VIOLATIONS RGPD

- **Mode de notification :**
- La notification peut se faire par email, téléphone, courrier postal ou tout autre moyen adapté à la situation.

Mesures correctives et préventives

Après la détection de la violation, il est essentiel de mettre en place des mesures correctives pour limiter les conséquences immédiates et des mesures préventives pour éviter que la violation ne se reproduise.

- **Mesures correctives :**
  - Réalisation d'une enquête interne pour identifier la cause de la violation.
  - Blocage ou suppression des données compromises.
  - Réinitialisation des accès ou des mots de passe.
- **Mesures préventives :**
  - Révision des politiques de sécurité.
  - Sensibilisation et formation des employés sur la gestion des données personnelles.
  - Mise en place de contrôles supplémentaires pour détecter les violations à un stade précoce.

Suivi et évaluation post-incidents

- **Rapport d'incident :**
- Un rapport détaillé de l'incident doit être rédigé après résolution, documentant toutes les étapes prises et les leçons apprises. Ce rapport doit être accessible aux parties prenantes, y compris la direction, le DPD, et la CNIL, le cas échéant.
- **Analyse de l'impact à long terme :**
- Après avoir traité la violation, une réévaluation des risques à long terme doit être effectuée pour identifier d'autres mesures à prendre et ajuster les processus existants si nécessaire.

Conclusion

Cette procédure vise à garantir que toutes les violations de données personnelles sont détectées, traitées et résolues en conformité avec le RGPD, tout en minimisant les risques pour les personnes concernées. Le respect de ces procédures assure une gestion appropriée des violations de données et renforce la confiance des parties prenantes dans la sécurité des données traitées par [Nom de l’organisation].

Signé :
[Nom du responsable]
[Date]