Note : Les bonnes pratiques en cas de vol de données

1. **Qu'est ce qu'une violation des données ?**

   L'article 4 paragraphe 12 du RGPD définit une violation des données personnelles de la manière suivante :

   « une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données. »

   Par conséquent, il s'agit de tout incident de sécurité d'origine malveillante ou non et se produisant de manière intentionnelle ou non, ayant comme conséquence de compromettre l'intégrité, la confidentialité ou la disponibilité de données personnelles.

   Par exemple :

   - Suppression accidentelle de données personnelles ;
   - Perte d'une clef USB non sécurisée contenant une copie de la base clients d'une société ;
   - Introduction malveillante dans une base de données ;
   - Attaque au ransomware provoquant une indisponibilité des données, une fuite de données ou tout autre conséquence néfaste sur les données personnelles stockées.

2. **Quelle réaction avoir dans l'hypothèse d'une fuite de données ?**

   a. Analyser les conséquences de ladite violation des données

   Pour savoir comment réagir à une fuite de données, et ce, quel qu'en soit la cause (cyberattaque, perte d'une source de stockage des données comme un disque dur, clés USB, ou encore du fait d'un sous-traitant) il faut dans un premier temps analyser les risques de ladite fuite de données.

   Pour réaliser l'estimation du risque de la violation des données, il faut prendre en compte les éléments suivants :

   - Le type de violation (affectant l'intégrité, la confidentialité ou la disponibilité des données) ;
   - La nature, la sensibilité et le volume des données personnelles concernées ;
   - La facilité d'identifier les personnes touchées par la violation ;
   - Les conséquences possibles de celles-ci pour les personnes ;
   - Les caractéristiques de ces personnes (enfants, personnes vulnérables, etc.) ;

- Le volume de personnes concernées ;
- Les caractéristiques du responsable du traitement (nature, rôle, activités).

Par exemple, il n'y a pas de risque si :

- La divulgation de données divulguées déjà rendues publiques ;
- La suppression de données sauvegardées et immédiatement restaurées ;
- La perte de données protégées par un algorithme de chiffrement à l'état de l'art ;
- Si la clé de chiffrement n'est pas compromise et si une copie des données reste disponible.

b. Une fois le risque connu, quelles mesures mettre œuvre

- Si la violation des données n'engendre aucun risque il faudra retranscrire ladite violation dans le registre de violation des données.
  Ce registre doit être tenu à jour quel que soit le risque inhérent à la violation des données subit.

  Le registre de la CNIL doit notamment contenir les points suivants :
  - La nature de la violation ;
  - Les catégories et le nombre approximatif des personnes concernées ;
  - Les catégories et le nombre approximatif d'enregistrements concernés ;
  - Les conséquences probables de la violation ;
  - Les mesures prises pour remédier à la violation et, le cas échéant, pour limiter les conséquences négatives de la violation ;
  - Le cas échéant, la justification de l'absence de notification auprès de la CNIL ou d'information aux personnes concernées.

  Pour compléter les informations à ajouter dans le registre de violation des données, vous pouvez utiliser le document d'aide à la préparation d'une notification mis à disposition par l'ANACOFI ou celui de la CNIL[1].

- Si la violation des données engendre un risque, il faudra d'une part remplir le registre des violations et notifier ladite violation des données[2] à la CNIL dans un délai maximal de 72h.
  Le point de départ du délai de 72h débute à partir du moment où le responsable de traitement a la certitude qu'un incident affectant la sécurité des données personnelles a eu lieu.

  La notification à la CNIL doit détenir à minima les éléments suivants :

[1] https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles
[2] https://notifications.cnil.fr/notifications/index

- La nature de la violation ;
- Les catégories et le nombre approximatif des personnes concernées ;
- Les catégories et le nombre approximatif d'enregistrements concernés ;
- Les conséquences probables de la violation ;
- Les coordonnées de la personne à contacter (DPO ou autre) ;
- Les mesures prises pour remédier à la violation et, le cas échéant, pour limiter les conséquences négatives de la violation.

Pour faire la notification à la CNIL, il n'est pas nécessaire d'avoir toutes les informations sur la violation des données. Il est possible de notifier les éléments inhérents à la violation des données au fur et à mesure que ceux-ci sont découvert. Ce qu'il faut, c'est notifier la violation des données avec les éléments disponibles dans les 72H maximum.

- Si la violation engendre un risque élevé, il faudra ajouter à la tenue du registre de violation des données et à la notification à la CNIL, la notification aux personnes concernées par ladite violation des données.
  Cette notification doit contenir à minima et en des termes clairs et précis les éléments suivants :
  - La nature de la violation ;
  - Les conséquences probables de la violation ;
  - Les coordonnées de la personne à contacter (DPO ou autre) ;
  - Les mesures prises pour remédier à la violation et, le cas échéant, pour limiter les conséquences négatives de la violation.

Le tableau suivant résume les différentes situations et obligation à respecter :

Pour les personnes concernées, la violation engendre :	**aucun risque**	**un risque**	**un risque élevé**
Documentation interne, dans le « registre des violations »	**X**	**X**	**X**
Notification à la CNIL, dans un délai maximal de 72h		**X**	**X**
Information des personnes concernées dans les meilleurs délais, hors cas particuliers			**X**

c. <u>Quel est le rôle de mon sous-traitant lors d'une violation des données</u>

- Lors d'une violation des données, le sous-traitant doit la notifier au responsable des traitements dans les meilleurs délais dès qu'il en a connaissance.
  Cela doit être notamment prévu dans le contrat de service entre le sous-traitant et le responsable des traitements (la société).
- L'obligation de notification à la CNIL peut-elle être confiée au sous-traitant ?
  Cette option est possible, néanmoins cela doit être prévus contractuellement et n'enlève en aucun cas la possibilité pour le responsable des traitements de réaliser la notification en fonction du risque estimé par celui-ci. Cela n'exonère pas non plus le responsable des traitements de réaliser la notification à ses clients de la violation des données.