**Suivi de violation des données à caractère personnel**

1. **Contexte**

Le (insérer la date), une violation de données est survenue dans le cadre de (insérer l’organisme/l’entité). L’origine de l’incident provient d’une erreur humaine qui a entraîné la présence sur (insérer le lieu) de données à caractère personnel de (insérer le nombre de personnes). L’incident a été détecté le (insérer la date et l’heure) et des mesures ont été rapidement prises le même jour pour supprimer les données et une procédure est en cours pour en supprimer l’historique définitivement.

1. **Procédure de violation des données**

***La violation de données impose le choix d’une ou plusieurs procédures adéquates :***

****

Les trois procédures peuvent se cumuler selon la gravité :

* ***Documentation interne*** : Sans risque pour la vie privée, la réglementation impose de prendre contact avec son responsable et son DPO et de remplir un registre des violations qui devra comporter **: la nature de la violation, les catégories et le nombre approximatif de personnes concernées, les catégories et le nombre approximatif de fichiers 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 et de l’absence d’information aux personnes concernées** ;
* ***Notification à la CNIL*** : En cas de risque pour la vie privée des personnes concernées, l’article 33 du RGPD impose de notifier à l’autorité de contrôle toute violation de données à caractère personnel, si possible **dans les 72 heures** au plus tard après en avoir pris connaissance. Si la notification à la Cnil a lieu dans un délai plus long, vous devez l’informer des motifs du retard. Cette notification doit comporter : **la nature de la violation, le nom et les coordonnées du DPO, les conséquences probables de la violation de données, les mesures prises pour remédier à la violation, atténuer les éventuelles conséquences négatives, ou pour prévenir la reproduction de la violation à l’avenir**.
* ***Informer les personnes concernées d’une violation de ses données à caractère personnel*** : En cas de risque élevé pour les personnes concernées, l’article 34 du RGPD impose d’informer la personne concernée en cas de violation des données personnelles la concernant. La communication à la personne concernée doit être **claire et simple**, et devra contenir les informations suivantes : **le nom et coordonnées du délégué à la protection des données à caractère personnel, les conséquences probables de la violation, les mesures prises pour remédier à la violation, atténuer les éventuelles conséquences négatives, ou pour prévenir la reproduction de la violation à l’avenir**.

1. **Cas de (insérer l’organisme/l’entité)**
2. **Détermination de la procédure adéquate en amont**
3. *Responsable de traitement*

(Insérer l’organisme/entité et son objectif)

Le responsable de traitement est (insérer le RT).

1. *Type de violation*

La violation de données a porté sur la confidentialité des données à caractère personnel sans en affecter l’intégrité, ni la disponibilité.

1. *Nature, volume et sensibilité des données*

Elle ne concerne que (préciser le nombre de personnes concernées par la violation).

Les données sont notamment : (préciser la nature des données à caractère personnel)

(Préciser si ces données entrent ou non dans la catégorie particulière de données issue de l’article 9 et 10 du RGPD).

1. *Facilité d’identification de la personne touchée par la violation*

Les données permettent (facilement ou difficilement) d’identifier la personne touchée par la violation.

1. *Conséquences sur les personnes*

La violation de données comporte (un risque théorique/comporte un risque/comporte un risque élevé) sur les droits et libertés des personnes. Un accès extérieur (a été/n’a pas été) révélé. Les lignes directrices du CEPD du 14 janvier 2021[[1]](#footnote-1) prévoient que le risque doit être évalué au regard de la nature, du volume et du contexte des données, ainsi qu’au regard de l’exposition et de sa durée, et des probabilités d’un risque effectif pour les personnes. La doctrine constante du régulateur européen s’agissant des notifications prévoit que lorsque la violation est (peu susceptible/est susceptible) de porter atteinte aux droits et libertés fondamentales des personnes concernées, le responsable de traitement (n’est pas tenu/est tenu) de notifier la violation à la CNIL[[2]](#footnote-2).

Dans notre cas, l’existence d’un accès externe et donc d’un risque effectif sur les droits et libertés des personnes est (peu probable/probable/réel).

Il en découle que conformément à la grille d’analyse du CEPD, la violation (n’est pas susceptible/est susceptible) de porter atteinte aux droits et libertés des personnes eu égard au type de données, à leur volume mais également aux accès effectifs aux données et à leurs réutilisations.

1. *Caractéristique des personnes*

Les personnes touchées par la violation sont des personnes vulnérables au sens des lignes directrices du CEPD et de la CNIL sur l’analyse d’impact relative à la protection des données.

1. **Procédure de documentation interne :**

|  |  |
| --- | --- |
| **Obligations** | **Cas de la violation du XX/XX/XXXX** |
| Nature de la violation | Atteinte à la confidentialité |
| Catégories et nombre approximatif de personnes concernées | Nombre de personnes |
| Catégories et nombre de fichiers | Nombre de fichiers |
| Conséquences probables de la violation | La probabilité d’une utilisation des données malveillante et susceptible de porter atteinte aux droits et libertés semble (très peu élevée/élevée/très élevée). |
| Notification CNIL | L’atteinte concerne (insérer le nombre de personnes) dès lors la violation est **(peu susceptible/susceptible)** d’atteindre les droits et libertés fondamentales des personnes et (nécessite/ ne nécessite pas) de notification à l’autorité de régulation, conformément aux lignes directrices du CEPD. |
| Information aux personnes concernées | L’atteinte concerne (insérer le nombre de personnes) de plus (aucune catégorie particulière/une catégorie particulière/des catégories particulières) de données à caractère personnel (ne figure/ figure/ figurent) dans le fichier atteint par la violation de données. |

1. **Mesures à prendre pour remédier à la violation et ou limiter les conséquences négatives de la violation et préconisations** :

Certaines mesures ont déjà été prises : (indiquer les mesures prises dès la violation)

Les mesures suivantes sont en cours : (indiquer les mesures en cours)

|  |
| --- |
| **Préconisations :**  Au regard de la procédure et de la nature de la violation de donnée et de la sensibilité du sujet, nous préconisons :   * De sensibiliser sur la protection des données à caractère personnel, notamment par le biais d’une mention d’information ; * D’interdire la conservation de données à caractère personnel en local sur les postes des agents ; * De documenter la violation dans le registre de violation ; * D’améliorer la rapidité de contact avec le responsable de traitement. |

1. <https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202101_databreachnotificationexamples_v1_en.pdf> [↑](#footnote-ref-1)
2. Lignes directrices 2021 ; Cas n°15, page 28  <https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202101_databreachnotificationexamples_v1_en.pdf> ; Lignes directrices 2018, page 13 <https://ec.europa.eu/newsroom/article29/items/612052/en> [↑](#footnote-ref-2)