PROCÉDURE À SUIVRE EN CAS DE VIOLATION DE DONNÉES

Références juridiques

- *Considérants 85 à 88 du règlement n°2016/679 du 27 avril 2016, dit « règlement général sur la protection des données »*
- *Articles 33 et 34 du règlement n°2016/679 du 27 avril 2016, dit « règlement général sur la protection des données »*

Principe de la violation de données

Le règlement général sur la protection des données (RGPD) impose des mesures très strictes concernant la protection des données à caractère personnel. Cependant, du fait **que le risque zéro n'existe pas**, une violation de donnée reste toujours possible.

L'article 4-12 du RGPD définit la violation de données comme « *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 manière, ou l'accès non autorisé à de telles données* ».

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.

Les articles 33 et 34 du RGPD posent ainsi un cadre juridique clair concernant la procédure à suivre en cas de violation de données.

CENTRE DE GESTION DE LA FONCTION PUBLIQUE TERRITORIALE DU GARD
Service « Protection des données »
183 chemin du Mas Coquillard – 30 900 NIMES
dpd@cdg30.fr
04 66 38 86 86

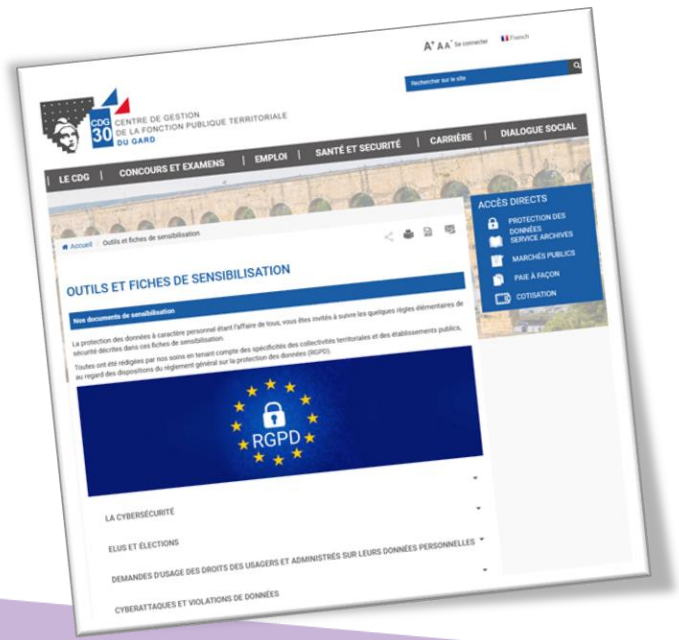
Que faire si vous êtes victime ?

1. ***Alertez immédiatement votre délégué à la protection des données*** pour que celui-ci vous conseille sur la marche à suivre et vous assiste dans la résolution de l'incident

2. ***Documentez l'incident*** afin de préparer la suite des événements et faciliter leur résolution. Cela nécessite notamment de :

   - Déterminer la nature de la violation (perte de données, suppression accidentelle, piratage informatique, envoi de données au mauvais destinataire, etc.)
   - Déterminer la catégorie et le nombre approximatif de personnes concernées par les données atteintes
   - Déterminer la catégorie et le nombre approximatif de données concernées par la violation
   - Décrire les mesures prises pour atténuer les effets de la violation et éviter que celle-ci ne se reproduise

Dans tous les cas, l'incident sera à consigner dans un **registre des violations de données** qui compilera toutes les violations et les actions entreprises pour les résoudre.



Afin de vous aider, nous vous proposons un modèle de registre sur notre site internet

CENTRE DE GESTION DE LA FONCTION PUBLIQUE TERRITORIALE DU GARD
Service « Protection des données »
183 chemin du Mas Coquillard – 30 900 NIMES
dpd@cdg30.fr
04 66 38 86 86

3 *Notifiez la violation de données à la CNIL !*

En cas de risque d'attente à la vie privée des personnes concernées par les données touchées par la violation de données, une notification de l'incident auprès de la CNIL est **obligatoire**, et ce **dans les 72h suivant la constatation de la violation**.

La notification se déroule via une plate-forme sécurisée sur le site internet de la CNIL (www.cnil.fr).

En cas d'impossibilité de réunir toutes les informations nécessaires à la notification dans les 72 heures, notamment en cas de besoin d'investigations supplémentaires, une notification initiale devra être déposée dans les 72 heures, suivie d'une notification complémentaire dès que l'ensemble des éléments seront réunis.

En cas de notification hors délais, les motifs du retard devront être exposés.

4 *Notifiez la violation de données aux personnes concernées !*

En cas de risque élevé d'atteinte à la vie privée des personnes concernées par les données touchées par la violation de donnés, une notification auprès des personnes concernées est **obligatoire en plus de la notification auprès de la CNIL**.

La notification doit à minima contenir et exposer, en des termes clairs et précis, la nature de la violation, les conséquences probables de la violation, les coordonnées du délégué à la protection des données, et les mesures prises pour remédier à la violation et en limiter les conséquences.

La notification doit être complétée, si nécessaire, de recommandations à destination des personnes pour atténuer les effets négatifs potentiels de la violation et leur permettre de prendre les précautions qui s'imposent, tel qu'un changement de mot de passe, la vérification de l'intégrité des données de leur compte utilisateur, etc.

La notification doit être réalisée « dans les meilleurs délais » (article 34 du RGPD).

CENTRE DE GESTION DE LA FONCTION PUBLIQUE TERRITORIALE DU GARD
Service « Protection des données »
183 chemin du Mas Coquillard – 30 900 NIMES
dpd@cdg30.fr
04 66 38 86 86