

Procédure de déclaration d'un incident sur des données à caractère personnel



Procédure de déclaration d’un incident sur des données à caractère personnelRGPD : articles types à intégrer dans la charte informatique

Rédigé Par:

**Sébastien CLAUDE**

Délégué à la protection des données

***Date de publication: 05/09/2018***

|  |  |  |
| --- | --- | --- |
| **Historique** | | |
| Version | Date de modification | Champ des modifications |
| 01 | 05/09/2018 | Création |
|  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Légitimité** | | | |
| **Rédigé par :**  Mr S. CLAUDE,  DPD GHT  Le | **Validé par :**  Le : | **Vérifié par :**  Mr S. CLAUDE,  DPD GHT  Le : | **Approuvé par :**  Le : |

Sommaire

[I . Description du document 4](#_Toc523928864)

[II . Préambule sur la sécurité des DCP 4](#_Toc523928865)

[1 ) La sécurité au sens DICT 5](#_Toc523928866)

[2 ) La notion de risque 5](#_Toc523928867)

[III . Gouvernance du dispositif 6](#_Toc523928868)

[1 ) Les acteurs impactés 7](#_Toc523928869)

[2 ) Les instances de décisions 7](#_Toc523928870)

[a / En interne à l’organisme 7](#_Toc523928871)

[b / Les instances nationales 7](#_Toc523928872)

[IV . Comment déclarer un incident ? 8](#_Toc523928873)

[a / Le processus de notification en interne 8](#_Toc523928874)

[2 ) que doit contenir la déclaration 9](#_Toc523928875)

[V . La gestion des incidents avec les sous-traitants 10](#_Toc523928876)

[a / Option possible 10](#_Toc523928877)

[VI . Les notifications aux individus 11](#_Toc523928878)

# Description du document

1. Le présent document propose un exemple de procédure de déclaration d’un incident relatif à des données à caractère personnel : perte, indisponibilité, intégrité (=corruption), confidentialité vol... Il a été élaboré à partir des documents suivants :

• <https://www.cnil.fr/fr/notifications-dincidents-de-securite-aux-autorites-de-regulation-comment-sorganiser-et-qui-sadresser> ; CNIL

* <https://www.cnil.fr/fr/les-violations-de-donnees-personnelles> ; CNIL

# Préambule sur la sécurité des DCP

Tous les organismes qui traitent des données personnelles doivent mettre en place des mesures pour prévenir les violations de données et réagir de manière appropriée en cas d'incident. Les obligations prévues par le RGPD visent à éviter qu’une violation cause des dommages ou des préjudices aux organismes comme aux personnes concernées.

Une violation de DCP concerne 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.

Exemples :

* suppression accidentelle de données médicales conservées par un établissement de santé et non sauvegardées par ailleurs ;
* perte d’une clef USB non sécurisée contenant une copie de la base clients d’une société ;
* introduction malveillante dans une base de données scolaires et modification des résultats obtenus par les élèves.

Les obligations des responsables du traitement concernant les violations de données personnelles, et notamment leur notification à la CNIL et aux personnes concernées, sont définies aux articles 33 et 34 du RGPD.

## La sécurité au sens DICT

La sécurité des données est définie par la norme ISO 27001 selon 4 critères :

* **La Disponibilité** : le système doit fonctionner sans faille durant les plages d'utilisation prévues et garantir l'accès aux services et ressources installées avec le temps de réponse attendu.
* **L’Intégrité**: les données doivent être celles que l'on attend, et ne doivent pas être altérées de façon fortuite, illicite ou malveillante.
* **La Confidentialité** : seules les personnes autorisées peuvent avoir accès aux informations qui leur sont destinées.
* **La Traçabilité** : garantie que les accès et tentatives d'accès aux éléments considérés sont tracés et que ces traces sont conservées et exploitables.

Il conviendra donc de considéré un incident dès lors qu’un de ces objectifs tel que définis pour le système d’information considéré ne sera pas rempli.

## La notion de risque

C’est en fonction du risque soulevé par les violations de données à caractère personnel que l’on va définir l’obligation de notification auprès de la CNIL et des individus : en effet toutes les violations ne doivent pas nécessairement être notifiées à l’autorité de contrôle ou aux personnes concernées. Ainsi, l’obligation de notifier dépend du risque que la violation de données personnelles fait peser sur **les droits et libertés des individus** dont les données ont été impactées :

* Si la violation n’entraîne **pas de risque** pour les droits et libertés des personnes concernées, le responsable du traitement :
  + doit **documenter**, en interne sous forme d’un registre, la violation qui vient de se produire ;
  + ne doit **pas notifier cette violation** ni à la CNIL, qui peut en revanche contrôler cette documentation interne, ni aux personnes concernées.
* Si la **violation entraîne un risque** pour les droits et libertés des personnes concernées, le responsable du traitement :
  + doit **documenter**, en interne sous forme d’un registre, la violation qui vient de se produire ;
  + doit **notifier** cette violation à la CNIL, au plus tôt et dans un délai maximal de 72h.
* Si la violation entraîne un **risque élevé** pour les droits et libertés des personnes concernées, le responsable du traitement :
  + doit **documenter**, en interne sous forme d’un registre, la violation qui vient de se produire ;
  + doit **notifier** cette violation à la **CNIL**, au plus tôt et dans un délai maximal de 72h ;
  + doit **communiquer** la violation **aux personnes concernées**, au plus tôt.

En synthèse :



# Gouvernance du dispositif

## Les acteurs impactés

Les deux acteurs incontournables en cas d’incident relatif à des données à caractère personnel sont :

* Le responsable du traitement ayant permis la collecte des données considérées.
* le délégué à la protection des données si il a été désigné au sein de l’organisme

En complément il conviendra de prévenir l’ensemble des responsables de traitements utilisant les données ayant fait l’objet de l’incident.

## Les instances de décisions

### En interne à l’organisme

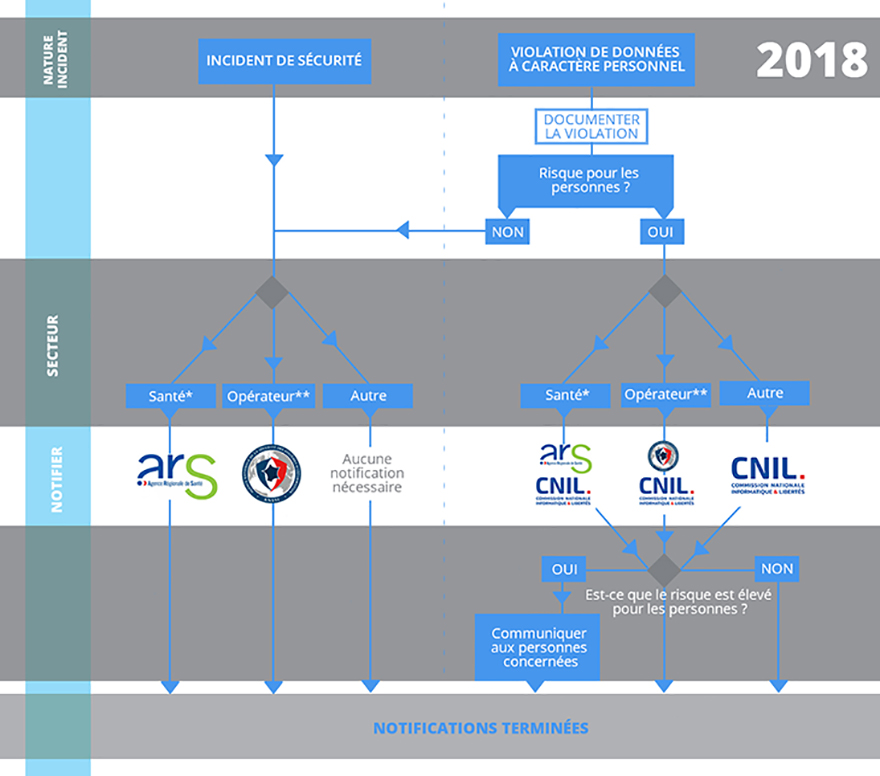
Pour accompagner l’ DPD et le RT il convient de mette en place une c**ellule de crise permanente** en charge de valider les notifications nécessaires pour toutes les violations présentant un risque pour les personnes. Celle cellule pourra faire appel de préférence aux personnes exerçant les fonctions suivantes :

* le directeur ou un représentant de l’encadrement supérieur de l’organisme,
* le responsable de la sécurité des systèmes d'information,
* le délégué à la protection des données à caractère personnel,
* le responsable de la gestion des risques ou de la qualité,
* le responsable de la communication,

### Les instances nationales

Après avoir évalué les informations remontées et déterminé si l’évènement de sécurité est un incident avéré, il est nécessaire de qualifier l’incident , notamment dans le but de déterminer la(les) autorité(s) devant être rendues destinataires de la notification, le cas échéant.

Ci-dessous les principaux organismes susceptibles d’être destinataire de la notification de l’incident :

\* Établissements de santé, hôpitaux des armées, laboratoires de biologie médicale et centres de radiothérapie

\*\* Opérateur d’importance vitale (OIV), opérateur de service essentiel (OSE) ou opérateur de service numérique (OSN) mettant à disposition des places de marché et les moteurs de recherche en ligne et des services d’informatique en nuage, service de confiance (SDC), ou opérateurs Télécom

# Comment déclarer un incident ?

### Le processus de notification en interne

Si vous détecter un incident ou avez un doute quant à l’intégrité de certaines informations à caractère personnel il convient de suivre le processus suivant :

* **Prévenir le DPD** : tout d’abord informer le délégué à la protection des données, il pourra vous aider à qualifier l’incident afin mettre l’organisation en place et adapté au risque évalué. A défaut s’adresser directement au responsable de traitement.
* **Informer** votre **hiérarchie** de la situation.

La suite de la démarche va être prise en charge par le délégué à la protection des données :

* **Prise de contact** avec le responsable de traitement si ce n’est pas fait.
* **Réunion** de la **cellule de crise** et mise en place des mesures techniques nécessaires (avec la DSI) pour que l’incident ne se reproduise pas
* **qualification** de l’incident : évaluation du risque et inscription sur le **registre des incidents.**
* **notification** à l’autorité de contrôle : la CNIL
* si la sécurité des personnes est engagée : la cnil préconisera une notification auprès des individus concernés
* Information des individus
* Définition d’un plan de sécurisation pour réduire les conséquences de l’incident et les actions à enclencher pour maîtriser une nouvelle survenu de celui-ci.

## que doit contenir la déclaration

Le DPD en charge de la déclaration auprès de l’autorité de contrôle devra fournir les éléments suivants :

* la description de la nature de la violation de données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;
* le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;
* la description des conséquences probables de la violation de données à caractère personnel ;
* la description des mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Si, et dans la mesure où il n’est pas possible de fournir toutes ces informations en même temps, les informations peuvent être communiquées de manière échelonnée sans retard indu.

Cette déclaration peut se faire en ligne auprès de la CNIL:

<https://notifications.cnil.fr/notifications/index>

ou bien par l’intermédiaire du formulaire téléchargeable à l’adresse suivante :

<https://www.cnil.fr/sites/default/files/typo/document/CNIL_Formulaire_Notification_de_Violations.pdf>

Ce document est à renvoyer par

# La gestion des incidents avec les sous-traitants

Le sous-traitant notifie au responsable de traitement toute violation de données à caractère personnel dans un délai maximum **de 8 heures ouvrées** après en avoir pris connaissance et par le moyen suivant :

* par **mail** directement auprès du **responsable de traitement**
* par **mail** ou **téléphone** par l’intermédiaire du **délégué à la protection des données**

**Coordonnées du DPD**

* par **téléphone** auprès du **service informatique**

**Coordonnées du service informatique**

Cette notification est accompagnée de toute documentation utile afin de permettre au responsable de traitement, si nécessaire, de notifier cette violation à l’autorité de contrôle compétente.

### Option possible

Après accord du responsable de traitement, le sous-traitant notifie à l’autorité de contrôle compétente (la CNIL), au nom et pour le compte du responsable de traitement, les violations de données à caractère personnel dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d’engendrer un risque pour les droits et libertés des personnes physiques.

La notification contient au moins :

* la description de la nature de la violation de données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;
* le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;
* la description des conséquences probables de la violation de données à caractère personnel ;
* la description des mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Si, et dans la mesure où il n’est pas possible de fournir toutes ces informations en même temps, les informations peuvent être communiquées de manière échelonnée sans retard indu.

Après accord du responsable de traitement, le sous-traitant communique, au nom et pour le compte du responsable de traitement, la violation de données à caractère personnel à la personne concernée dans les meilleurs délais, lorsque cette violation est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique.

# Les notifications aux individus

La communication à la personne concernée décrit, en des termes clairs et simples, la nature de la violation de données à caractère personnel et contient au moins

* la description de la nature de la violation de données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;
* le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;
* la description des conséquences probables de la violation de données à caractère personnel ;
* la description des mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.