Process plainte CNIL

Dans une plainte CNIL, on ne cherche pas la responsabilité du responsable de traitement (RT) dans la violation mais dans l'insuffisante sécurisation du traitement des données à caractère personnel (DCP).

I. L’intérêt à agir :

Le plaignant peut-il déposer une plainte CNIL ?

- Soit la personne a reçu une notification de la violation. Dans ce cas, l’e-mail ou tout autre moyen de notification est joint à la plainte.
- Soit il faut montrer que la personne est dans le fichier qui a subi la violation : réception de mails avec une adresse unique, faisceaux d’indices : Phishing ciblé...

II. Fondement de la plainte :

La plainte doit comporter les manquements à l’origine de la violation des DCP.

Il est important de bien qualifier juridiquement la situation car la CNIL a tendance à écarter facilement les demandes.

⚠ Attention ici la CNIL demande parfois de faire un recours au droit d’accès (art. 15 RGPD) et risque de se fonder uniquement sur l’article en question et non plus sur la violation.

A. DCP insuffisamment sécurisées.

Fondements juridiques : art 5(1)f, 25 et 32 du RGPD

Dans les faits, parfois, la notification de violation contient des indices de manquement, par exemple :

- Si la notification indique "un compte de notre prestataire" => absence d'authentification multi-facteurs et/ou de blocage d'un compte après X tentatives de connexion infructueuses (x <= 10, pour la CNIL).
- Si la fuite porte sur une grande volumétrie annoncée par le pirate auteur de la violation (38 millions de clients qui sortent par un seul compte de prestataire) c'est qu'il n'y a pas de limitation de la volumétrie de ce qui peut être exfiltré.

- Si il y a un délai de 1 mois entre la violation et la notification, il y a un manquement en ce qui concerne l’absence de détection active des intrusions.
- Si la notification indique : "suite à signalement externe", ça peut confirmer l’absence de détection des intrusions

À ce stade il faut chercher des indices.

B. Mentions manquantes à la notification de violation.

« La notification doit contenir une description de la nature de la violation de données, des conséquences probables de la violation de données à caractère personnel, ainsi que 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. Par ailleurs, elle doit communiquer 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 obtenue.

Le considérant 86 du RGPD précise que cette communication doit formuler des recommandations à la personne physique concernée pour atténuer les effets négatifs potentiels puisque que son objectif est de permettre aux personnes concernées de prendre les précautions qui s'imposent. »

Il s’agit d’extraits de la décision SAN-2026-001 de la CNIL, aussi disponible sur Légifrance (points 168 et suivants).

C. Durée de conservation des DCP non justifiée.

Les données personnelles ne peuvent être conservées indéfiniment : une durée de conservation doit être déterminée par le responsable de traitement en fonction de l’objectif ayant conduit à la collecte de ces données. Ce principe de conservation limitée des données personnelles est prévu par le RGPD et la loi Informatique et Libertés.

Plus d’info ici : Les durées de conservation des données

Il peut s’agir de la conservation des DCP au-delà du raisonnable (plus de 2ans) et en base active (= dans l'environnement de travail immédiat, par distinction avec une base d'archive intermédiaire.

Une telle conservation augmente mécaniquement la portée d'une violation, par définition même puisque des DCP qui n'auraient plus dû être là sont dérobées...

Dans la vrai vie : Pour détecter ça, soit se référer à l'annonce du pirate auteur de la violation, soit à la politique de confidentialité (ex. : les fédérations sportives ont la gentillesse d'écrire qu'elles conservent infiniment les DCP…) soit demander au mandant.

D. Manquements annexes.

Obligation de transparence : absence de mention de la durée de conservation des DCP dans la politique de confidentialité et qu'elle n'y figure pas (art 5(1a) + 12 à 14 du RGPD)

III. Justificatifs à fournir :

- Justificatif d’identité : soit c'est un justificatif à usage unique France identité, soit vérifier que le document est filigrané ou caviardé au maximum,
- Mandat : vérifier l’identification du responsable de traitement puis signer (uniquement par un représentant légal de l’association PURR),
- Soit notification de violation, soit la preuve de présence dans le fichier,
- Toute pièce utile, par exemple si l'on cite la politique de confidentialité dans le corps de la plainte, on la met en pièce jointe pour se couvrir d'un éventuel changement ultérieur

IV. En pratique :

Vérifier qu’il s’agit bien d’une violation et pas d’autres problématiques (dans ce cas une action au cas par cas devra être envisagée).

Les différentes étapes :

1. Réception des informations,

Mandat : https://agir.asso-purr.eu.org/

Echanges par messagerie chiffrée (cf. point 5 pour les modalités d’échanges)…

2. Investigations,

Tout peut servir du moment que c’est légal.

3. Rédaction de la plainte,

Voir si d’autres plaintes ont été déposées. Si c’est le cas indiquer le numéro de la première plainte déposée afin de réaliser une série.

La rédaction de la plainte est réalisée en descendant les guides ou recommandations ou lignes directrices de la CNIL ou du Comité européenne à la protection des DCP (CEPD). Il est donc nécessaire soit connaître les références, soit d'aller chercher.

Il est recommandé d'utiliser des termes neutres afin de faciliter la réutilisation des plaintes voir de pouvoir les mettre à disposition en CC BY NC SA bureau@asso-purr.eu.org.

4. Dépôt de la plainte,

L'association a un compte sur le téléservice de la CNIL.

5. Notification du plaignant.

On indique que la plainte a bien été envoyée au plaignant par l'e-mail donné lors de la signature du mandat.

a. Option mail direct :

Mettre : copie : procedures@asso-purr.eu.org Réponse à : procedures@asso-purr.eu.org

Objet : Dépôt de plainte auprès de la CNIL

Proposition de mail :

```
Bonjour,

Dans le cadre de votre mandat en date du XXXXX, la plainte à l'encontre de XXXXXX a été déposée, ce jour, auprès de la CNIL.

Bien cordialement,

XXXXX
Volontaire auprès de la PURR
```

b. Option passage par l'adresse « procédures »

Variante en passant par l'adresse procédures (attention il faut vérifier que votre adresse d'envoi est enregistrée dans la liste : à vérifier auprès de @aeris).

Ecrire un mail en mettant l'adresse procedures@asso-purr.eu.org comme destinataire

Au début du mail mettre :

```
x-list-name: procedures@asso-purr.eu.org
x-resend: <destinataire>
```

puis mettre le corps du mail

6. Suites ?

[En attente de rédaction]

Plus d’infos sur le wiki : https://wiki.asso-purr.eu.org/

Revision #5
Created 2026-03-19 09:57:18 UTC by Mint
Updated 2026-03-19 11:36:16 UTC by aeris