



# Protection des données personnelles : état des lieux en 2023

Vincent Rasneur  
Direction des technologies et de l'innovation  
Service de l'expertise technologique

# La CNIL

---

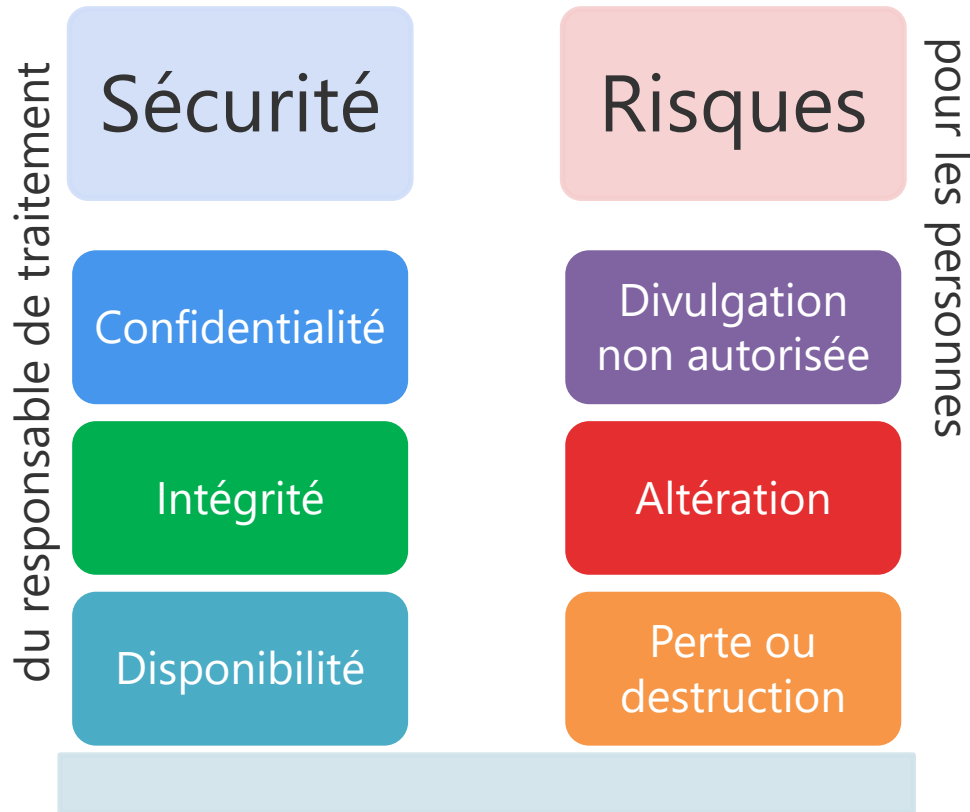
- ◊ **Régulateur des données personnelles depuis 1978**
- ◊ **Autorité administrative indépendante**
- ◊ **Membre du Comité européen de protection des données (CEPD, ex « G29 »)**



Une évolution des atteintes aux données à caractère personnel ?

## **LES VIOLATIONS DE DONNÉES**

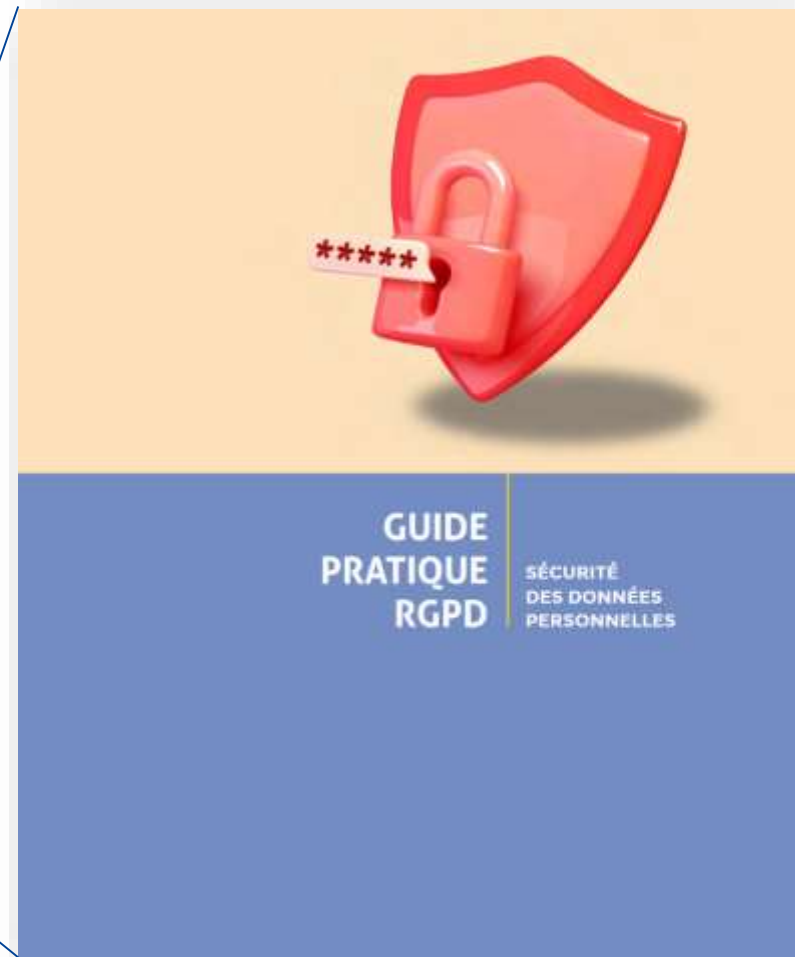
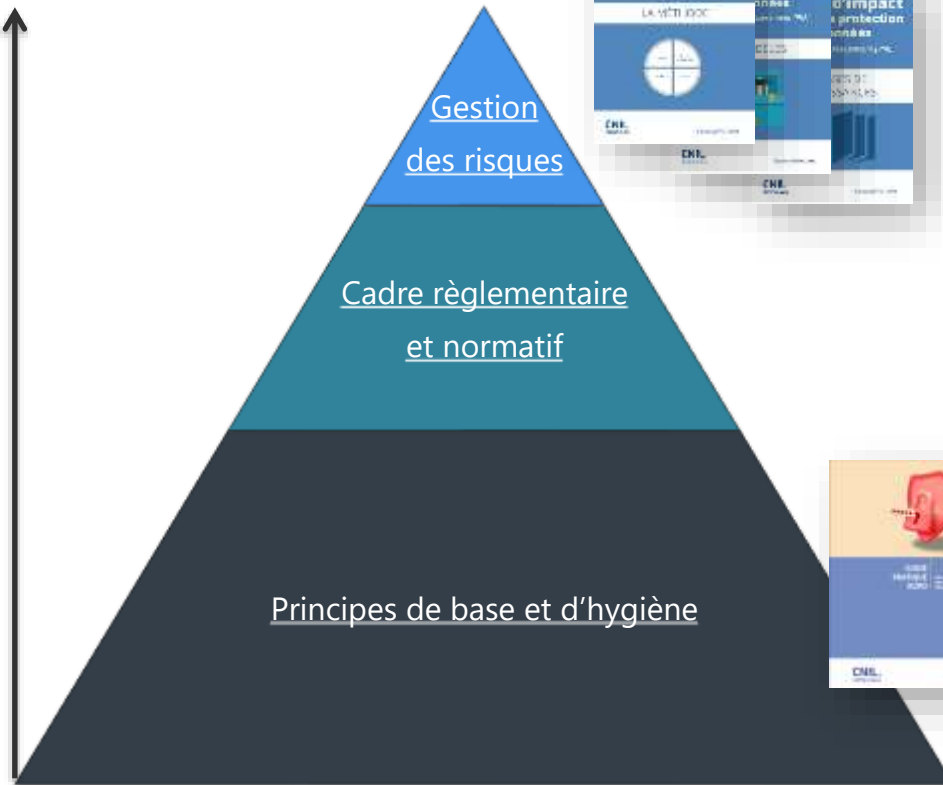
# Obligation de sécurité au sens du RGPD = maîtriser les risques liés aux violations



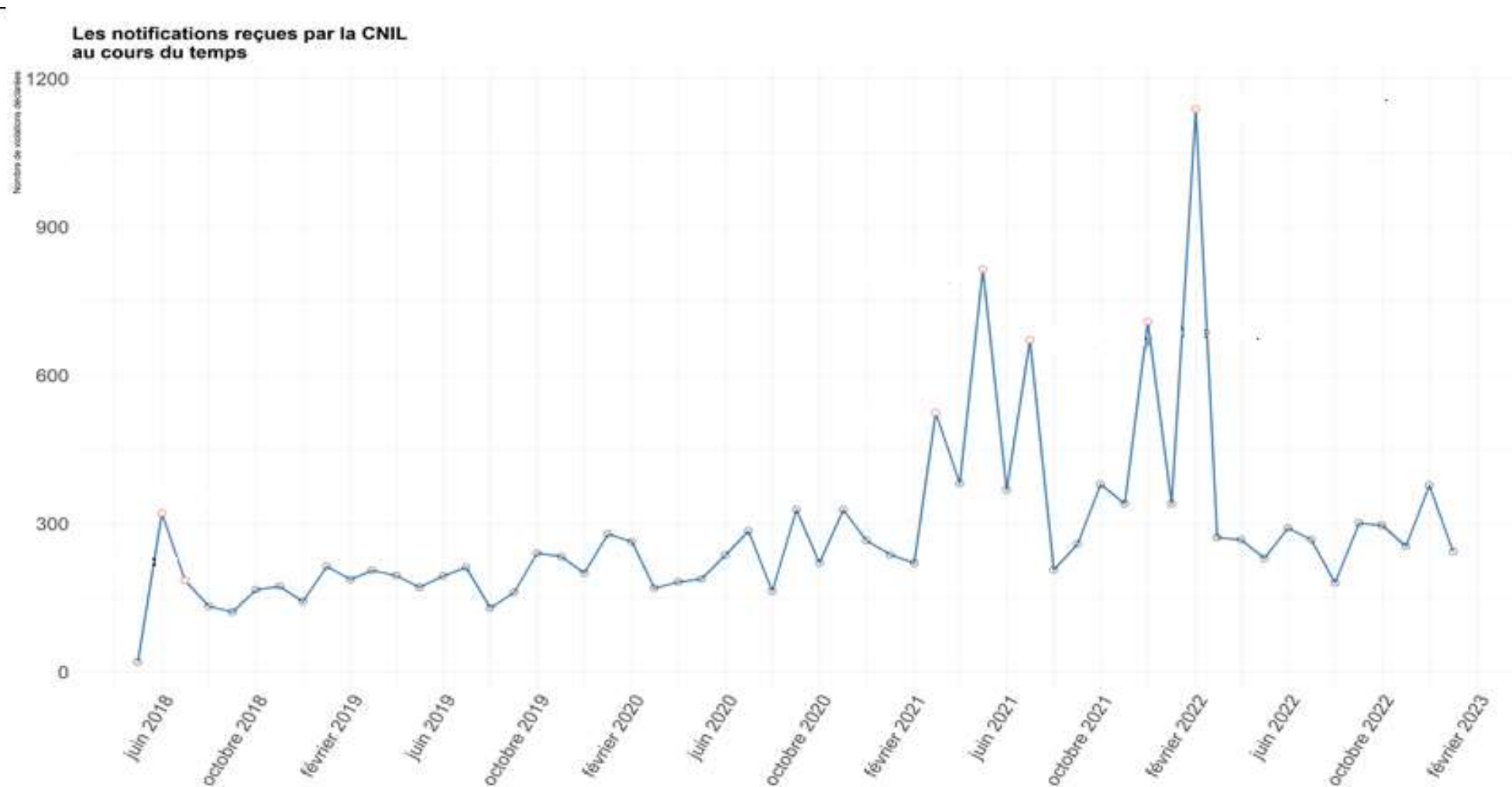
Contrôle de la CNIL faisant suite à une violation de données sensibles

# Mais quel est le bon niveau ?

Niveau de risque  
(sur les personnes)



# 4000 notifications de violations en 2022



# Les violations en France en 2022

---

- **92%** des notifications concernent une **perte de confidentialité**
- **63%** des notifications concernent une **attaque externe**
- **30%** des notifications concernent une attaque par **rançongiciel**
- **Professionnalisation et spécialisation de la sphère criminelle**
  - Crime organisé déterminant avec précision ses cibles
  - Recherche d'accès discrets et pérennes aux réseaux de leurs victimes

# 5 – Piratage des sites web



© belymishka - Fotolia

- « Un client nous contacte par téléphone pour nous indiquer qu'il trouvait bizarre qu'il ait besoin de taper deux fois ses coordonnées de carte bancaire. »

Fiche 1

SENSIBILISER LES  
UTILISATEURS

Fiche 9

SÉCURISER LES  
SITES WEB

## 4 – L'ordinateur disparu



- « Suite à un cambriolage du cabinet, nous nous sommes fait voler trois ordinateurs portables. Ils contenaient les données des procédures engagées pour nos clients. »

Fiche 6

SÉCURISER  
L'INFORMATIQUE MOBILE

Fiche  
13

ENCADRER LA  
MAINTENANCE ET LA FIN  
DE VIE DES MATÉRIELS

## 3 – Mauvais destinataire...



- « Nous avons omis de placer en copie cachée plus d'un millier de patients lors de l'envoi par courrier d'une enquête sur le suivi des maladies vénériennes. »

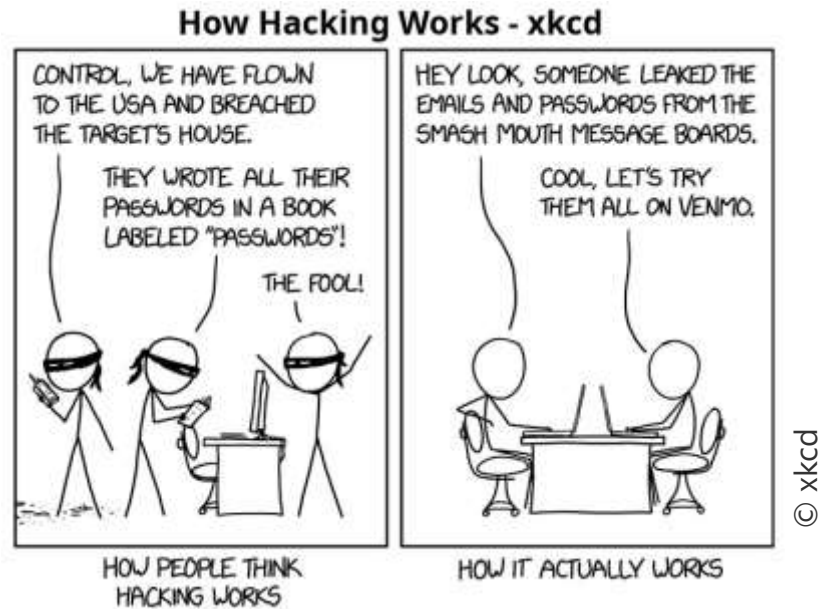
Fiche 3

GÉRER LES  
HABILITATIONS

Fiche  
15

SÉCURISER LES  
ÉCHANGES

## 2 – Bourrage d'identifiants



- « Ces attaques ont été réalisées depuis 3543 IPs distinctes. 98 comptes ont été accédés illégitimement. Les RIB de ces personnes ont été remplacés. »

Fiche 2

AUTHENTIFIER LES  
UTILISATEURS

Fiche 4

TRACER LES  
OPÉRATIONS ET  
GÉRER LES INCIDENTS

# 1 – Rançongiciels



© Chapatte, NY Times

- « Le vecteur d'origine de l'attaque était un compte utilisateur détenu par notre partenaire Jojo. Une fois le compte compromis, les pirates ont accédé en VPN à notre infrastructure. »







Fiche 7

PROTÉGER LE RÉSEAU  
INFORMATIQUE  
INTERNE

Fiche  
10

SAUVEGARDER ET  
PRÉVOIR LA  
CONTINUITÉ  
D'ACTIVITÉ

# Le traitement des violations à la CNIL

Pour les personnes concernées, la violation engendre :	aucun risque	un risque	un risque élevé
Documentation en interne par le RT (registre)			
Notification à la CNIL avant 72h	-		
Information des personnes concernées	-	-	



Quels constats faire pour les actions répressives de la CNIL ?

## **ACTIONS RÉPRESSIVES**

# Avant les sanctions : les signalements



## Thématiques prioritaires de contrôle pour 2023 :

- Caméras « augmentées »
- Applications mobiles
- Fichiers bancaires
- Dossiers patients

# En cas de contrôle



## CHARTRE DES CONTRÔLES

La charte des contrôles a pour objectif de rappeler, aussi précisément que possible, les droits et obligations des organismes faisant l'objet d'un contrôle, au regard notamment de la loi Informatique et Libertés et du RGPD.

Disponible ici :  
[https://www.cnil.fr/sites/default/files/atoms/files/cnil-chartre\\_des\\_controls.pdf](https://www.cnil.fr/sites/default/files/atoms/files/cnil-chartre_des_controls.pdf)

# Sanctions CNIL et sécurité des données

## Les sanctions de la CNIL en 2022



**21 sanctions** pour  
un montant de  
**101 277 900 €**



Un tiers des  
sanctions comporte  
un manquement **à la  
sécurité des données  
personnelles**



**3 décisions** de la CNIL en  
coopération avec d'autres  
**autorités européennes**

**18 dossiers** européens  
**examinés par la CNIL**



**Outre la sécurité, parmi les manquements les plus fréquents figurent :**

- le défaut d'information des personnes
- le non-respect de leurs droits
- le défaut de coopération avec la CNIL

Comment mettre en œuvre le RGPD dans la pratique ?

## **LES OUTILS POUR VOUS AIDER**

# Pour se former

## Formation en ligne « L'atelier RGPD »

La responsabilité de traitement d'une société doit-elle obligatoirement communiquer le registre de sa société à une personne la lui demandant ?

Sélectionnez la bonne réponse puis validez.

Oui

Non

Valider

**MODULE 3 : LES RESPONSABILITES DES ACTEURS**

Module 3 : les responsabilités des acteurs

- Objectif 1 : Nouvelle logique de responsabilité : l'accountability
- Objectif 2 : Partage des responsabilités
- Objectif 3 : Responsabilité spécifique des sous-traitants

**MODULE 4 : LE DPO ET LES OUTILS DE LA CONFORMITE**

Module 4 : le DPO et les outils de la conformité

- Objectif 1 : La régulation à la protection des données

## Guides et fiches thématiques

Mises à jour : comment protéger les données de santé ?

Groupements facultatifs de certifiés et protection des données de santé ?

Qu'est-ce qu'une donnée de santé ?

## Ateliers, webinaires

Agenda

Tous En cours Prochainement Terminés À venir

1 événement à venir

09 MARS 2019

Webinaire : La régulation à la protection des données

# Des guides pratiques selon vos besoins



Guide pour aider les TPE et PME à se mettre en conformité avec le RGPD. Il présente les grandes étapes pour protéger les données personnelles de son entreprise.

[https://www.cnil.fr/sites/default/files/atoms/files/bpi-cnil-rgpd\\_guide-tpe-pme.pdf](https://www.cnil.fr/sites/default/files/atoms/files/bpi-cnil-rgpd_guide-tpe-pme.pdf)

Ainsi que des guides sectoriels (collectivités territoriales, associations, etc.)

Guide de bonnes pratiques (avec exemples) pour les acteurs du développement web ou applicatif dans la mise en conformité de leurs travaux

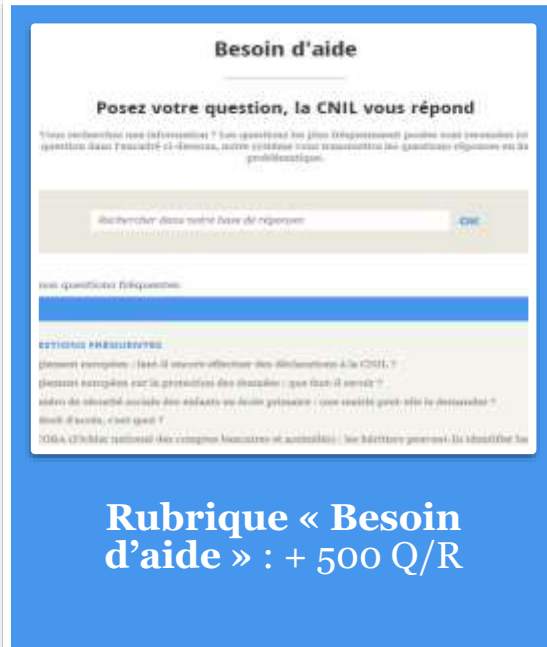
<https://lincnil.github.io/Guide-RGPD-du-developpeur/>



Guide **RGPD CNIL**.  
pour l'équipe de  
développement

# Pour se renseigner davantage

---



**Besoin d'aide**

Posez votre question, la CNIL vous répond

Vous souhaitez une information ? Souhaitez les plus d'informations possible sans poser de question dans l'espace ci-dessous, notre système vous retournera les questions réponses en la problématique.

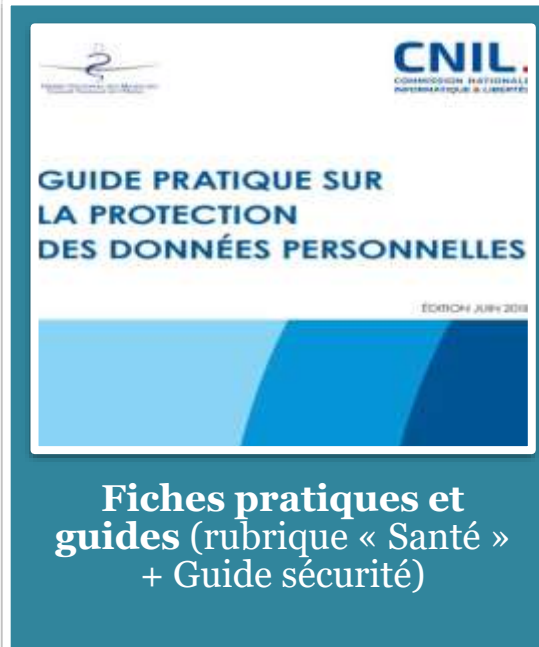
Rechercher dans notre base de réponses  OK

Les questions fréquentes

**QUESTIONS FREQUENTES**

Comment remplir : (est-il encore efficace des démarches à la CNIL ?)  
Comment exercer ses droits (accès des données) : que faut-il savoir ?  
Aides de sécurité sociale des enfants ou des personnes : comment peut-on le demander ?  
Mort d'un être cher ?  
Où aller pour obtenir des copies gratuites et gratuites : les lettres gratuites de la CNIL

**Rubrique « Besoin d'aide » : + 500 Q/R**



**CNIL**  
COMMISSION NATIONALE INFORMATIQUE & LIBERTÉ

**GUIDE PRATIQUE SUR LA PROTECTION DES DONNÉES PERSONNELLES**

ÉDITION JUIN 2011

**Fiches pratiques et guides (rubrique « Santé » + Guide sécurité)**



**Votre réseau sectoriel (homologues, fédérations, etc.)**

# Pour poser une question

Par téléphone au 01 53 73 22 22

---

## Permanence juridique

- Du lundi au vendredi (sauf le mercredi)
- De 10h à 12h et de 14h à 16h

## Permanence santé

- Tous les lundis de 9h30 à 12h

## Permanence DPO

- Du lundi au vendredi (sauf le mercredi)
- De 10h à 12h

Merci de votre attention !