Le Règlement Général sur la Protection des Données (RGPD)

David Rozier
DPO CHUGA

Patrick Guillot
DPO UGA

De quoi parle-t-on ?

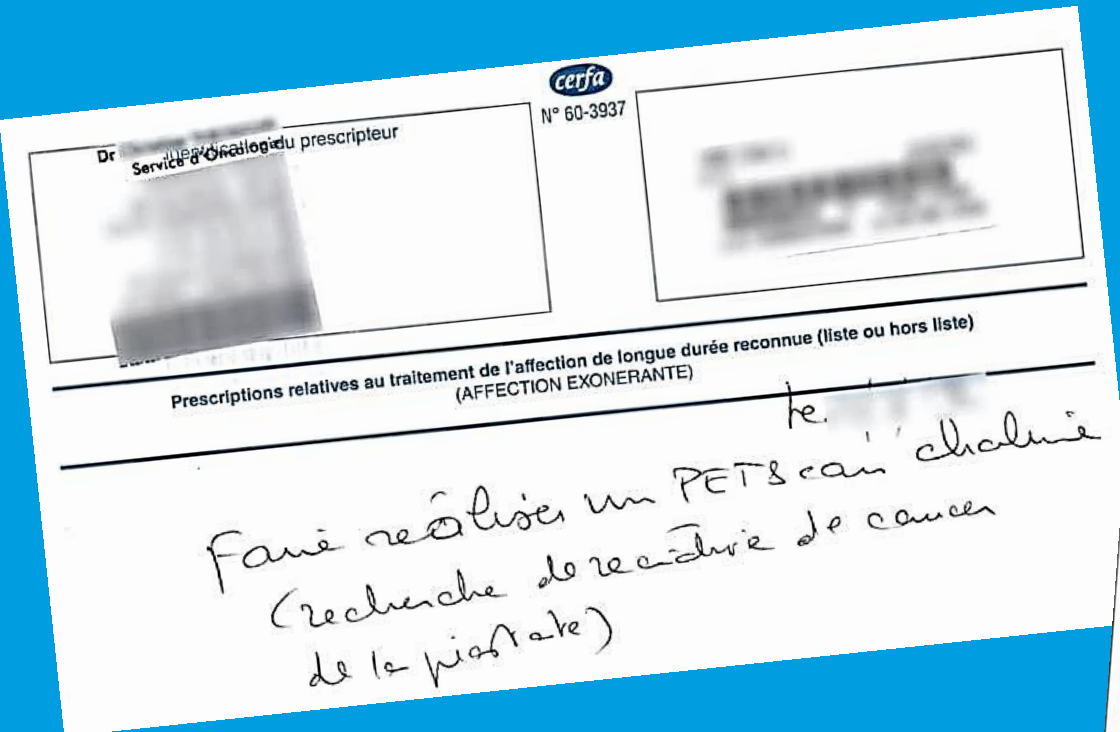
De **données personnelles,** de droits et d'utilisation

De la **protection des données** personnelles
…à **l'université** et dans un **CHU**,
…notamment pour les activités de **recherche**,
…de **lois** nationales et européennes.

« Est-ce vraiment un souci ?

Les données médicales sont déjà protégées par le secret professionnel et les mesures informatiques classiques. »

Obtenu par recherche Google



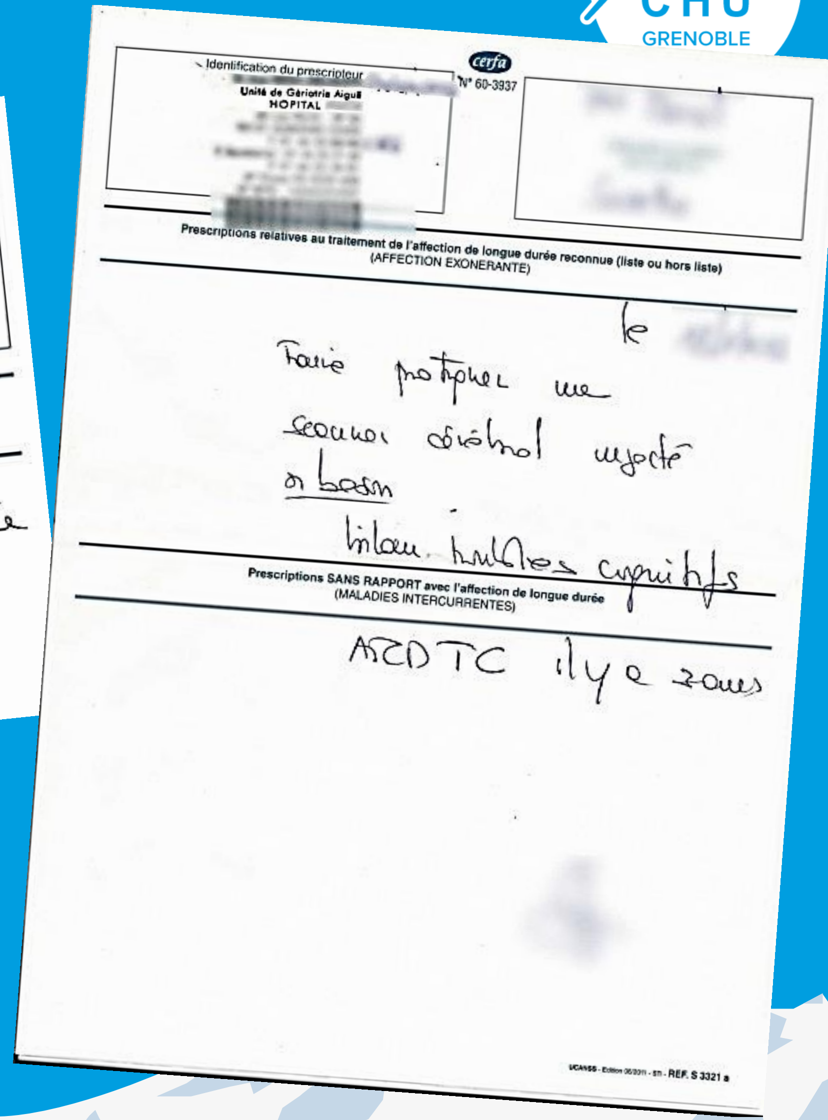
cerfa N° 60-3937

Dr Identification du prescripteur
Service d'Oncologie

Prescriptions relatives au traitement de l'affection de longue durée reconnue (liste ou hors liste)
(AFFECTION EXONERANTE)

le

Faire réaliser un PET Scan choline
(recherche de récidive de cancer
de la prostate)



Identification du prescripteur
Unité de Gériatrie Aiguë
HOPITAL

cerfa N° 60-3937

Prescriptions relatives au traitement de l'affection de longue durée reconnue (liste ou hors liste)
(AFFECTION EXONERANTE)

le

Faire pratiquer une
scanner cérébral injecté
si besoin
bilan troubles cognitifs

Prescriptions SANS RAPPORT avec l'affection de longue durée
(MALADIES INTERCURRENTES)

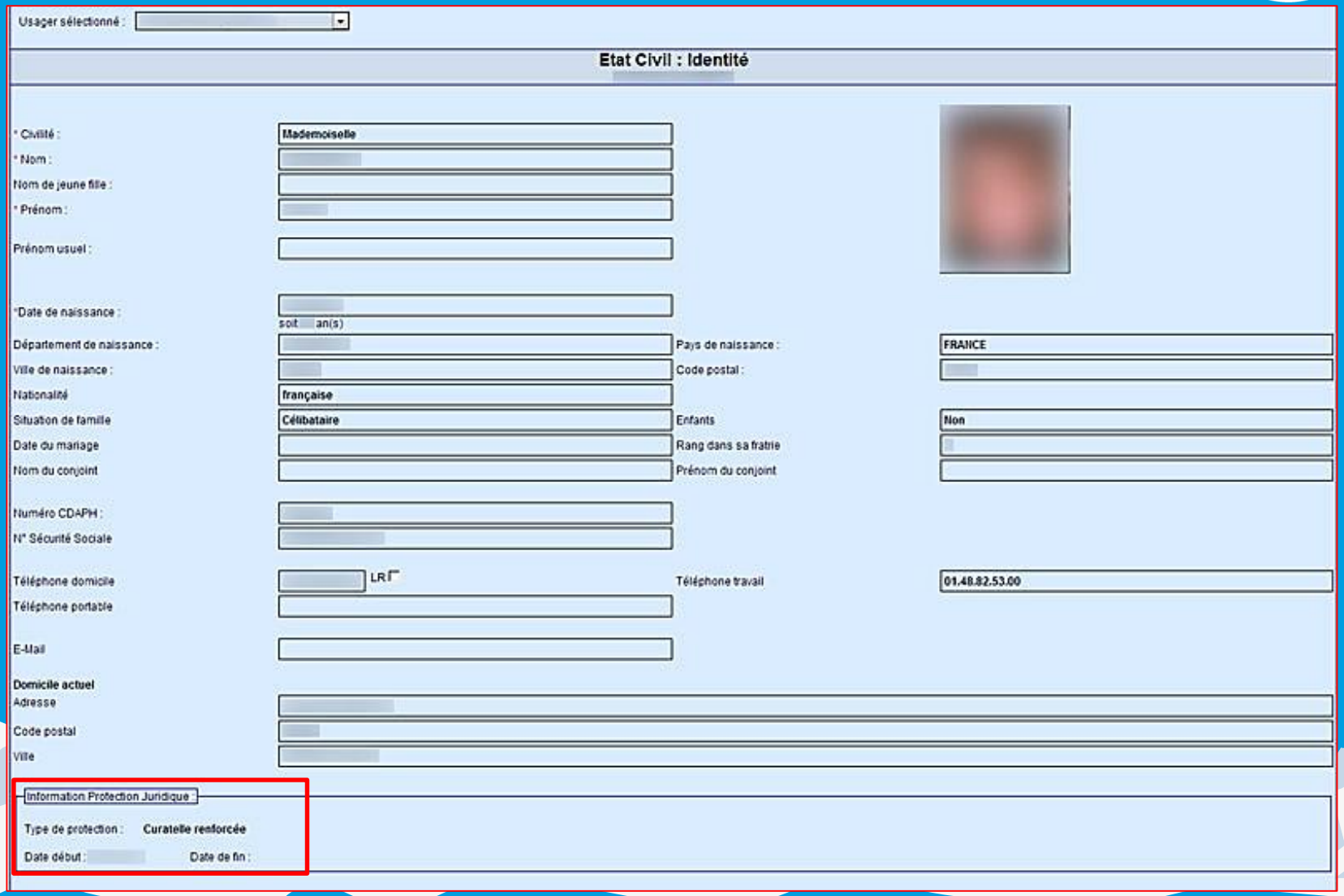
ATCD TC ilya 2 ans

REF. S 3321 a

Obtenu par recherche Google

Patient	Date d'entré	Service	Secteur	Méd. Suiv.	LIT	Provenance	Nom Spécial	Discipline
M. AI	/2012							- HEMATO-CANCEROLOGIE
M. AU	/2012							SOINS SUITE-READAP. POLYV.
Mme	/2012							SOINS SUITE-READAP. POLYV.
Mme	/2012							SOINS SUITE-READAP. POLYV.
M. BE	/2012							SOINS SUITE-READAP. POLYV.
Mme	/2012							SOINS SUITE-READAP. POLYV.
M. BI	/2012							- HEMATO-CANCEROLOGIE
M. BC	/2012							- HEMATO-CANCEROLOGIE
Mme	/2012							- Soins Paliatifs
Mme	/2012							- HEMATO-CANCEROLOGIE
Mme	/2012							SOINS SUITE-READAP. POLYV.
M. BR	/2012							- HEMATO-CANCEROLOGIE
Mme	/2012							SOINS SUITE-READAP. POLYV.
Mme	/2012							SOINS SUITE-READAP. POLYV.

Obtenu par recherche Google



Usager sélectionné :

Etat Civil : Identité

* Civilité :	Mademoiselle		
* Nom :			
Nom de jeune fille :			
* Prénom :			
Prénom usuel :			
*Date de naissance :	soit an(s)		
Département de naissance :		Pays de naissance :	FRANCE
Ville de naissance :		Code postal :	
Nationalité	française		
Situation de famille	Célibataire	Enfants	Non
Date du mariage		Rang dans sa fratrie	
Nom du conjoint		Prénom du conjoint	
Numéro CDAPH :			
N° Sécurité Sociale			
Téléphone domicile	LR	Téléphone travail	01.48.82.53.00
Téléphone portable			
E-Mail			

Domicile actuel

Adresse	
Code postal	
Ville	

Information Protection Juridique :

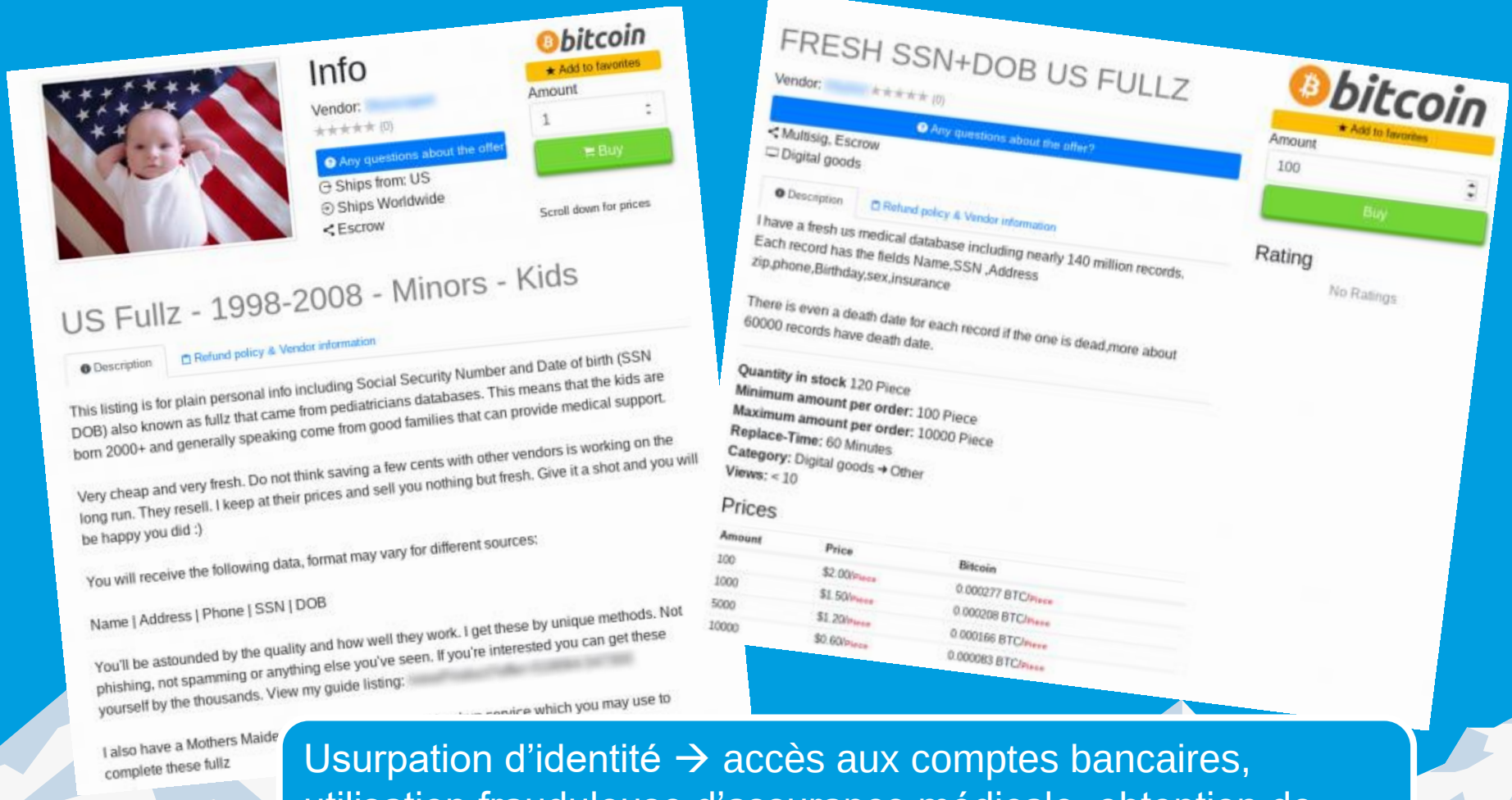
Type de protection : **Curatelle renforcée**

Date début : Date de fin :

« OK, bon,…
mais finalement…,
en quoi est-ce un problème ? »

Réponse 1 : Impacts financiers multiples

Alimentation d'une économie du piratage, détournement argent public, etc.



Usurpation d'identité → accès aux comptes bancaires, utilisation frauduleuse d'assurance médicale, obtention de médicaments ou matériel médical, etc.

Réponse 2 : de réels impacts potentiels sur la vie privée

Stigmatisation sociale (cadre privé ou pro)
Refus d'assurance sur la vie
Refus d'assurance santé
Refus de crédit immobilier
Difficultés à obtenir un emploi
Exclusion des postes à responsabilité
Augmentation de primes d'assurances
Refus de services
…
…

Réponse 3: L'éthique du secret médical

« Admis dans l'intimité des personnes, je tairai les secrets qui me seront confiés »

Le serment d'Hippocrate,
les codes de déontologie (médicale ou infirmier),
le code de la santé publique,

incluent tous le secret professionnel dans les **devoirs généraux**.

Réponse 3: L'éthique du secret médical

« Admis dans l'intimité des personnes, je tairai les secrets qui me seront confiés »

Le serment d'Hippocrate,
les codes de déontologie (médicale ou infirmier),
le code de la santé publique,

incluent tous le secret professionnel dans les **devoirs généraux**.

Ce n'est pas un hasard, ni le résultat d'une mode, le serment d'Hippocrate date du 4ème siècle AvJC (cad bien avant la création de Google).

Réponse 3: L'éthique du secret médical

« Admis dans l'intimité des personnes, je tairai les secrets qui me seront confiés »

Il permet d'assurer
qu'aucun obstacle de type 'jugement moral'
ne vienne enfreindre

- le recours à une assistance médicale
- la bonne qualité de la prise en charge par manque d'ouverture du patient
- la participation à la recherche médicale

L'obligation morale de protection des données de santé est
une condition nécessaire à l'accès aux soins pour tous,
au progrès de la médecine,
elle concourt à l'intérêt général de santé publique.

« Convaincus, j’espère! »

Le Règlement Général sur la Protection des Données (RGPD)

(ou GDPR: General Data Protection Regulation)

Qu’est-ce que le RGPD ?

En France, la Loi Informatique et Libertés encadre l’utilisation de données personnelles, depuis 1978.

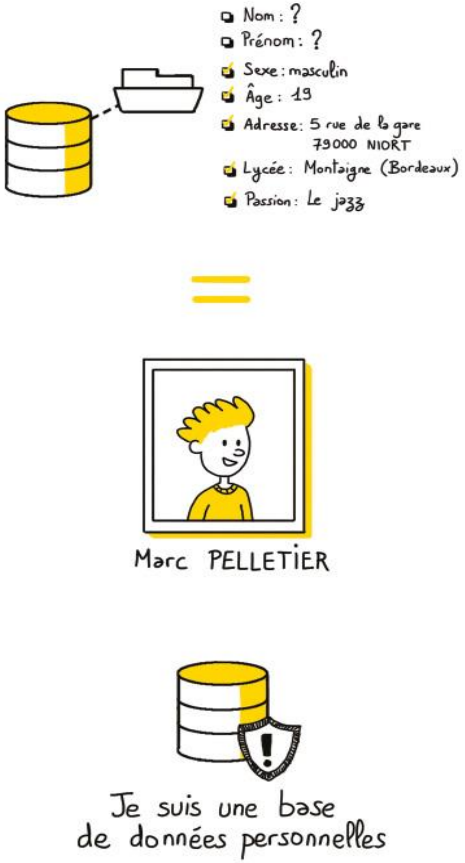
A l’échelle de l’Europe, le Règlement Général sur la Protection des Données (RGPD) impose un nouveau cadre juridique, depuis mai 2018.

Objectif: stopper les abus à l’heure de la multiplication des exploitations de masse de données, en parallèle avec l’explosion des cyberattaques.

Réinstaurer une confiance citoyenne envers la transformation numérique.

Crédits du schéma: Site internet publique de la CNIL

Qu’est-ce qu’une donnée personnelle?



Une notion très large : « toute information se rapportant à une personne physique identifiée ou identifiable ».

Une personne peut être identifiée :

- **directement** (exemple : nom, prénom)
- **ou indirectement**
  - **à partir d’une seule donnée** (exemple : numéro de sécurité sociale, ADN)
  - **à partir du croisement d’un ensemble de données** (exemple : une femme vivant à telle adresse, née tel jour, abonnée à tel magazine et militant dans telle association)

(exemples : un identifiant (n° client), un numéro (de téléphone), une donnée biométrique, plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale, mais aussi la voix ou l’image).

Crédits du contenu : Site internet publique de la CNIL

Un traitement de données personnelles?

Toute utilisation ou manipulation de données personnelles.

Ce traitement peut être :

- Un objectif en soi: l'étude des paramètres biologiques d'un prélèvement sanguin pour effectuer un diagnostic diabétique.
- Une manipulation servant un autre traitement: surveillance vidéo d'un bâtiment (la finalité de l'entreprise n'a rien à voir avec la vidéo, mais cette surveillance est nécessaire dans l'éventualité d'un problème de sécurité potentiel)

Dans un monde où :

- l'automatisation est omniprésente
- et la donnée utilisée comme la base de tout raisonnement

les traitements de données personnelles se comptent par centaines dans un établissement tel qu'un CHU ou une université.

Crédits du contenu : Site internet publique de la CNIL

Les ‘acteurs’ ou ‘rôles’ principaux

Le RGPD définit les rôles suivants parmi les rôles centraux pour la protection des données personnelles :

- **Le responsable de traitement** → donneur d’ordre, responsabilité juridique
  Délégations (‘sachants’ applicatifs ou techniques)

- **Un sous-traitant** → exécutant, responsabilité croisée, contractualisée

- **Les ‘personnes concernées’** → les personnes auxquelles se rapportent les données personnelles traitées

- **Le DPO** → ‘pilotage de la gouvernance des données personnelles’ (CNIL), il/elle analyse, conseil, alerte, tel un ‘représentant’ local de la CNIL.
  Sa nomination est obligatoire pour tout organisme public, pour tout organisme traitant des données personnelles en masse, et tout organisme traitant des données sensibles.

Les principes généraux

Il existent de multiples synthèses de ce long règlement.

Je vous propose un ultra-résumé en 4 principes :

1. Licéité, loyauté, transparence – *l'Esprit du règlement*
2. Restriction de finalité – *Définir chaque traitement*
3. Minimisation de l'exposition et analyse d'impact - *Concevoir*
4. Protection et surveillance - *Exécuter*

Principe 1 - Licéité, transparence, loyauté

L'esprit du nouvel règlement

Responsabilisation envers un engagement
plutôt qu'autorisations multiples

- Licéité : la justification permettant d'envisager un traitement de données

- Transparence : renforcement de l'information des personnes concernées

- Loyauté: Information accessible, renforcement des droits, facilitation d'exercice

Principe 2 - Restriction de finalité

Définir un traitement

Un traitement a une finalité précise et explicite qui restreint l'utilisation des données associées

Cette finalité est importante car vont en découler les caractéristiques du traitement (licéité, durée de conservation acceptable, besoin de consentement/information, destinataires pertinents, données nécessaires).

Par exemple:

'Gestion hygiène soins' : trop vague

- 'Prise en charge patients infections nosocomiales' ok → durée identique données de soins principales, destinataires: équipes soignantes
- 'Suivi professionnels infectés' ok → les destinataires peuvent inclure la RH (congés maladie, remplacements, etc.)

Principe 3
Analyse d'impact & Minimisation de l'exposition – 1/2

Concevoir

L'Analyse d'Impact sur la Protection des Données (AIPD), ou *Privacy Impact Assessment* (PIA) :

- Identifier les faiblesses de protection malgré nos mesures de protection.

- Concevoir un plan d'actions (parfois simplement modifier la conception) pour réduire ces risques à un niveau acceptable

Une analyse conduite par le responsable de traitement avec l'assistance du DPO.

Principe 3
Analyse d'impact & Minimisation de l'exposition – 2/2

Concevoir

Une des conséquences importante de l'AIPD/PIA : réduire l'exposition.

- Proportionnelle au **volume de données** (types de données – colonnes, et nombre d'enregistrements – lignes)
- Proportionnelle au **temps d'utilisation** (durée: chaque traitement possède une finalité donc une durée bornée. Idem pour les données)
- Proportionnelle au **nombres et catégories de destinataires**
- … et finalement proportionnelle au **nombre de traitements** (un traitement dont les résultats ne seraient pas exploités doit être stoppé)

Principe 4 – Protection et Surveillance

Exécuter

Lorsque le traitement de données est validé (loyal, transparent, défini, bien conçu) :

- Mise en place (implémentation) en application des mesures de protection réfléchies dès la conception : par l'architecture, par la technologie.
  - Identifiées lors de l'Analyse d'Impact sur la Protection des Données
  - Mesures surveillance en place, etc.

- Surveillance et transparence : Mise en place d'un suivi, identification des violations de données, et déclaration sous 72h à la CNIL.

L’impact concret pour le domaine de la santé

Un impact Hors-Recherche – Un impact Recherche

Les traitements de données à finalités hors-recherche deviennent exemptes de formalités externes auprès de la CNIL, comme c'est le cas dans la globalité des autres domaines.

Par contre, les traitements de données à finalités de recherche en santé restent soumis à formalités auprès de la CNIL, sauf s'ils sont conformes à une Méthodologie de Référence (MR).

Dans tous les cas, bien sûr, les critères de conformité RGPD sont appliqués (information, droits, sécurisation, limitation de finalité, etc.)

Une AIPD/PIA omniprésente

Dans tous les domaines hors-santé, l'analyse d'impact (AIPD/PIA) est à conduire en cas de risques importants détectés lors d'une première évaluation haut-niveau.

- En santé, la conduite systématique de cette analyse est obligatoire pour tout traitement de données.
- En effet, toute donnée de santé est considérée comme donnée sensible.

Premier exemple d'amende en hospitalier public – Juin 2018

« Le CNPD (Comissão Nacional de Proteção de Dados), l'équivalent de la Cnil, a infligé une sanction financière de 400 000 euros au Centre Hospitalier Barreiro-Montijo, proche de Lisbonne, pour manquement au règlement européen.
Le régulateur a constaté que plusieurs personnels administratifs avaient des accès réservés aux médecins**. En parallèle, il a observé que 985 médecins avaient des habilitations pour accéder au dossier médical des patients, alors que l'établissement ne comprend que 296 médecins. Cet écart s'expliquerait par la présence de vacataires, mais le hic est que les comptes de ces médecins temporaires demeurent tout le temps actifs. Enfin, la délégation du régulateur a créé un compte test et a pu avoir accès à des données patients, montrant une faiblesse dans la gestion des comptes (habilitation, gestion des profils, ...)**

Des arguments faibles et une sanction forte

L'établissement de santé s'est défendu dans un premier temps en soulignant l'incompétence du régulateur au motif que le RGPD n'a pas été adapté en droit national. Un argument qui ne tient pas, car le règlement produit ses effets directement dans le corpus juridique des Etats membres sans transposition. Autre argument, la politique d'habilitation à certaines données est définie par des entités tierces, notamment les services IT du ministère de la santé. **Enfin, le centre hospitalier considère ne pas avoir les outils informatiques adéquats pour gérer les différents scénarios d'accès aux données patients. Une excuse peu valable**, car les solutions actuelles comprennent une gestion fine des habilitations.

Des raisonnements qui n'ont manifestement pas convaincu le CNPD. Ce dernier a reconnu trois infractions au RGPD : violation des principes d'intégrité et de confidentialité des données, violation du principe de limitation d'accès aux données et incapacité pour le responsable du traitement des données à garantir l'intégrité des données. Pour les deux premiers manquements, le régulateur inflige 150 000 euros d'amende et 100 000 euros pour la troisième infraction. Le centre hospitalier peut faire appel de cette décision. »

Source: https://www.cio-online.com/actualites/lire-premiere-amende-rgpd-pour-un-hopital-portugais-10762.html

Références

- www.cnil.fr : le site de la CNIL regorge d'information pour pro ou particuliers,

Ainsi que la loi Informatique et Libertés

Ainsi que les textes originaux et synthétiques des MR

- Sur Eur-Lex, le site des lois européennes, le RGPD original:

https://eur-lex.europa.eu/eli/reg/2016/679/oj

- Sur Legifrance, entre autres, les délibérations de la CNIL :

https://www.legifrance.gouv.fr/initRechExpCnil.do

- Code de la santé publique :
  https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006072665&dateTexte=20180601

UN JOUR AU CHU

2 819

Patients accueillis

3 229

Consultants

290

Passages aux urgences

5 792

Repas servis

19

Tonnes de linge traité

www.chu-grenoble.fr

04 76 76 75 75
CHU Grenoble Alpes, Bd de la Chantourne, 38700 La Tronche