



OBLIGATIONS ET RISQUES RGPD POUR L'EXPERT

JFC CNEJITA du 18/06/2019

« Experts de justice – Comment prévenir les principaux risques informatiques et la mise en responsabilité »

Denis JACOPINI

Denis JACOPINI



EXPERT INFORMATIQUE

Diplômé en :

- Droit de l'Expertise Judiciaire ;
- Cybercriminalité, Sécurité de l'information ;
- Investigation Numérique Pénale.

Certifié par LTSI en :

- Gestion des Risques sur la sécurité des S.I.
- Formé par la CNIL ;
- Loi I&L, RGPD, Santé, Collectivités...

RGPD

Je forme

des référents (ou futurs DPO) ;

J'accompagne

des organismes à se mettre en conformité.

RGPD

Règlement Général sur la Protection des Données

GDPR

Général Data Protection Regulation

C'EST QUOI ?

C'est **un règlement européen** qui encadre le traitement des données personnelles sur le territoire de l'Union européenne.

Ce nouveau règlement européen s'inscrit dans la continuité de la **Loi française Informatique et Libertés** de 1978 et renforce le contrôle par les citoyens de l'utilisation qui peut être faite des données les concernant.

Source : <https://www.cnil.fr/fr/rgpd-de-quoi-parle-t-on>

À QUOI ÇA SERT ?

RGPD : N'aurait-on pas quelques données à protéger ?



RGPD : Quelques de fuites de données



800 000



1 600 000



1 900 000

Anthem

80 000 000



labio
Laboratoire de Biologie Médicale

15 000 dossiers patients

ASHLEY
MADISON®
Life is short. Have an affair.®
34 000 000

MOSSACK FONSECA
11 500 000 docs

F.B.I.
20 000

AdultFriendFinder®
412 000 000

Instagram
6 000 000

EQUIFAX®
143 000 000

Pizza Hut
60 000

UBER
57 000 000

flunch
50 000

facebook®
200 à 600 millions

twitter
32 000 000

Dropbox
68 000 000

LinkedIn
167 000 000

YAHOO!
3 000 000 000

RGPD : Exemples de documents ayant fuité

De  Service d'ophtalmologie prescripteur





































































































































Ordonnance de prescription de Pet Scan

CENTRE DENTAIRE MUTUALISTE	
Mutuelle Dentaire _____ _____ _____	DEVIS PROTHETIQUE Intitulé _____ Praticien _____ Proposition 1 du _____ (devis valable jusqu'au _____)
Assuré : _____ RO N° _____ Org.Affiliation : _____ Code Risque _____ Patient : Sylvie _____ Né(e) le : _____ (N° interne _____) RCI N° _____	Mme _____ Sylvie _____ _____ _____

Designation	Dent(s)	Cotation	Base SS	ED / HN	Montant
Lambeau d'assainissement (PARODONTOLOGIE)		HN 0.00	0.00	250.00	250.00
Lambeau d'assainissement (PARODONTOLOGIE)		HN 0.00	0.00	250.00	250.00
Lambeau d'assainissement (PARODONTOLOGIE)		HN 0.00	0.00	250.00	250.00
Comblement osseux (PARODONTOLOGIE)		HN 0.00	0.00	170.00	170.00
Comblement osseux (PARODONTOLOGIE)		HN 0.00	0.00	170.00	170.00
Totaux			0.00	1090.00	1090.00

Devis de mutuelle

Utilisateur sélectionné :

Etat Civil : Identité

* Civité :
 Nom :
 Nom de jeune fille :
 Prénom :
 Prénom usuel :
 Date de naissance :
 Département de naissance :
 Ville de naissance :
 Nationalité :
 Situation de famille :
 Date du mariage :
 Nom du conjoint :
 Numéros CDAFH :
 1^{er} Secours Sociale :
 Téléphone domicile :
 Téléphone portable :
 E-Mail :
 Domicile actuel :
 Adresse :
 Code postal :
 Ville :



Pays de naissance :
 Code postal :
 Enfants :
 Rang dans sa fratrie :
 Prénoms du conjoint :



Informations juridiques :
 Type de protection :
 Date début : Date de fin :



Fiche d'identification d'une femme sous curatelle renforcée

Patient	Date d'entrée	Service	Secteur	Méd. Suiv.	UT	Provenance	Nom Spécial/Disipline
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 Palliatifs
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.

Liste de patients d'un hôpital

Toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée»); est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale;

« article 4 du règlement (UE) 2016/679 du parlement Européen et du Conseil »

**Information ou groupe d'information
permettant d'identifier quelqu'un**

Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.

« article 34 de la Loi 78-17 Informatique et Libertés du 6 janvier 1978 modifié par la loi n°2004-801 du 6 août 2004 »

Obligation d'intégrité et de confidentialité

Le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en oeuvre les mesures prescrites à l'article 34 de la loi n° 78-17 du 6 janvier 1978 précitée est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.

« article 226-17 du Code pénal → article 34 de la loi Informatique et Libertés »

Pas de sécurité = risque juridique

Les violations des dispositions suivantes font l'objet, conformément au paragraphe 2, d'amendes administratives pouvant s'élever jusqu'à 10 000 000 EUR ou, dans le cas d'une entreprise, jusqu'à 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu ;

« article 83 du règlement (UE) 2016/679 du parlement Européen et du Conseil »

Pas de sécurité = risque juridique

Les données à caractère personnel doivent être traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité) ;

« article 5 du règlement (UE) 2016/679 du parlement Européen et du Conseil »

Attention aux fuites !!!!



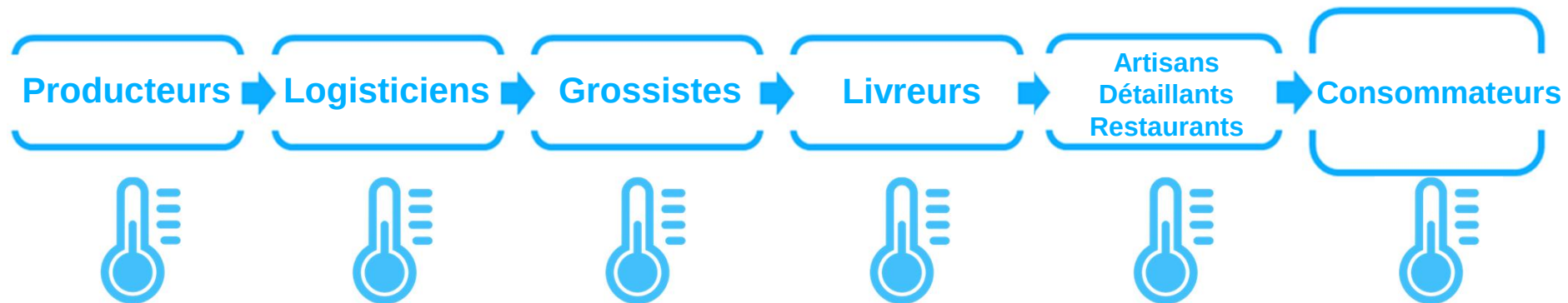
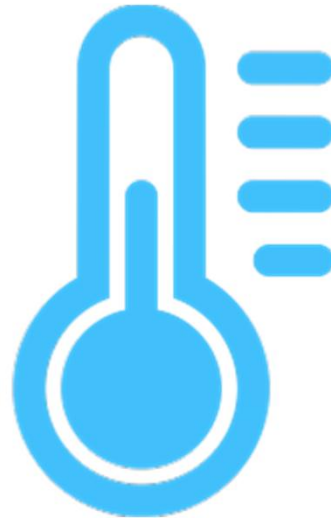
Le RGPD s'applique à toute organisation, publique et privée, qui traite des données personnelles pour son compte ou non, dès lors :

→ qu'elle est établie sur le territoire de l'Union européenne,

→ ou que son activité cible directement des résidents européens.

Source : <https://www.cnil.fr/fr/rgpd-de-quoi-parle-t-on>

Seuls les particuliers ne sont pas concernés





La justice collecte



POUR LA JUSTICE
nous traitons
(nous sommes sous-traitants)



NOUS TRAITONS



NOUS STOCKONS



NOUS COMMUNIQUONS
À DES SOUS-TRAITANTS

OBLIGATION DE CONFIDENTIALITÉ, D'INTÉGRITÉ ET DE DISPONIBILITÉ



La justice ou les conseils collectent

Nous collectons des preuves ou des pièces



**POUR LA JUSTICE
nous traitons**
(nous sommes sous-traitants)



NOUS TRAITONS



NOUS STOCKONS



**NOUS COMMUNIQUONS
À DES SOUS-TRAITANTS**

OBLIGATION DE CONFIDENTIALITÉ, D'INTÉGRITÉ ET DE DISPONIBILITÉ



**POUR LA JUSTICE
OU L'HUISSIER
nous collectons**
(nous sommes sous-traitants)



NOUS TRAITONS



NOUS STOCKONS



**NOUS COMMUNIQUONS
À DES SOUS-TRAITANTS**

OBLIGATION DE CONFIDENTIALITÉ, D'INTÉGRITÉ ET DE DISPONIBILITÉ

Règlement européen sur la protection des données personnelles se préparer en 6 étapes

*En mai 2018, le règlement européen sera applicable.
De nombreuses formalités auprès de la CNIL vont disparaître.
En contrepartie, la responsabilité des organismes sera renforcée.
Ils devront en effet assurer une protection optimale des données
à chaque instant et être en mesure de la démontrer
en documentant leur conformité.*



Désigner
un pilote



Cartographier
vos traitements de
données personnelles



Prioriser
les actions



Gérer
les risques



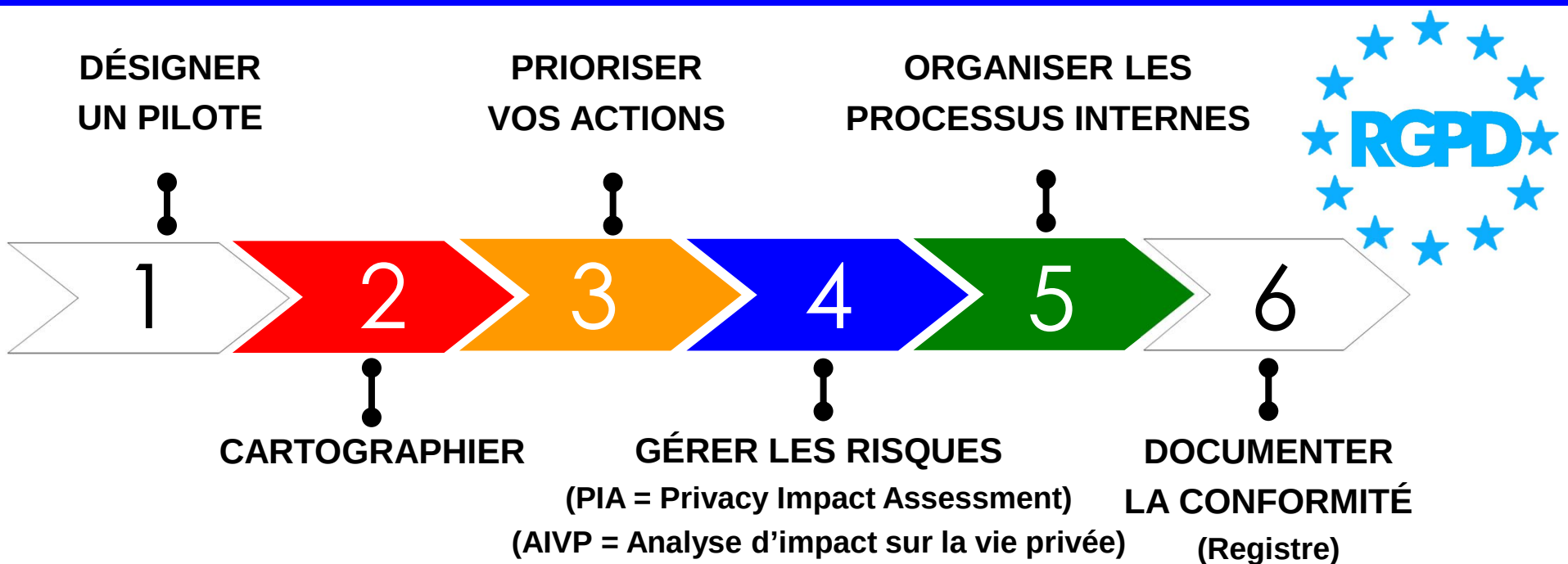
Organiser
les processus internes



Documenter
la conformité

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

RGPD : Dans tous les cas pour commencer, 6 phases à respecter



DÉSIGNER UN PILOTE : Qui sera le référent, le DPO (Data Protection Office)

CARTOGRAPHIER : Audit des traitements / principes essentiels

PRIORISER LES ACTIONS : On ne peut pas tout améliorer d'un coup

GÉRER LES RISQUES : Réaliser une AIVP (Analyse d'Impact sur la Vie Privée)

ORGANISER LES PROCESSUS INTERNES : Modifier/Créer des procédures – Sensibiliser

DOCUMENTER LA CONFORMITÉ : Tenir à jour un document recensant les travaux réalisés

Personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre;

« article 4 du règlement (UE) 2016/679 du parlement Européen et du Conseil »

Responsable de Traitement : Généralement : Le Boss

Personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement ;

« article 4 du règlement (UE) 2016/679 du parlement Européen et du Conseil »

Sous-traitant : Celui qui fait pour quelqu'un

Lorsqu'un traitement doit être effectué pour le compte d'un responsable du traitement, celui-ci fait uniquement appel à des sous-traitants qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du présent règlement et garantisse la protection des droits de la personne concernée ;

« article 28.1 du règlement (UE) 2016/679 du parlement Européen et du Conseil »

On ne peut faire appel qu'à des sous-traitants validés

➔ TRAITEMENT

- ☐ LICITE
- ☐ LOYAL
- ☐ TRANSPARENT

➔ COLLECTE POUR DES FINALITÉS

- ☐ DÉTERMINÉES
- ☐ EXPLICITES
- ☐ LÉGITIMES

➔ MINIMISATION DES DONNÉES

- ☐ ADÉQUATES
- ☐ PERTINENTES
- ☐ LIMITÉES AU STRICT NÉCESSAIRE

➔ CONSERVATION DE DONNÉES

- ☐ EXACTES
- ☐ TENUES À JOUR
- ☐ LE TEMPS DE LA FINALITÉ
- ☐ EN GARANTISSANT LA SÉCURITÉ

☐ RESPECTER CES PRINCIPES ET POUVOIR LE DÉMONTRER

« article 5 du règlement (UE) 2016/679 du parlement Européen et du Conseil »

Le traitement des données à caractère personnel qui révèle l'**origine raciale** ou **ethnique**, les **opinions politiques**, les **convictions religieuses** ou **philosophiques** ou l'**appartenance syndicale**, ainsi que le traitement des **données génétiques**, des **données biométriques** aux fins d'identifier une personne physique de manière unique, des données **concernant la santé** ou des données concernant **la vie sexuelle** ou l'**orientation sexuelle** d'une personne physique sont interdits.

Extrait de « article 9 du règlement (UE) 2016/679 du parlement Européen et du Conseil »

Données sensibles = Ne pas toucher sauf si obligé

Lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel.

« article 35 du règlement (UE) 2016/679 du parlement Européen et du Conseil »

**Analyse d'impact obligatoire si risque élevé
pour le propriétaire des données en cas de fuite ou de perte**

Règlement européen sur la protection des données personnelles

GUIDE DU SOUS-TRAITANT
EDITION SEPTEMBRE 2017

Applicable à partir du 25 mai 2018 à l'ensemble de l'Union européenne, le règlement européen sur la protection des données (RGPD) renforce les droits des résidents européens sur leurs données et responsabilise l'ensemble des acteurs traitant ces données (responsables de traitement et sous-traitants) qu'ils soient ou non établis au sein de l'Union européenne.

Le règlement impose des obligations spécifiques aux sous-traitants dont la responsabilité est susceptible d'être engagée en cas de manquement.

Ce guide a pour objectif de vous accompagner, en tant que sous-traitant, dans la mise en œuvre de ces nouvelles obligations.

Il pourra être enrichi de toutes les bonnes pratiques remontées par les professionnels.

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

DEPUIS QUAND ?



Denis JACOPINI



**MERCI POUR
VOTRE ATTENTION**

