Protection des données du patient: les nouvelles règles

Plan

Présentation synthétique du RGPD

- Champ d’application
- Risques
- Définitions essentielles

Les grands principes de protection des données

Que faire concrètement?

Abréviations et traductions

Français		Anglais	
AIPD	Analyse d'impact relative à la protection des données	**DPIA (PIA)**	Data Privacy Impact Analysis Privacy Impact Assessment
	Autorité de contrôle		Supervisory authority
CCT	Clause contractuelles types	**SCC**	Standard Contractual Clauses
CEP	Comité Européen pour la Protection des Données (ex G29)	**EDPB**	European Data Protection Board (ex W29)
CNIL	Commission informatiques et libertés		
DPD	Délégué à la Protection des Données	**DPO**	Data Protection Officer
RGPD	Règlement Général sur la Protection des Données	**GDPR**	General Data Protection Regulation
	Règles d'entreprise contraignantes	**BCR**	Binding Corporate Rules
RT	Responsable de traitement		Controller
ST	Sous-traitant		Processor
MR	Méthodologie de référence		
DCP	Données à Caractère personnel		Personal Data

Abréviations textes juridiques

Abréviation	Texte
RGPD	Règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)
LIL	Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés *modifiée*
CSP	Code de la santé publique
CP	Code pénal

Préambule

https://www.youtube.com/watch?v=79uD8mX7oeM

https://www.youtube.com/watch?v=F7pYHN9iC9I (UK)

Le sujet des DCP oppose 2 conceptions idéologiques et culturelles:

- libérale, anglo-saxonne
- Protectionniste, d'influence européenne

Enjeu: concilier liberté individuelle et innovation.

Champ d’application – Risques

PRÉSENTATION SYNTHÉTIQUE DU RGPD

Le Règlement Général sur la Protection des Données

Entrée en vigueur et applicabilité:

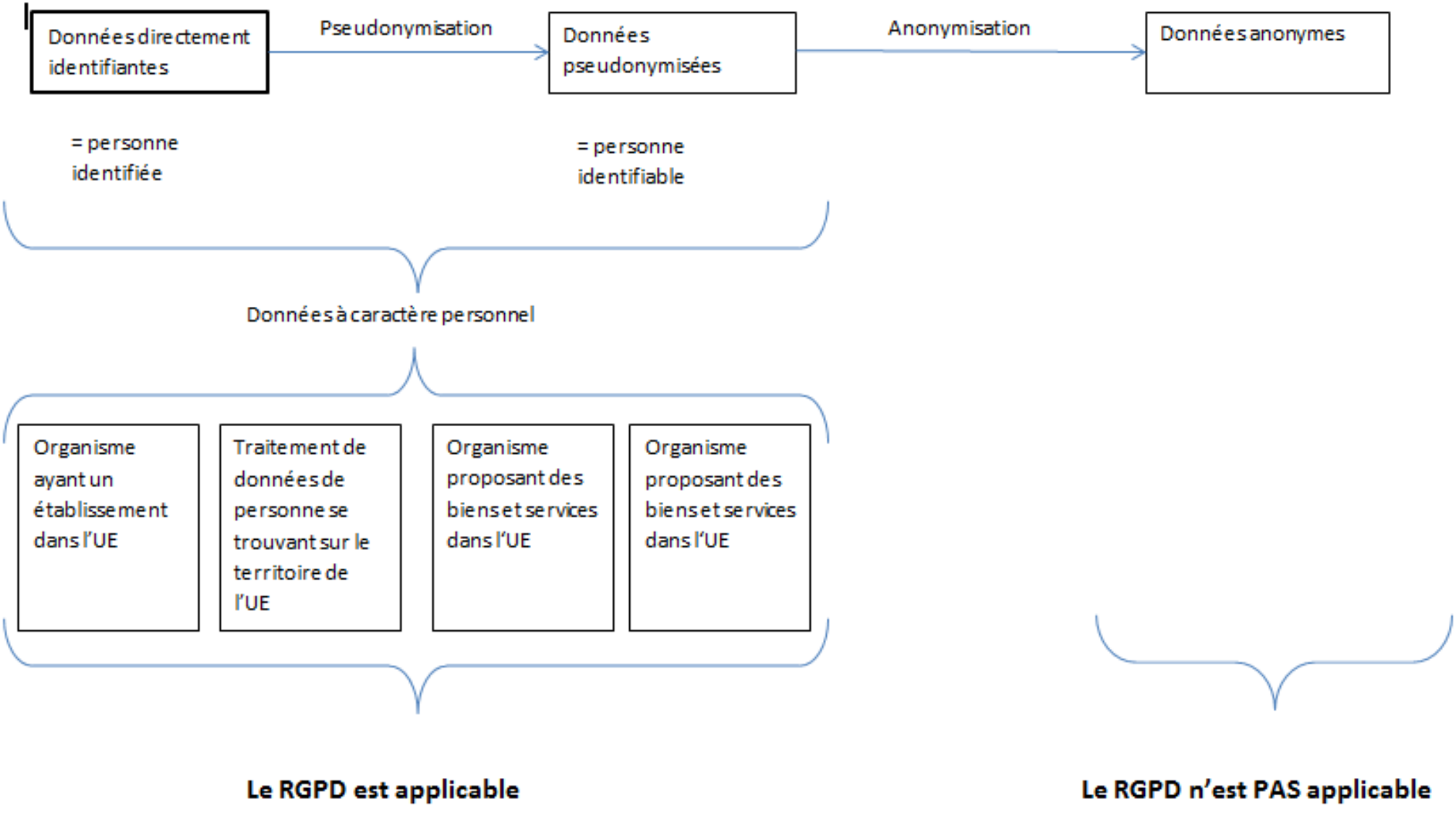
- Règlement UE 2016/679 du 27 avril 2016, relatif à la protection des données physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données:
- Publié au JOUE le 4 mai 2016
- En application le 25 mai 2018.

RGPD bicéphale:

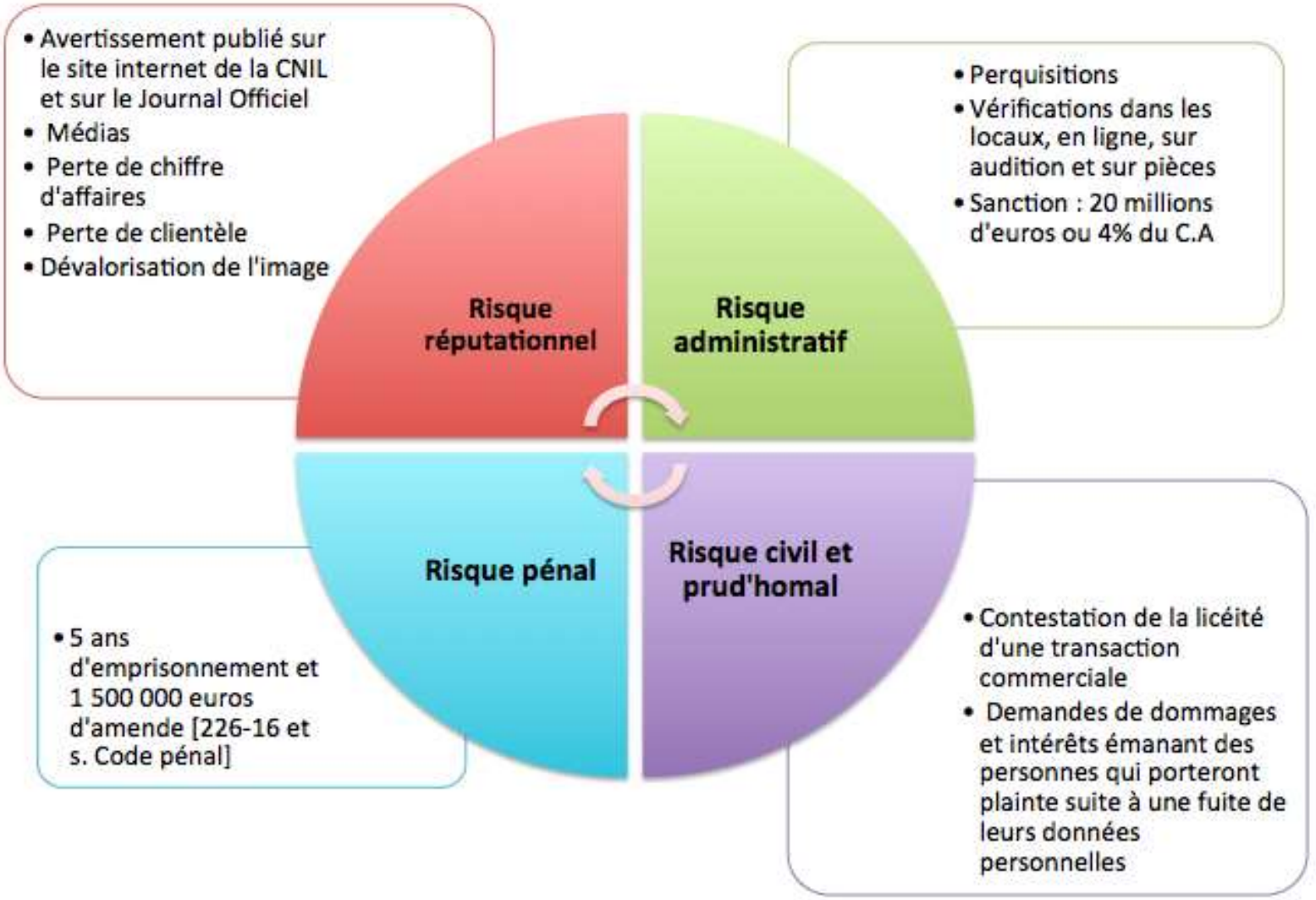
- Protection des données individuelles v/s pratique des marketplace et GAFAM (entre autres…)
- Sécurité: protéger les données c/ cyberattaque

But: aboutir à une politique de gouvernance vertueuse des données personnelles

Le RGPD: application en résumé



Le RGPD: les risques



Secteur public: litige salarié/employeur: Tribunal administratif

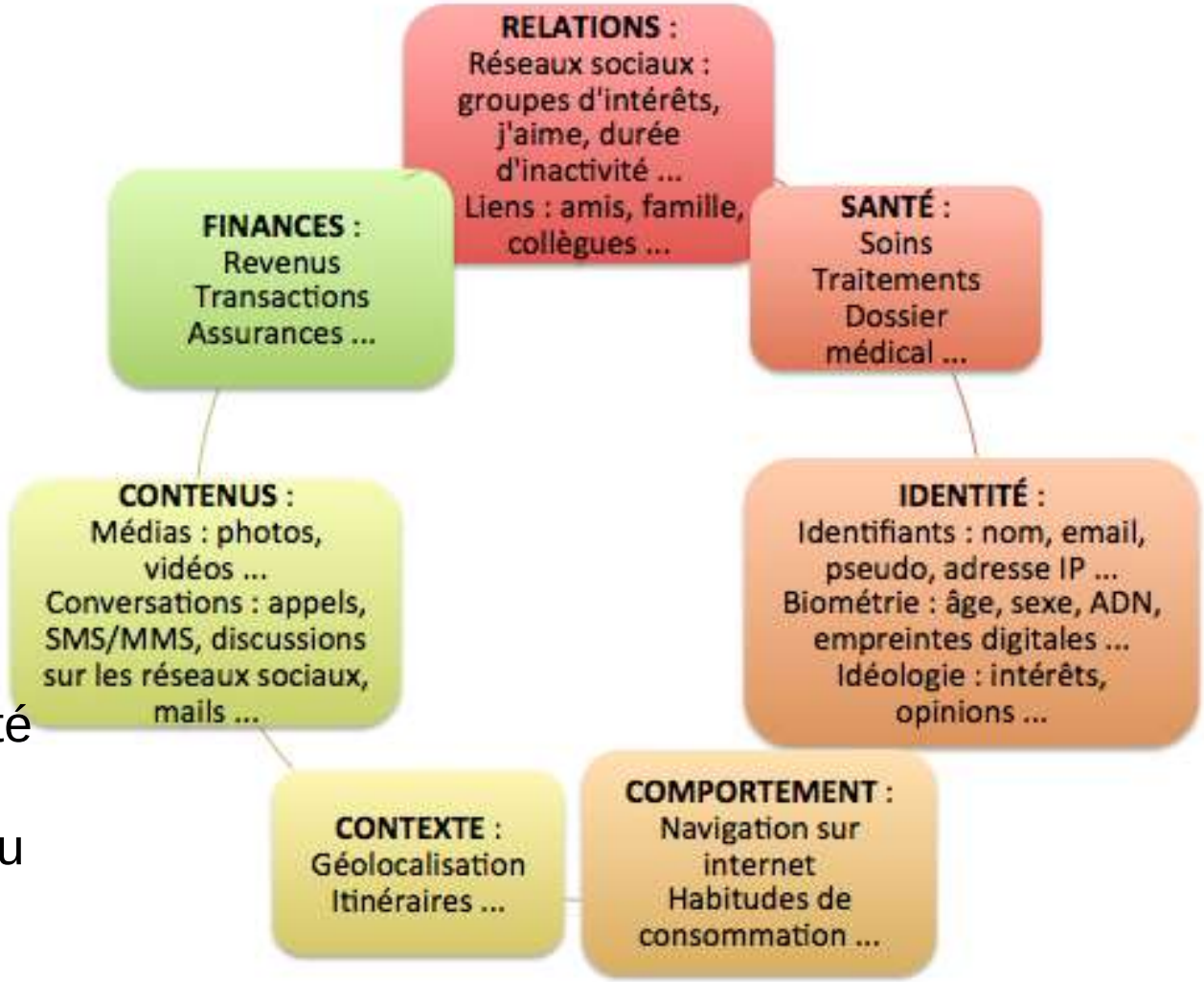
Art 4 RGPD & Art 2 LIL

DÉFINITIONS ESSENTIELLES

RGPD: définitions essentielles

Donnée personnelle (4 critères)

- Toute information
- Relative à une personne physique ;
- Identifiée ou qui peut être identifiée, directement ou indirectement ;
- Par référence à un identifiant (nom, n° d'identification, des données de localisation …) ou à un ou plusieurs éléments qui lui sont propres (identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale). »



RGPD: définitions essentielles

Données sensibles

Données de santé/médicales

Religion ou philosophie

Données génétiques

Appartenance syndicale

DCP relative à la santé:
-Physique ou mentale, passée, présente, future
-Prestation de service de soins de santé (dès l'inscription)
-Relevant des informations sur l'état de santé de cette personne

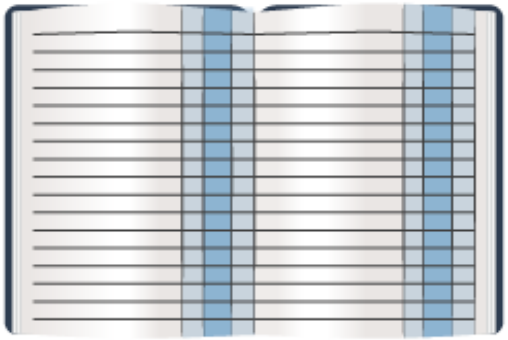
=> Inclut les données génétiques et biométriques

Opinions politiques

Icônes: Desmarais Avocat

RGPD: définitions essentielles

Traitement



Registre des traitements

Constitue un traitement de données :

- Toute opération ou ensemble d'opérations
- Portant sur des données à caractère personnel
- Et ce quel que soit le procédé utilisé : il peut s'agir d'un fichier informatisé ou non.

Exemples fournis par la loi :la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction.

RGPD: définitions essentielles

Responsable de traitement

Le responsable de traitement est la personne, l'autorité publique, le service ou tout autre organisme qui détermine les finalités et les moyens du traitement.

Ex: Directeur/trice générale d'un centre hospitalier

Sous traitant

Traite les données pour le compte, sur instruction et sous l'autorité d'un responsable de traitement.

Ex: gestion paie par prestataire externe, analyse biologique sous traitée…

Doits des patients et nouveautés

GRANDS PRINCIPES DU RGPD

Grands principes 1/2

Droits des personnes concernées

- Droit d'information (sur le traitement des DCP)
- Droit d'accès, rectification, effacement (conditions particulières)
- Droit d'opposition (sauf si obligation légale) pour motifs légitimes
- Droit à la limitation du traitement (gel)
- Droit à la portabilité

Grands principes 2/2

Nouveautés

- Finalité: déterminée, explicite et légitime
- Minimisation des données
- Tenir le registre des traitements
- Base légale (exécution d'un contrat, réglementaire – code du travail - , intérêt légitime, mission d'intérêt public…) SINON: consentement
- Penser cycle de vie de la donnée : archivage et suppression
- Sécuriser les données personnelles

Nouveauté recherche

Cas 1	- recherche **conforme à une méthodologie de référence (MR)**	- **déclaration de conformité à cette norme.** Saisine de l'INDS et du CEREES non requise.
		- **conventionnement** avec les établissements participants
		- **information des personnes concernées**, avant le début du traitement
Cas 2	- recherche **non-conforme à une méthodologie de référence (MR)**	- **Soumission du dossier à l'INDS** qui transmettre le dossier d'abord au **CEREES** puis à la **CNIL**.
		- **conventionnement** avec les établissements participants
		- **information des personnes concernées**, avant le début du traitement

Déclaration de conformité à faire par l'établissement.
Attention ! Déclaratif => prouver les mesures mises en oeuvre en cas de contrôle.

CNIL: renforcement du droit des patients (information++)

Application des principes directeurs du RGPD

QUE FAIRE?

Que faire? La théorie

1. Penser « protection de la vie privée dès la conception » du traitement/service
2. Penser « sécurité par défaut au maximum »
3. S’interroger sur la pertinence des DCP récoltées
4. Sensibiliser vos équipes (mooc CNIL, information individuelle patient, circuit de la donnée, guide CNIL pour le médecin libéral)
5. Exiger autant des prestataires extérieurs

Que faire? La pratique 1/3

- Vérifier les traitements déjà en cours (minimisation, archivage, suppression)
- Pour les nouveaux traitements :

- minimisation des DCP, éviter les champs vides et « commentaires»
- Informer les patients du traitement de leurs DCP et de la possibilités d'exercer leurs droits
- Identifier un service/personne pour les demandes d'exercice des droits

Que faire? La pratique 2/3

- Limiter les copies, duplications, extractions
- Obligation de confidentialité (dossier patient)
- Politique d'archivage dématérialisé + Réflexion sur le choix du support pour la conservation dématérialisée et une lecture durable
- Sécurité: matrice des droits; gestions des habilitations; mesures organisationnelles. Attention aux comptes génériques
- Gestion des traces et journalisation des accès

Que faire? La pratique 3/3

Chefs de projet :

- Nouveau projet: penser à l'anonymisation et la suppression (éventuelle) des données dans le cahier des charges pour choisir un éditeur

- Logiciel déjà en cours d'utilisation: voir ces possibilités avec l'éditeur (au cas par cas en fonction des données personnelles qui transitent par les applicatifs)

- Faire une analyse d'impact sur la protection des données (PIA)

Sources et liens utiles

CNIL

https://www.cnil.fr/sites/default/files/atoms/files/guide-cnom-cnil.pdf

ANSSI

Desmarais avocats: icônes RGPD (Licence creative commons)

Merci!

Des questions?

Coralie ACHARD-TORTUL
Direction des Parcours patient, de la Qualité-gestion des risques et des Relations avec les Usagers - DPQRU
coralie.achard-tortul@chu-limoges.fr
Tél : 05.55.05.61.30
Déléguée à la protection des données