PHARMARKETING

CPDIS
Cercle des Pharmaciens et Dirigeants des Industries de Santé

Protection des données (RGPD) : Applications concrètes dans l'industrie pharmaceutique

15 octobre 2019

Bertrand Le Bourgeois, MSc, Dipl. Ing.
Membre des Bureaux de AMMIS, ACDM et DMB
Membre de AFAR (Groupes de travail Essais Cliniques et Data Privacy)
Membre de AFCDP l'Association Française des DPOs

acdm association for clinical data management

Data Management Biomédical

AFAR AFCDP

Association des Métiers Médicaux des Industries de Santé

Registered Training Organisation N° 11940969494

Sommaire

PharMarketing : ce que nous faisons

- Cabinet de conseil en RGPD, Systèmes d'Information, Audit et Qualité
- Basé en France, avec des collaborateurs dans toute l'UE
- Le fondateur est ancien Directeur Informatique et Auditeur Interne dans l'industrie, et a 18 ans d'expérience chez des prestataires de la Recherche Clinique en Europ, industriels, CROs, Hôpitaux et recherche académique (eCRF, Monitoring, Electonic Health Records, Safety, Data Management, etc.)
- Membre du Bureau Directeur de Data Management Biomédical et de l'Association for Clinical Data Management
- Membre actif de l'Association Française des Affaires Réglementaires (Groupes Rech. Clinique et Data Privacy); membre AFCDP, l'association française des DPOs
- Intervenant dans conferences en Europe et US

DATADOCKÉ

Organisme de formation N° 11940969494

PharMarketing

Services

- Représentation légale essais cliniques et RGPD
- Formations (Organisme N° 11940969494)
- Audit, Gap Analysis
- Analyse d'Impacts pour les processus critiques (PIA)
  - En particulier pour vos prochaines études cliniques ou observationnelles
- Audits Informatiques, Audits sous-traitants
- Revue de contrats, Audits qualité
- Délégués à la Protection des Données externes - Europe
- Formations en sécurité d'entreprise, Compliance, AQ

DATADOCKÉ

PharMarketing

Equipe

Extract of Customers as of 13 August 2019 (blinded)

CRO France Belgium

Small Biotech - France

Small Biotech - US ★

Mid-size CRO France

Scientific Assoc. France

Top 5 Global Pharma / Medical Device - France

Small CRO - France

Software company France

Mid-size Ph. I CRO UK

Big Mid-size Pharma France

Small CRO - France

Safety CRO - UK

Small Biotech - US ★

Phase IV CRO - UK

★ GDPR EU Legal Representative

Extract of Customers as of 13 August 2019 (blinded)

Small Biotech - France	Top 15 Global Medical Device Company - Germany	Biotech - US
Small CRO - France	Small CRO - US ★★	Small CRO - France
Small CRO - France	Small Biotech - UK	Mid-Size Biotech - US
Small Biotech – Canada and US	CRO - France	Small Safety CRO - France

★ GDPR EU Legal Representative ★ Privacy Shield DPO

Sommaire

La Réglementation RGPD

Réglementation Générale sur la Protection des Données (RGPD)

General Data Protection Regulation (GDPR)

C'est simple !

EUGDPR.org

Responsable de traitement et sous-traitant

- **Responsable de traitement (RT) (Controller) :**
  - Organisation déterminant les objectifs et les moyens
- **Sous-traitant (ST) (Processor) :**
  - Organisation collectant ou manipulant des données personnelles pour le compte d'un responsable de traitement
  - Peut-être co-responsable de traitement

Une CRO est responsable de traitement pour (par ex) la gestion de son personnel, et sous-traitant pour la recherche sponsorisée par un industriel.

RGPD : Qui est dans la cible ?

- Toute organisation* manipulant des données personnelles de résidents de l'UE

- Toute organisation établie en UE

(*) RT ou ST, établi en UE ou en dehors

RGPD : Principes

- Réglementation européenne qui s'applique par défaut à tous les pays de l'EU depuis le 25 mai 2018
- Cibles :
  - toute organisation* manipulant des données personnelles de résidents de l'UE
  - Toute organisation établie en UE
- Tous les **sous-traitants** sont maintenant légalement responsables
- **Pénalités** jusqu'à 20M€ ou 4% du chiffre d'affaires annuel en cas de non respect + actions légales en justice
- Responsabilisation des organisations (Suppression de la majeure partie des declarations préalables à la CNIL)

*dans l'UE et hors UE
** le plus grand des deux

Obligations

- **72 heures*** pour prévenir la CNIL en cas de **perte de données** personnelles importante (fuite de données – data breach)
- **Un mois**** pour répondre à la **demande d'un résident européen**
- **Obligation de nommer un délégué à la protection des données** (Data Protection Officer - DPO) **indépendant**
  - Le DPO doit être joignable par les patients, les investigateurs, les employés etc dans la langue locale
  - Le DPO doit avoir 3 compétences : Informatique et gestion de données, metier de la société, réglementaire
- Obligation de tenir un **registre des traitements**, et de faire une **analyse d'impact** de risque pour chaque traitement critique
- Tenue d'un **registre des fuites de données** et d'un **registre des demandes entrantes** de residents de l'EU
- **Formation et information**

(*) y compris WE et jours fériés, (**) extensible dans cas particuliers

Le nouveau cadre de la protection des données de santé

Rappel des principes clés

LICÉITÉ, LOYAUTÉ, TRANSPARENCE

LIMITATION DES FINALITÉS

MINIMISATION DES DONNÉES

EXACTITUDE

LIMITATION DE LA CONSERVATION

INTÉGRITÉ ET CONFIDENTIALITÉ

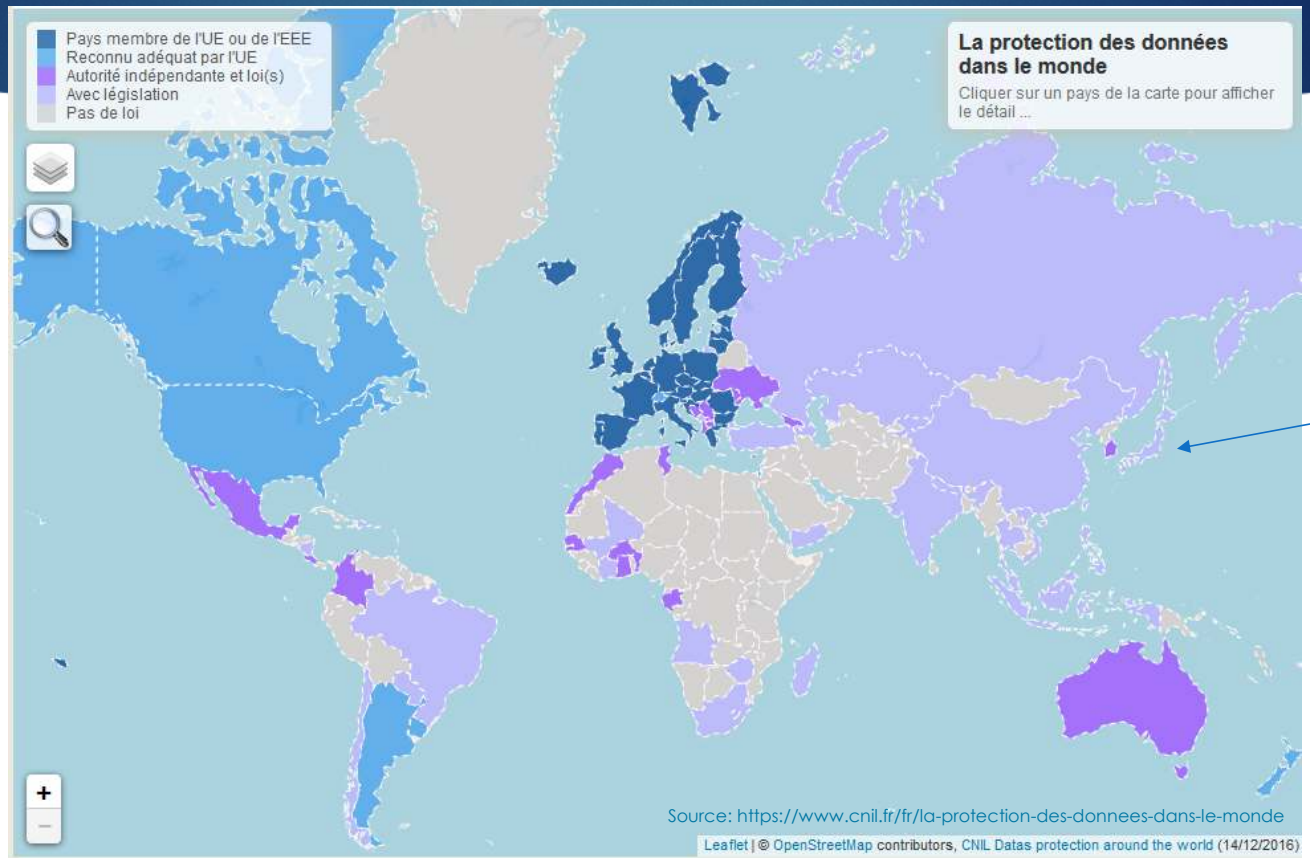
Source: CNIL – Atelier Santé du 11 décembre 2018

Renforcement des droits des personnes

1. Transparence
2. Accès
3. Rectification
4. Opposition
5. Effacement
6. Limitation (nouveau droit)
7. Portabilité des données (nouveau droit)
8. Décision individuelle automatisée

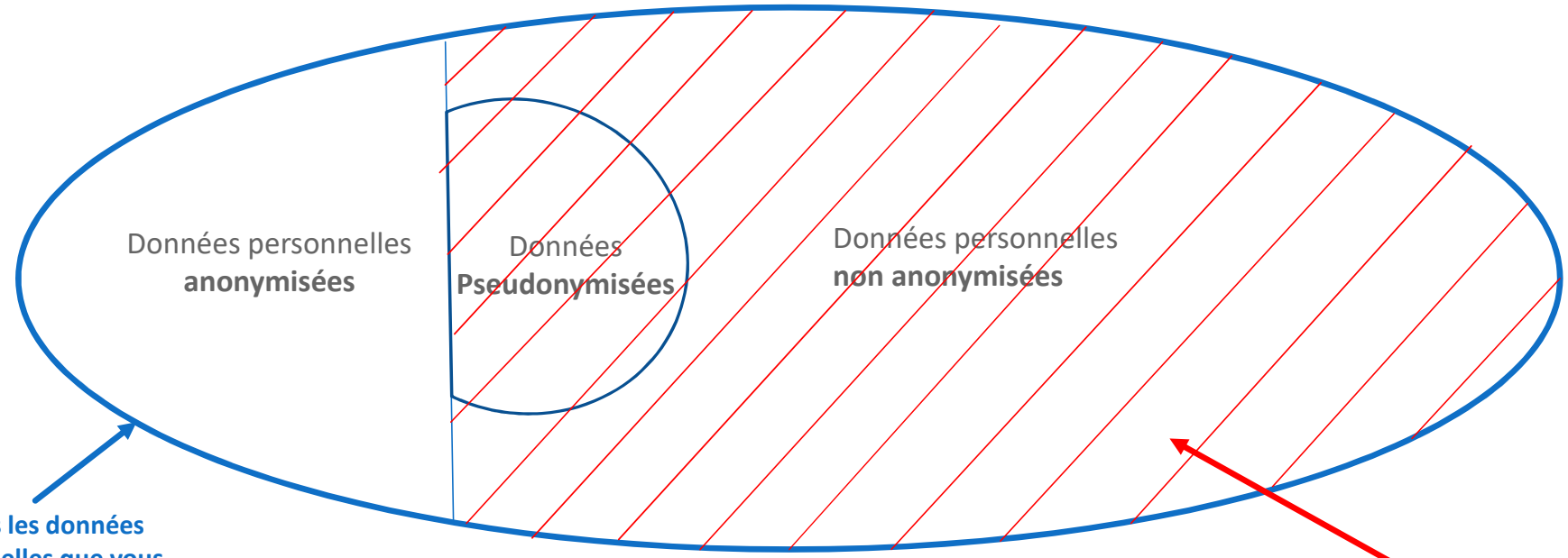
Source: CNIL – Atelier Santé du 11 décembre 2018

Géographie (suite)



Japon adéquat depuis janvier 2019

Données pseudonymisées et données anonymisées



Source: Silicon Marketing SAS

Traitement critique

Lorsque votre traitement a pour objet ou pour effet :

1. l'évaluation d'aspects personnels ou notation d'une personne (exemple : scoring financier) ;
2. une prise de décision automatisée ;
3. la surveillance systématique de personnes (exemple : télésurveillance) ;
4. le traitement de données sensibles (exemple : santé, biométrie, etc.) ;
5. le traitement de données concernant des personnes vulnérables (exemple : mineurs) ;
6. le traitement à grande échelle de données personnelles ;
7. le croisement d'ensembles de données ;
8. des usages innovants ou l'application de nouvelles technologies (exemple : objet connecté) ;
9. l'exclusion du bénéfice d'un droit, d'un service ou contrat (exemple : liste noire).

Si vos traitements de données répondent à au moins 2 de ces 9 critères, vous devez, *a priori*, conduire une analyse d'impact sur la protection des données (PIA : Privacy Impact Assesment), avant de commencer les opérations de traitement.

Source: Guide TPE/PME de la CNIL, mai 2018 page 25
https://www.cnil.fr/sites/default/files/atoms/files/bpi-cnil-guide-rgpd-tpe-pme.pdf

* Aussi appelé Data Protection Impact Analysis (DPIA) ou Analyse d'impact sur la vie privée

Le Délégué à la Protection des Données (DPD)

- En anglais 'Data Protection Officer' (DPO)
- Ancien Correspondant Informatique et Libertés, avec des responsabilités accrues
- Obligatoire si le RT ou le ST a un traitement de données personnelles avec un risque important pour la vie privée des personnes
  - Ou si le type de traitement est mentionné nommément par le GDPR, l'EDPB, ou la 'liste noire' d'une DPA locale, ou dans les cas prévus à l'article 37 RGPD
- Independant
- Aide à la realisation des livrables obligatoires, et pointe la boîte mail DPO régulièrement
- Tient à jour les livrables
- Vérifie la conformité de l'organisation
- Point de contact pour les DPA, les citoyens, les ST et les RT
- Le DPD peut-être partagé par plusieurs organisations
- Il doit être joignable facilement
- Les communications doivent se faire **dans la langue des DPAs et des citoyens**
- Les moyens de contacter le DPD doivent être publiés par le RT ou le ST

Guidelines for DPO – WP 29 - WP 243 rev.01 https://www.cnil.fr/sites/default/files/atoms/files/guidelines_on_dpos_5_april_2017.pdf

Livrables

Obligatoires :

- Registre des traitements de données personnelles
- Fiches d'information ou de consentement révisées
- Procédure de gestion des demandes entrantes de citoyens + Log
- Procédure de gestion des fuites de données + Log
- Formation du personnel
- Revue des mentions légales
- Revue des procédures IT

Si le risque (pour la vie privée des citoyens) paraît important, ou si le traitement est dans une 'liste noire' :

- DPIA
- DPD

Sommaire

I – Principes RGPD 20'

II – Application à la recherche clinique en France 20'

III – Exemple - Success Story - Problem Solving - Cas d'école 20'

II – Application au secteur des Ind. De Santé en France

C'est le mille-feuilles !

EUROPEAN COMMISSION
Press Release Database

EUROPEAN MEDICINES AGENCY
SCIENCE MEDICINES HEALTH

GAMP 5 Guide

ICH
harmonisation for better health

E6 Good Clinical Practice

CFR - Code of Federal Regulations Title 21
FDA Home · Medical Devices · Databases

GDPR

edpb
European Data Protection Board

Trust Services and Electronic identification (eID)

Proposal for an ePrivacy Regulation

Digital Single Market
#DSM

ISO

enisa
European Union Agency for Network and Information Security

International

Local

Projet de loi
relatif à l'organisation et à la transformation du système de sante

CNIL.

HAS
HAUTE AUTORITÉ DE SANTÉ

ansm
Agence nationale de sécurité du médicament et des produits de santé

Interaction entre de nombreuse lois et guidances

- Propres au secteur Santé et / ou recherche clinique
  - E.g.: EU PV Regulation 2010 /1235, EU CT Regulation 2014/536, CFR 21, GCP, ICH…
  - Lois locales: code de santé publique, Centres de Ressources Biologiques, MR-00X, AU-013,.
- ePrivacy : Directive UE (Règlement en attente), loi locale, code de conduite emails marketing
- Règlement eIDAS N°910/2014 : signatures électroniques
- Lois sur le patrimoine
- Lois locales sur les durées de stockage
- Bonnes pratiques de sécurité informatique (CNIL, ANSSI, associations)

EUROPEAN MEDICINES AGENCY
SCIENCE MEDICINES HEALTH

GAMP 5 Guide

ICH
harmonisation for better health

E6 Good Clinical Practice

Impact de ces lois sectorielles :

- Droit du patient à la modification ou oubli : opposition
- Obligation de contrôler les sous-traitants
- Réutilisation des données patients pour une autre étude, un registre, ou un entrepôt de données de santé : des limitations
- Réutilisation des données patients après son décès
- Les Els peuvent être conservés sans limite de temps (suivant avis de l'autorité locale)

Feed back du terrain

- C'est simple et c'est du bon sens
- Important d'avoir un accès privilégié à la CNIL
- Très peu de demandes de patients inclus dans études
- L'erreur humaine est la source la plus commune de fuite de données

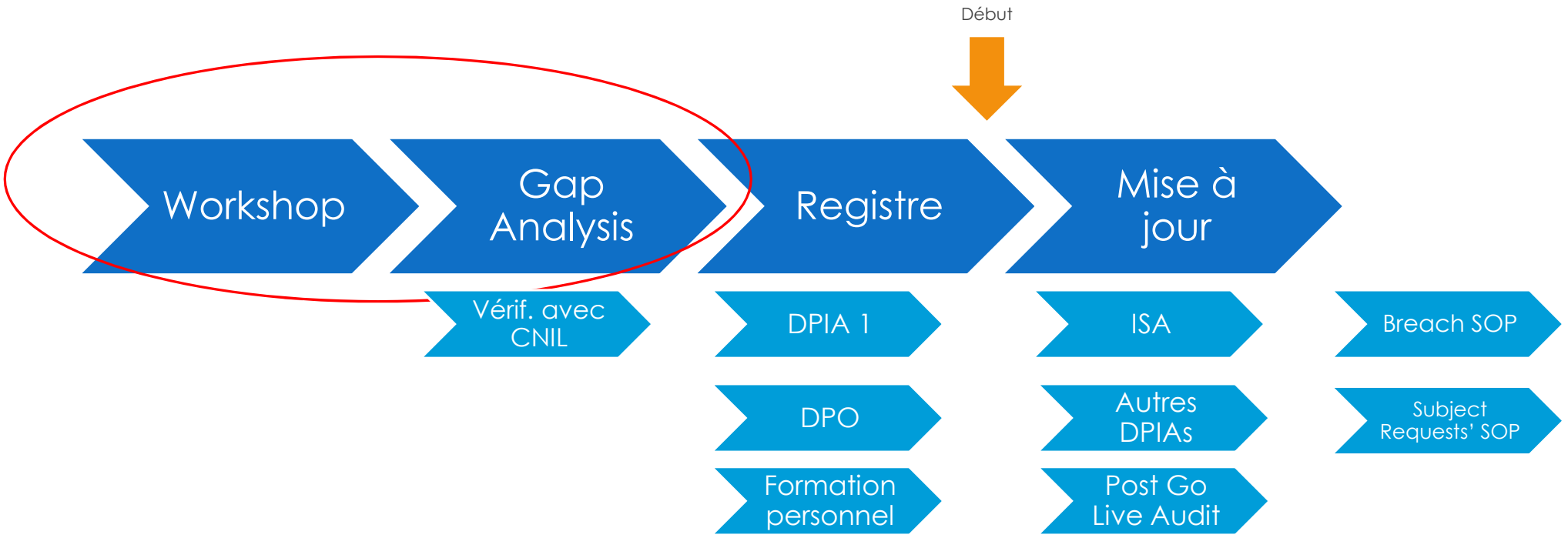
Sommaire

I – Principes RGPD 20'

II – Application à la recherche clinique en France 20'

III – Exemple - Success Story - Problem Solving - Cas d'école 20'

Méthodologie PharMarketing



Exemple

Merci de votre attention

Bertrand Le Bourgeois, MSc, Dipl. Ing.

b.p.lebourgeois@pharmarketing.net

D +33 1 48 83 87 25

www.pharmarketing.net

DATADOCKÉ

Organisme Formation enregistré sous le N° 11940969494

acdm association for clinical data management

AFAR AFCDP

DMB Data Management Biomédical

AMMIT Association des Métiers Médicaux des Industries de Santé