La protection des données dans la recherche en SHS

Edouard BÉNARD – Juriste en protection des données

Service Contrats de Recherche et Valorisation (CoREV)
Direction de la Recherche et de la Valorisation (DRV)
Pôle Recherche International Partenariats Innovation (RIPI)

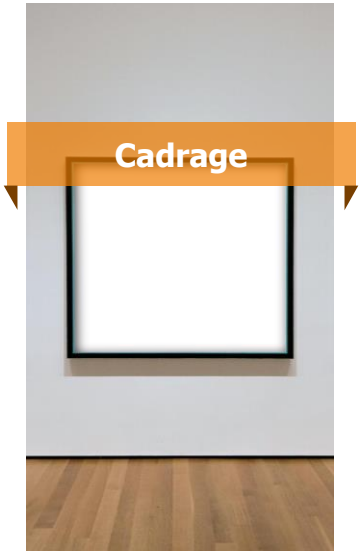
université de BORDEAUX

Sommaire

Conformité réglementaire

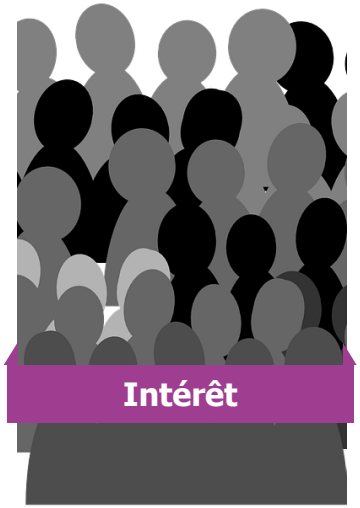
Contexte et enjeux

Comprendre le fonctionnement de l'humain



Protéger les participants contre toute atteinte physique et psychique, tout en évitant de nouvelles dérives

Réflexion approfondie pour protéger les personnes, quelle qu'elles soient, ainsi que leurs données



Doit toujours primer sur le reste

Dispositions générales

Carte d’identité

25 Mai 2018

Toute l’Union européenne

Tous les organismes traitant des données de personnes se trouvant dans l’UE

Périmètre

Applicable à :

- **Toute organisation** traitant des données à caractère personnel de **résident de l'UE**
- Toute organisation **hors UE** lorsque ses activités de traitement sont liées à une **offre de biens ou services** à l'égard de résidents de l’UE ou au **profilage** de celles-ci

Objectifs

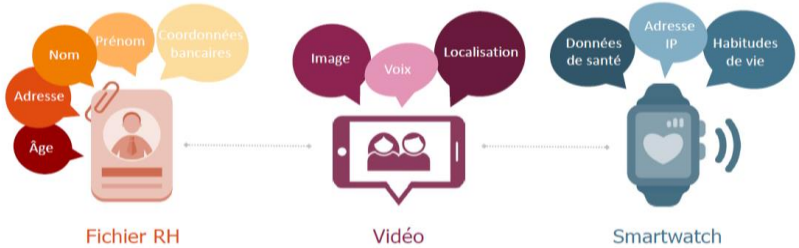
- Renforcer la protection des **données à caractère personnel**
- Intégrer la **proactivité et la sécurité durant tout le cycle de vie** de la donnée

Ambitions

- Harmoniser le **droit de la protection des données personnelles** au sein de l’UE, en particulier avec la multiplication des échanges transfrontaliers
- **Renforcer les droits** des individus et **clarifier les obligations** des organisations

Vue d'ensemble sur les notions essentielles

Une donnée à caractère personnel correspond à toute information permettant **d'identifier**, **directement** ou **indirectement**, une personne physique : la **personne concernée**
(indépendant du volume, du format, etc.).



Données « standards »	*Nom, prénom, adresse email, âge...*
Données « à risque »	*Coordonnées bancaires, géolocalisation...*
Données « sensibles »	*Religion, infractions, santé, origine ethnique...*

Les opérations réalisées

Traitement

Toute opération sur des données personnelles, effectuée de manière automatisée ou non, et appliquées à des données à caractère personnel

Exemples : collecte, conservation, diffusion, effacement ou suppression, enrichissement, etc.

Les acteurs de la conformité

Responsable du traitement

- Personne physique ou morale
- Finalité et moyens

Sous-traitant

- Personne physique ou morale
- Traite les données pour le compte du responsable

Data Protection Officer

- Chef d'orchestre de la conformité

D’un régime déclaratif à un régime de responsabilisation

Responsabilité	Gestion des risques	Privacy by design
• Plus de déclaration préalable à la CNIL • Consultation de la CNIL en cas de risque • Documentation interne	• AIPD/PIA (Analyse d’Impact relative à la Protection des Données) • Réduction des risques • Assurer la sécurité tout au long du traitement	• Dès la détermination des moyens • Protection optimale • Traitements conformes RGPD

Déclaratif

Responsabilisation

Les sanctions

Loi informatique et libertés

- Jusqu’à **150 000 €**
- **300 000 €** en cas de récidive

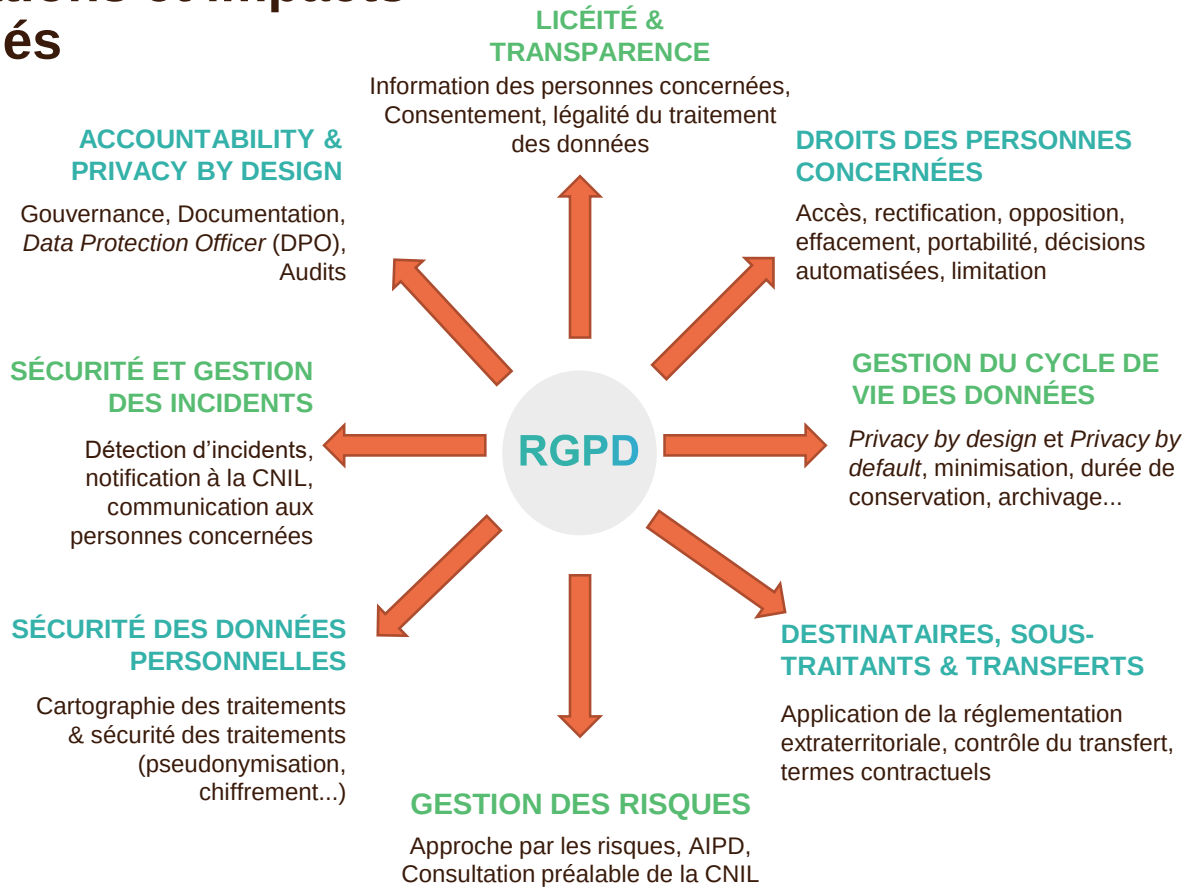
Loi pour une République numérique

- Jusqu’à **3 M€**

RGPD

- Jusqu’à **20 M€**
- ou **4% du CA mondial annuel**

Obligations et impacts associés



Comment assurer la conformité de son projet ?

ÉTAPE 1 : Cartographie des données

*La cartographie des données est un processus permettant de **recenser**, puis de **visualiser** les données soumises au régime de protection des données, étape indispensable de la mise en conformité.*

Périmètre de contrôle

Cartographie RGPD

- Traitements
- Acteurs
- Données
- Origine

Cartographie des travaux

- Stratégie
- Organisation
- Application
- Méthodologie

L'intérêt

- Conformité aux obligations légales
- Mesure de l'impact de la loi sur votre projet/étude
- Recensement précis de vos données

Documentation comportant notamment

- Traitement des données contrôlées
- Type de données traitées
- Origine des données
- Acteurs traitant les données
- Flux des données, origines et destinations

ÉTAPE 2 : Analyse d’impact sur la Protection des Données (AIPD)

*L’AIPD permet **d’analyser** et de **remédier** aux risques qu’un traitement peut engendrer sur la vie privée des personnes concernées.*

Une approche par les risques

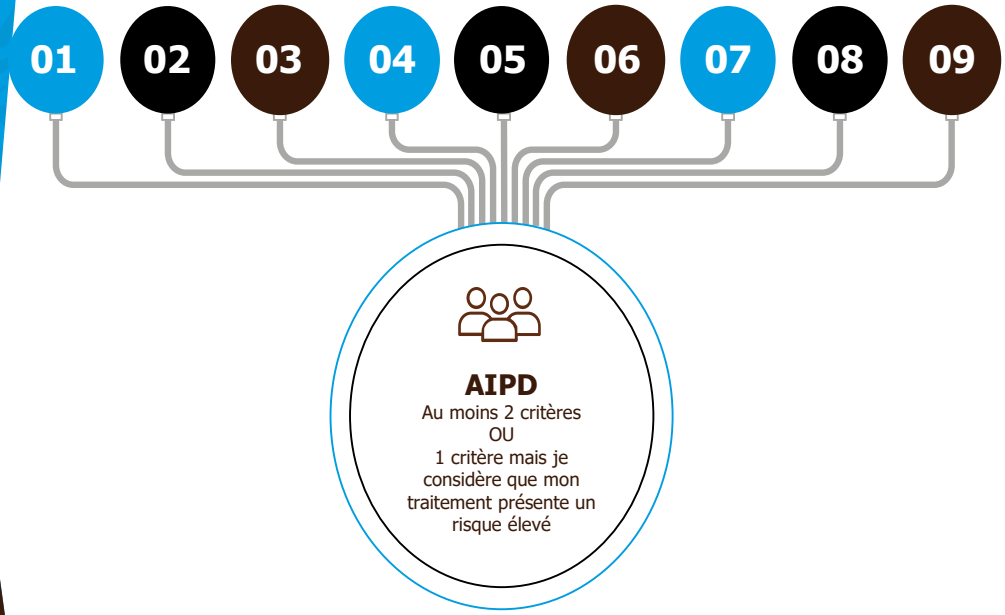
L’intérêt

- Conformité aux obligations légales
- Niveau de protection élevé des données traitées
- Connaissance et maîtrise des risques
- Valorisation de la données

Les conclusions

- Un rapport détaillé sur les risques qu’un traitement peut engendrer sur la vie privée
- Une visibilité sur les mesures à adopter pour diminuer ou faire disparaitre les risques

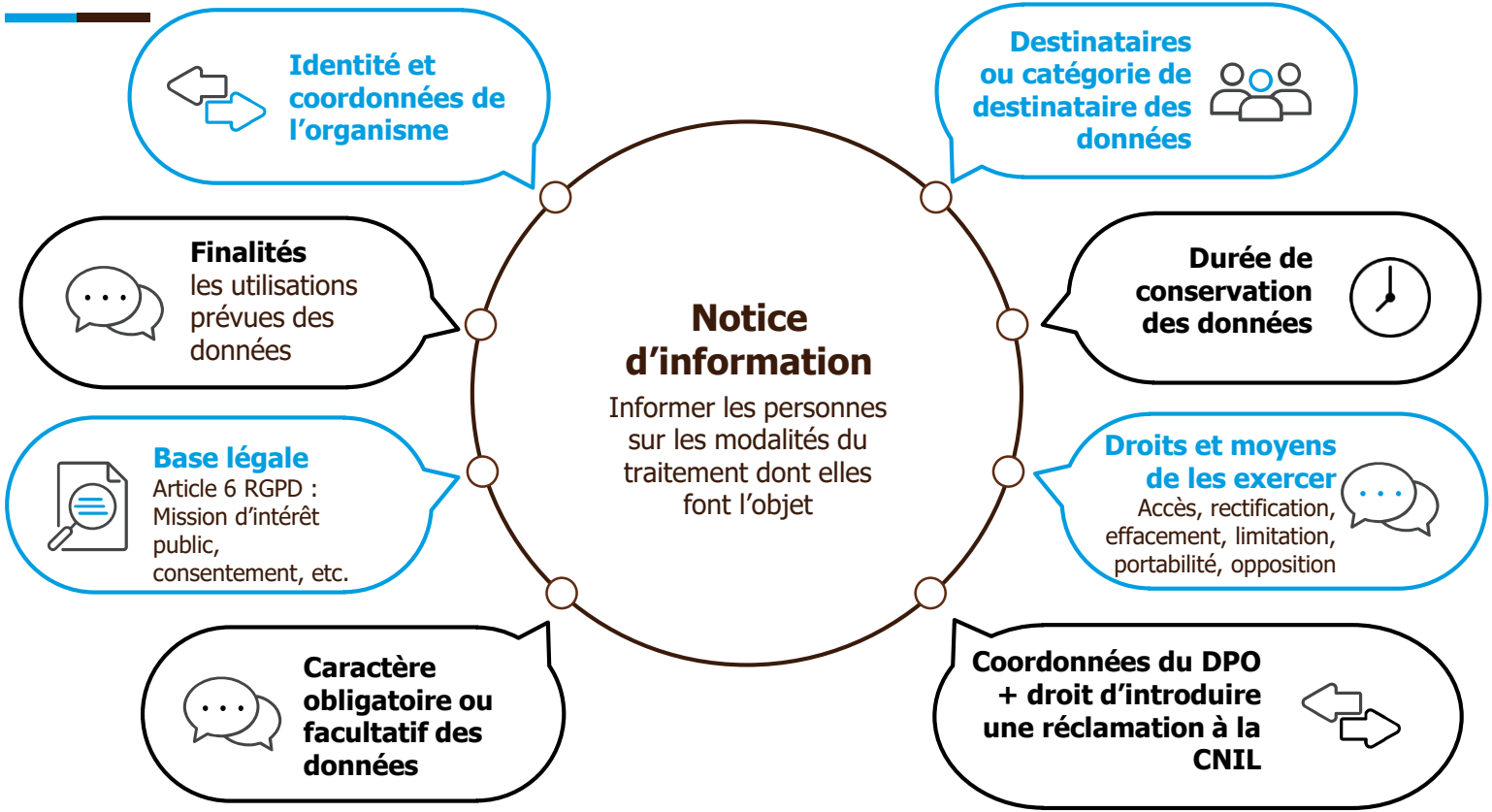
ÉTAPE 2 : Analyse d'Impact sur la Protection des Données (AIPD)



- **Évaluation/scoring**
- **Décision automatique** (effet légal)
- **Surveillance systématique**
- **Données sensibles** (santé, géolocalisation, etc.)
- **Collecte à large échelle** (selon contexte)
- **Croisement de données**
- **Personnes vulnérables** (patients, personnes âgées, enfants, etc.)
- **Usage innovant** (utilisation d'une nouvelle technologie)
- **Exclusion du bénéfice d'un droit/contrat** (scoring bancaire, allocations, etc.)

Recherche clinique (RIPH et RNIPH multicentriques) : AIPD obligatoire

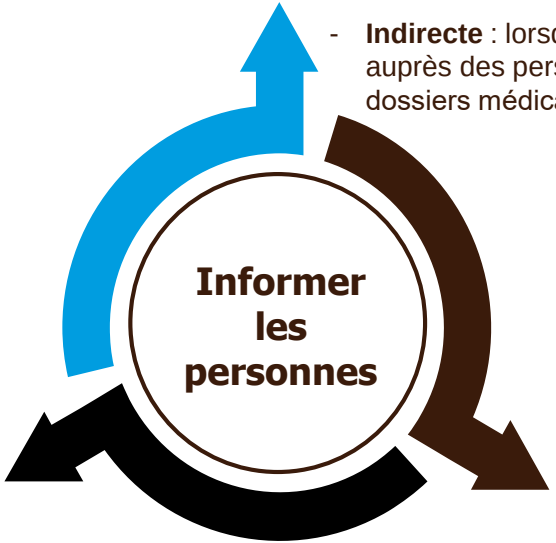
ÉTAPE 3 : Notice d'information



ÉTAPE 3 : Notice d'information

DÈS LA COLLECTE DES DONNÉES

- **Directe** : lorsque les données sont reccueillies auprès des personnes (ex : formulaire/questionnaire en ligne)
- **Indirecte** : lorsque les données ne sont pas reccueillies directement auprès des personnes (ex : données récupérées à partir des dossiers médicaux du patient, d'un partenaire académique, etc.)



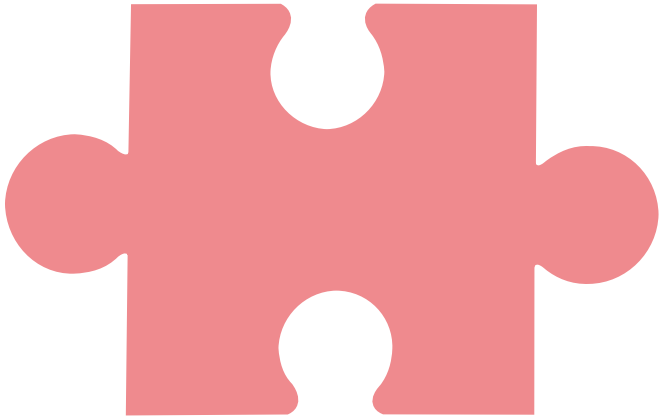
SOUS QUELLE FORME ?

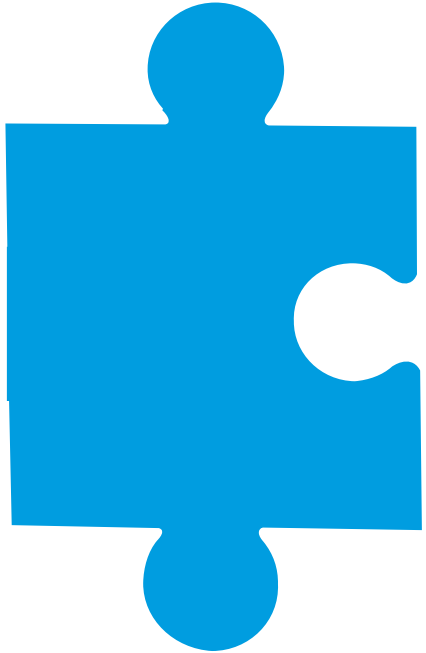
- Facile d'accès
- Fournie de manière claire et compréhensible
- Écrite de manière concise, afin d'amener les informations pertinentes

A QUEL MOMENT ?

- **Collecte directe** : au moment du reccueil des données
- **Collecte indirecte** : Dès que possible (notamment lors du premier contact avec la personne) et au plus tard, dans un délai d'un mois
- **Modification substancielle/événement particulier** : nouvelle finalité, nouveaux destinataires, changement dans les modalités d'exercice de droits, violation de données

Le consentement





Consentement Code de déontologie

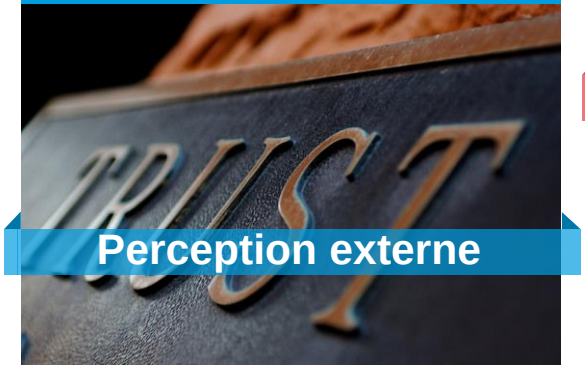
- **Prérequis pour conduire la recherche (le cas échéant)**

Consentement RGPD

- **Base légale du traitement de DCP (article 6 RGPD)**

Valeur ajoutée de la conformité RGPD

Gain en visibilité Externe et argument de confiance



La mise conformité au RGPD, de par sa forte exposition juridique et médiatique en fait un véritable **facteur de confiance** auprès du grand public, des partenaires académiques et industriels.

Amélioration des Processus internes, optimisation organisationnelle

La mise en conformité au RGPD, permet via la mise œuvre de ses principes, une **rationalisation** des processus organisationnels dans un objectif de responsabilisation des différents acteurs traitant des données à caractère personnel en interne (**institutionnel**, **formation**, **recherche**).

Volet cybersécurité

Au travers, entre autres, des obligations de notification et de sécurisation des données, la mise en conformité s'inscrit dans le **renforcement de la sécurité du SI** et permet de **gagner en maîtrise** sur celui-ci.

Conclusion

Pour résumer

1 CONCEPTION DU PROJET

- ✓ Quel est mon périmètre de recherche ?
- ✓ De quels types de données ai-je besoin ?
- ✓ Où est-ce que les données seront collectées ?
- ✓ Où les données seront-elles stockées ?

2 VÉRIFICATION DE CONFORMITÉ

- ✓ Complétion du questionnaire
- ✓ Notice d'information
- ✓ AIPD (le cas échéant)

3 VALIDATION + GO

- ✓ Relecture dossier
- ✓ Inscription au registre de traitement + validation DPO