

Ecole thématique 2020

EXPLO-SHS

12-16 oct. - La Rochelle



# Bonnes pratiques et cadre réglementaire

Isabelle André-Poyaud

UMR PACTE Grenoble

Mercredi 14 octobre 2020

# Avant propos

---

Vision d'un praticienne non juriste qui collecte, exploite et analyse des données d'enquêtes dans un laboratoire SHS et qui se pose des questions quant au cadre juridique.

# Objectifs de ce focus

---

- Apporter un éclairage sur le RGPD « règlement général sur la protection des données »
- Apporter un éclairage sur les plans de gestion de données (DPM) par un retour d'expérience
- Identifier des bonnes pratiques à adopter à toutes les étapes du cycle de vie de la donnée

# Plan

## Partie 1 - Le cadre réglementaire des données à caractère personnel en France

- Contexte historique de la loi informatique et libertés (Lil) et du RGPD
- Définir les notions clés (données personnelles, sensibles, traitement, fichier)
- Le Champ d'application du RGPD
- Les principes du RGPD
- Que faire en pratique (cas d'application)

## Partie 2 - Les plans de gestion de données

- Contexte
- Définition et contenu
- Un retour d'expérience : le plan de gestion de données de l'ANR Mobikids

# Introduction

L'**exploration** de données sous entend souvent l'existence d'un corpus de données déjà constitué.

Elle n'a de sens que **sur des données de qualité** :

- informations suffisantes pour en comprendre le sens,
- contrôles de cohérence vérifiés, données nettoyées...

Disposer de données de qualité, c'est **aussi prendre en compte le cadre réglementaire dès leur acquisition**

- point particulier sur les **données à caractère personnel** qui peuvent poser problème.

# Partie 1 - Le RGPD

# Contexte historique

1973

Développement de l'informatique, **volonté d'interconnexion de fichiers administratifs** par le numéro de sécurité social (projet Safari)

1974

Projet SAFARI rendu public dans les médias ! Début des **réflexions sur les risques de l'informatique sur la vie privée**

1978

Création de la **Loi informatique et libertés** et de la **CNIL**  
« informatique au service des citoyens mais ne doit pas leur porter atteinte »

1995

Publication de la **directive européenne sur les données personnelles**

2004

**Loi informatique et libertés 2** (intégration de la directive européenne et des évolutions technologiques et informatiques)

2016

14 avril - **Adoption** par le parlement européen du texte sur le **Règlement Général sur la Protection des Données**.

2018

7 octobre - Loi pour une république numérique (Loi Lemaire)

25 mai - **Entrée en application du RGPD**

→ Des lois qui se lisent en complément les unes des autres 7

# Champ d'application du RGPD

Le RGPD fixe le cadre de la protection des données personnelles et de leur circulation pour l'ensemble de l'UE.

- Tous les organismes publics, privés établis sur le territoire européen → **Laboratoires de recherche concernés**
- Tous les organismes publics, privés qui visent un traitement de données personnelles sur les citoyens et ressortissants de l'UE.



→ Définir un cadre commun à l'ensemble des pays de l'UE  
→ Proposer une bulle protectrice aux citoyens et résidents de l'UE.



# Enjeux du RGPD

- **Rendre aux personnes leurs droits** sur leurs données, limiter les risques d'atteinte à la vie privée (mise en oeuvre d'étude d'impact)
- **Imposer une sécurité maximale** des données à caractère personnel
- **Associer tous les acteurs dans cette responsabilité** (responsable de traitement RT, sous-traitants ST)
  - RT : personne physique ou morale qui initie le traitement, détermine les finalités et les moyens de traitement
    - Dans une UMR, DU=RT , responsable scientifique assure la conformité pour le DU
  - ST : effectue une prestation pour le compte et sur instruction du RT
  - (ex : HUMA-NUM pour ses accès à la plateforme d'enquête en ligne sphinx)
  - Possibilité de co-responsabilité de RT dans des projets complexes
- **Inversion de la preuve** : RT doit prouver à chaque instant la conformité d'un traitement de données personnelles avec le RGPD
  - Formalités de déclaration à effectuer auprès du délégué à la protection des données (déclaration à la Cnil supprimée sauf cas exceptionnels)

# Les principales définitions

En France ces **définitions** étaient déjà **posées dans la Loi informatique et libertés**

- données personnelles
- Données sensibles
- Traitement
- Fichier
  
- Personnes vulnérables

# Données personnelles

Toute information se rapportant à une personne physique et permettant son identification de manière directe ou indirecte.

**3 possibilités** d'identifier une personne

## 1 Directement

Il suffit d'une information pour retrouver une personne

### Exemple

nom, prénom, voix, photographie, vidéo,

## 2 Indirectement

Prises seules ces informations ne suffisent pas mais avec une table de correspondance oui

### Exemple

adresse IP, Numéro de téléphone, Numéro dans une table de correspondance

## 3 Par combinaison d'informations

informations fines permettant de retrouver une personne

### Exemple

âge, lieu résidence, Profession et une pratique de loisir

→ Possibilité d'identifier une personne avec des données nombreuses ou très précises

→ Réidentification d'une personne de plus en plus facile avec l'essor de l'intelligence artificielle

# Données sensibles

Données particulièrement encadrées par la loi en raison de leurs risques d'atteinte à la vie privée et aux libertés individuelles.

Il s'agit

- de l'origine raciale ou ethnique,
- des opinions politiques,
- des convictions religieuses ou philosophiques,
- de l'appartenance syndicale,
- des données génétiques et biométriques,
- des données de santé,
- des données sur la vie sexuelle et l'orientation sexuelle

auxquelles s'ajoutent :

- les données sur les infractions
- les données sur les condamnations pénales
- Le numéro de sécurité sociale (collecte autorisée par décret au conseil d'état)

**En principe, ces données ne peuvent pas être collectées.**

**Existence d'une exception recherche avec le consentement de la personne.**

**Si données rendues publiques par la personne** (opinion politique d'un élu).

Le délégué à la protection des données (DPP-DPO) peut demander un étude d'analyse d'impact sur les risques d'atteinte à la vie privée.

# Définition d'un traitement

Un « traitement de données personnelles » est une opération ou un ensemble d'opérations, portant sur des données personnelles, quel que soit le procédé utilisé.

## Des actions de traitements

- collecter
- structurer-organiser
- conserver
- extraire
- communiquer par transmission
- mettre à disposition
- enregistrer
- consulter
- adapter-modifier
- utiliser
- diffuser
- rapprocher des fichiers

## Tous les supports sont concernés

- support numérique : ordinateur, serveur, tablette, enregistreur, clé usb, cloud...
- support papier

Le **RGPD ne s'applique pas aux données personnelles** collectées uniquement dans le cadre **de la sphère domestique** (ex : son carnet d'adresse...)

# Identifier des personnes vulnérables

Des **dispositions sont à respecter** pour le traitement de données personnelles auprès de **populations vulnérables**.

## Exemples de populations dites « vulnérables »

- Enfants de moins de 15 ans,
- Personnes âgées,
- Salariés enquêtés sur leur établissement professionnel,
- prisonniers,
- réfugiés, demandeurs d'asile...

## Exemple d'une disposition :

Enquête auprès de personnes de moins de 15 ans nécessite le consentement du mineur et de la personne disposant de l'autorité parentale.

Le Délégué à la protection des données pourra demander la mise en œuvre d'une étude d'impact

# Les 8 règles d'or du RGPD

- Une base légale du traitement
- Une (des) finalité(s) définie(s)
- Une minimisation des données
- Une exactitude des données
- Une conservation limitée des données
- Une obligation de sécurité des données
- Une transparence aux personnes
- Des droits des personnes renforcés

# Le Fondement du traitement

Une démarche de mise en œuvre d'un **traitement de données personnelles repose sur une base légale** (6 fondements possibles)

- **Le Consentement**
- L'exécution d'un contrat
- L'obligation légale
- **L'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le Responsable de Traitement**  
→ Fondement de l'exécution de recherche publique
- La sauvegarde des intérêts vitaux
- **L'exécution d'une mission d'intérêt légitime** poursuivie par le responsable de traitement



# Le consentement

**Manifestation libre, spécifique, éclairée, révoicable et univoque** d'une personne qui donne son accord pour un traitement de données à caractère personnel.

- **Libre** : donner la possibilité d'accepter ou de refuser, ne pas exercer de pression,
- **Spécifique** : valable uniquement pour le traitement expliqué et objectifs associés ;
  - Pas de possibilité de conserver les coordonnées pour autre réutilisation sauf si demandé
  - Prévoir un consentement avec cases à cocher quand différents traitements : enregistrement de la voix, traitement des données, possibilité d'une réutilisation des données)
- **Éclairé** : donner suffisamment d'informations (à minima connaître)
  - identité et coordonnées du responsable de traitement,
  - les finalités,
  - les catégories de données collectées, durées de conservation,
  - l'existence d'un droit de retrait du consentement, les coordonnées du service pour exercer ces droits
  - les transferts envisagés hors UE
- **Univoque** : donné sans ambiguïté, pas de possibilité de pré-cocher des cases
- **Révoicable** : possibilité de le retirer à tout moment,

**Difficulté de ce fondement : Apporter la preuve (d'où consentement écrit) → tenir un registre des consentements, atténue le droit à l'oubli et l'effacement**

# Finalité d'un traitement

Les données ne peuvent être utilisées que dans un cadre d'objectif(s) déterminé(s) à l'avance

- **Explique le pourquoi de la mise en œuvre d'un traitement** (explication compréhensible donnée aux personnes concernées)
  - **Définit le périmètre** d'un traitement
  - **Légitime** (répondre au cadre des activités de recherche du laboratoire)
- Clé de voute de la pertinence des données, de leur durée de conservation, de la liste des personnes qui peuvent accéder aux données.
- Possibilité de sanction pénale en cas de détournement de finalité

# Finalité d'un traitement

## Finalité et recherche : que dit le RGPD ?

Prise en compte de la difficulté d'évaluer entièrement une finalité en amont

**« souvent, il n'est pas possible de cerner entièrement la finalité du traitement des données à caractère personnel à des fins de recherche scientifique au moment de la collecte des données ».**

(considérant 33)

- Donner un objectif de recherche plus large et le repreciser par la suite au délégué à la protection des données (il faut pouvoir justifier le pourquoi de cette finalité large)
- Attention ne pas donner uniquement un argument de finalité de recherche scientifique : c'est trop vaste !
- Possibilité de faire évoluer une finalité mais elle doit rester compatible avec la finalité de départ (penser à re-solliciter le DPD) ; Rgpd prend en compte la possibilité d'une seconde vie « des données de recherche » (penser au cas de la réutilisation)

# Minimisation et exactitude des données

Découle de la finalité d'un traitement

**Minimisation** : collecter uniquement les données nécessaires pour répondre aux objectifs du traitement, Avoir un lien direct avec la finalité envisagée (pertinence)

## Questions à se poser ?

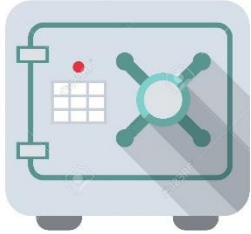
- A quoi va me servir cette donnée?
- Est-elle indispensable à mon objectif ?
- Ai-je besoin de cette précision ?

**Exactitude** : être en mesure de gérer les modifications, retraits, effacements

# Conservation des données

- Durée de conservation limitée des données personnelles → participe à la possibilité du droit à l'oubli
- Dépend de la finalité de traitement,
- Dès que l'objectif est atteint, prévoir selon les cas :
  - les effacements nécessaires de toutes les données ou un certain nombre
    - Attention, toutes les données ne sont pas destinées à être supprimées (supprimer la table de correspondance d'une enquête, supprimer les adresses mail de contact une fois la collecte close)
  - l'anonymisation ou pseudo-anonymisation des données
  - l'archivage des données : condition d'archivage doit être évaluée pour chaque traitement (passer d'une base active à un archivage intermédiaire et/ou définitif\*)
    - \*Archivage définitif : conditions à respecter selon le code du patrimoine

# Sécurisation des données



Point majeur du RGPD

Présente à toutes les étapes du traitement,

Concerne le responsable de traitement et le sous-traitant

A adapter selon la sensibilité des données

A mettre en place au niveau du laboratoire et au niveau individuel

- Réfléchir au lieu de stockage des données : Privilégier les structures d'hébergement de nos tutelles et d'Hum-Num. Utiliser des outils de transferts sécurisés entre les partenaires (FileSender), Attention : les transferts de données hors UE sont encadrés

## Quelques exemples de mesures de sécurité

Sécurité physique :

- Fermer les portes des bureaux,
- Sécuriser les salles serveurs,
- Donner un accès réservé aux salles serveurs

Sécurité logique :

- mot de passe individuel et robuste sur chaque machine,
- mise à jour des antivirus
- Verrouiller son poste informatique,
- Eviter les comptes partagés,
- Disposer d'une journalisation des accès à un serveur,

# Transparence de l'information

Un responsable de traitement s'engage à **être transparent vis-à-vis des personnes** sur les données qu'ils collectent et traitent.

- Une personne doit comprendre ce qui justifie le traitement
- Comprendre les conditions de traitement
- Connaître les modes d'accès à ses données

→ se joue **lors de la collecte** (directe et indirecte) **et lors de modifications importantes du traitement** (finalités, destinataires, problème de sécurité)

**Obligation de fournir un certain nombre d'informations** (diapo suivante) **en amont du traitement sur différents supports**

- Utiliser un langage clair, simple et compréhensible, adapté aux personnes concernées
- Effort à faire tant sur la forme que le fond des documents transmis
  - Formuler des phrases courtes,
  - Hiérarchiser l'information (jouer sur la typographie pour mettre en évidence les informations importantes)
  - Eviter les termes juridiques, techniques et abstraits de type (nous pourrions utiliser vos données, il est possible que, il se peut)

# Les informations à communiquer

## En cas de collecte directe :

- Identité et coordonnées du RT
- Finalité et base juridique du traitement
- Caractère obligatoire ou non de la collecte
  - Si fondement obligatoire donner les raisons et conséquences d'un refus
- Données concernées par le traitement et leur utilisation
- Durée de conservation des données (en année précise ou en termes de critère (ex : à la fin de la période contractuelle))
- Droits sur les données traitées et modalités d'exercices des droits
- Coordonnées du délégué à la protection des données et de la Cnil
- Les transferts de données hors EU s'ils ont lieu (vers qui et comment)

## En cas de collecte indirecte :

- + informations demandées dans la collecte directe
- sources des données, catégories des données



# Les droits couverts par le RGPD

Droits définis dans la Loi informatique et libertés : **Accès, modification, effacement (oubli), opposition,**

S'y ajoute :

Droit à la **portabilité** des données : possibilité de récupérer ses données dans un format interopérable

Droit à la **limitation du traitement** : geler un traitement pendant le temps de faire valoir un droit d'opposition ou de rectification

Droit de **ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé**

Droit de **connaître les violations de sécurité**

→ Exercices des droits à soumettre au responsable de traitement, délégué à la protection des données et en dernier recours auprès de la Cnil.

→ Des délais de réponse raccourcis : réponse maximale 1 mois après réception de la demande (même si on ne peut pas satisfaire la demande en expliquer la raison)

# Droits des personnes / actions à mener

Droits	Que faire ?
Droit d'accès	Donner toutes les données à la personne et lui expliquer tous les traitements opérés
Droit de rectification	Mettre à jour les données dans les meilleurs délais
Droit à l'oubli	Retirer les données dans les plus brefs délais, s'applique à partir de la réception de la demande de la personne, Si interconnexion : vérifier que tous les liens sont coupés
Consentement retiré	Enlever du fichier toutes les données personnelles du demandeur, s'effectue une fois le consentement reçu
Droit à la limitation	Isoler les données pour qu'elles ne soient plus traitées sur une opération ou toute opération spécifique
Droit à la portabilité	Transmettre à la personne ses données dans un format interopérable
Droit à l'opposition	Arrêter tout traitement des données personnelles du demandeur

# Cas d'application 1

Réaliser une **enquête par questionnaire en ligne** sur les **pratiques de consommation** auprès de personnes de plus de 18 ans résidant en France.

Les données de l'enquête seront exploitées par différents partenaires, soient des **membres d'UMR et d'unités d'accueil situées en France**.

Les porteurs du projet ont choisi **d'utiliser une plateforme d'enquêtes gérée par les services d'une université**.

Quelles démarches adopter ?

# Démarches à effectuer exercice 1

Identifier la présence de données à caractère personnel : (données **personnelles**, données sensibles)

Reconnaître des populations potentiellement vulnérables : **Non**

Intervention de sous-traitants ? **Oui (plateforme en ligne installée sur serveur de l'université)**

Identifier le responsable de traitement

Contacteur le délégué à la protection des données du RT (lui expliquer les objectifs du traitement pour définir la base légale)

Remplir le formulaire de déclaration au registre des données personnelles de l'unité du RT (connaître la politique du DPO quant à la tenue du registre : par le délégué ou au labo)

Adresse du formulaire pour les laboratoires ayant défini le DPD CNRS

[https://intranet.cnrs.fr/protection\\_donnees/donnees/Pages/default.aspx](https://intranet.cnrs.fr/protection_donnees/donnees/Pages/default.aspx)

Joindre les documents pour évaluer la sécurité des données collectées sur la plateforme d'enquêtes en ligne (se tourner vers le sous-traitant pour disposer des documents)

Joindre le questionnaire, sa notice d'information, les mentions d'informations sur site internet

Expliquer comment les personnes sont contactées (si utilisation d'une mailing liste préciser qui l'a fournie...),

Expliquer comment les personnes sont informées de la mise en œuvre de ce traitement (mail avant le lancement de l'enquête, mail avec les informations et un lien vers le questionnaire...).

# Démarches à effectuer exercice 1

## Les informations aux personnes - avant ou au moment du lancement de l'enquête

- Prévoir une notice d'informations complète à télécharger (cf informations page 23)
- Prévoir une page d'informations sur le site du projet, labo,
- Renvoyer vers ce lien pour plus d'informations

## Dans le questionnaire

- Rappeler les objectifs du traitement, les coordonnées du RT, la personne, service à contacter pour exercer ses droits
- Prévoir une case à cocher pour faire attester la personne de la lecture des mentions d'informations (j'ai lu et compris les informations transmises dans la notice d'informations)
- Donner la possibilité de ne pas continuer l'enquête
- Prévoir une case à cocher pour savoir si la personne a 18 ans ou plus (pb des mineurs )
- Prévoir des réponses facultatives à toutes les questions du questionnaire

**Après la collecte** : pseudo-anonymiser des données, retirer les mails

# Cas d'application 2

- Collecter des données indirectement identifiantes via une API (en ayant l'accord de la société)

## → Cas d'une collecte de données indirectes

Identifier les catégories de données personnelles,  
le nombre de personnes concernées par cette extraction

### Mes démarches :

- Contacter le DPD pour l'informer de ce traitement
  - définir avec lui la base légale de traitement
  - identifier avec lui le besoin de mener une étude d'impact en fonction des données personnelles récupérées et du nombre de personnes
- Remplir le registre des données personnelles
- Respecter les mesures de sécurité définies dans le registre
- Informer les personnes de cette collecte de données indirectes
  - difficulté de contacter toutes les personnes ; mentionner le traitement sur le site du laboratoire en précisant la liste des informations en cas de collecte indirecte

# Du sur mesure

Deux exemples assez simples,  
mais chaque traitement est souvent unique !

Certaines déclarations au registre sont plus complexes que d'autres... peuvent nécessiter une études d'impact sur les risques d'atteinte à la vie privée

D'où la nécessité d'anticiper !

Par ses principes, le RGPD (comme la Lil avant) nous conduit à **anticiper les chaînes de traitement de données à caractère personnel**

- nous **développons ainsi des bonnes pratiques** qui nous conduisent à produire des données de qualité qui **assurent le respect des personnes et la sécurité informatique**
- Ces bonnes pratiques s'inscrivent dans la plupart des étapes du cycle de vie des données.

**Pourquoi ne pas s'approprier d'autres outils pour continuer à produire des données de qualité, quelle que soit leur nature ?**

Le plan de gestion des données DMP pourrait-il répondre à ce besoin ?



# Partie 2 - Les plans de gestion des données

# Contexte de mise en œuvre des DMP

## Les DMP s'inscrivent dans un enjeu d'ouverture des données.

- La Loi Lemaire (7 octobre 2016) - ouverture des données financées à hauteur de 50% sur fonds publics (sauf si exceptions dont RGPD)
- Plan national de la science ouverte (juillet 2018)

Pour tendre vers l'ouverture des données, celle-ci doivent être produites avec qualité (prise en compte des maillons de la chaîne situés en amont de cette étape)

→ d'où l'idée d'impulser une politique autour de la gestion des données

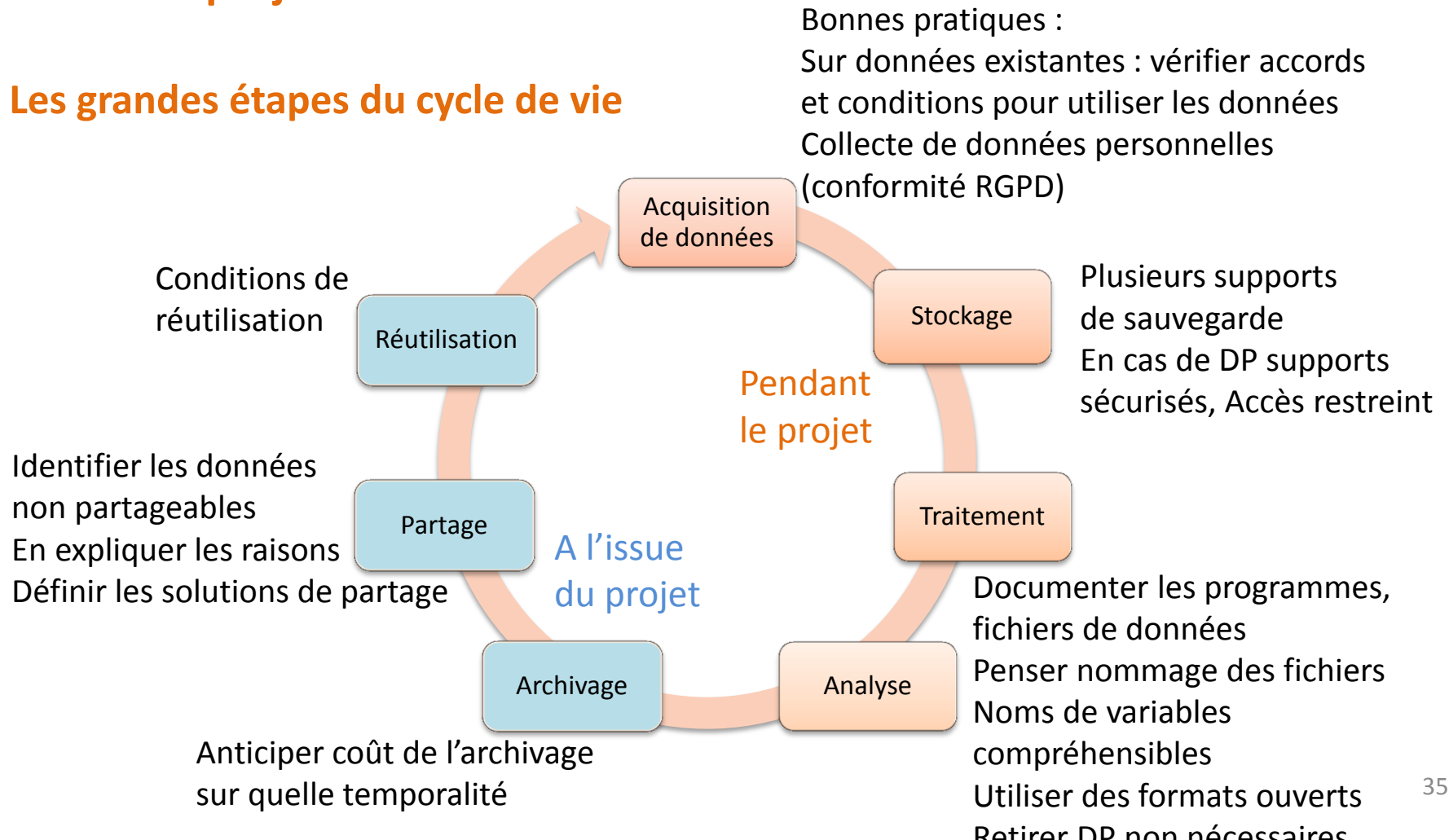
### → Les plans de gestion des données : outils de cette politique

- Rendus obligatoire par certains financeurs (ANR depuis 2019, H2020 2016 et ERC 2017)
- Encouragés par certains établissements (universités, EPST)

# Définition d'un DMP

Plan de gestion des données : **document écrit, formalisé** qui **visent à suivre les données d'un projet tout au long de leur cycle de vie pendant et à l'issue du projet.**

## Les grandes étapes du cycle de vie



# Définition d'un DMP

DMP **encourage les réflexions autour du PRINCIPE FAIR** (données Faciles à trouver, accessibles, interopérables, réutilisables)

- Décrire finement la nature des données,
- Décrire les méthodes d'obtentions (collecte auprès de personnes, collecte sur internet, recueil avec des capteurs, les technologies utilisées)
- Décrire le contenu des données (création de métadonnées, de dictionnaire des variables...)
- Gérer le stockage immédiat et à plus long terme (savoir où se trouve les données, donner les moyens d'accéder à ces espaces de stockage)

Initié au début d'un projet et l'accompagne pendant toute sa durée

- mise à jour à jour régulière du DMP (projets ANR et européens : à minima 3 versions, possibilité d'en faire davantage !)

Temporalité

dans les 6 mois du  
début du projet

à mi-parcours

finale à la fin du projet

# Contenu d'un DMP

Structuré autour de **7 thématiques** et de questions

Quelles ressources financières et humaines pour une gestion à long terme ?

Ressources financières et humaines

Responsable scientifique, nom du projet, financeur, N° convention, partenaires

Informations administratives liées au projet

Quelles données, produites, utilisées ?  
De quel type,  
Sous quel format,  
Quel volume ?

Qui peut accéder après le projet ? Dans quel délai ?  
Sous quelles conditions ?

Accès, Partage des données

Collecte des données

**DMP**

Cadre légal – propriété intellectuelle

Documentation et métadonnées

Quels accords entre les partenaires pour utiliser les données ?  
Statut particulier de certaines données ?

Stockage, sécurité sauvegarde

Comment les données sont décrites ? Où trouver ces descriptions ?  
Quels standards sont utilisés ?

Où sont stockées les données, métadonnées ?  
Comment sont protégées les données ? Qui gèrent les accès ?

# Retour d'expérience sur le DMP de Mobi'kids



Projet ANR financé en 2017 (coord : S.Depeau, UMR ESO)

Une équipe pluridisciplinaire (géographes, géomaticiens, informaticiens, statisticien, urbanistes, architecte, psychologue, juriste) ;

2 partenaires privés et 4 équipes de recherche

**Objectif :** Observer et comprendre la mobilité quotidienne des enfants et leurs conditions d'apprentissage de l'autonomie dans leurs déplacements

Suivi d'enfants 9-12 ans et de parents pendant 5 jours sur 2 périodes successives (en CM2 et 6e) dans Rennes et son agglomération

# Mobikids : des données et des outils

Un corpus de données diversifiées :

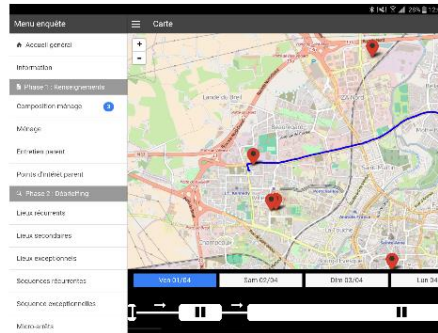
des traces gps, des enquêtes par questionnaires, des entretiens, du son, de la vidéos/photos, des cartes mentales, des notes d'observations sur les errains.

C'est aussi le développement de :

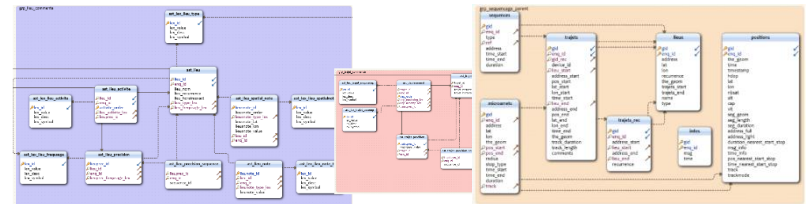
Dataloggers GPS



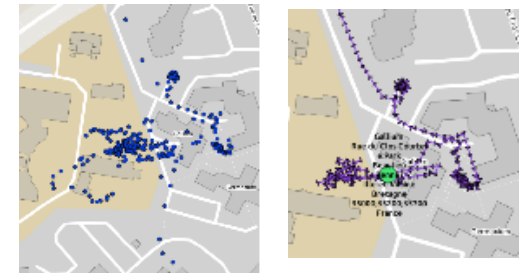
Une application tablette pour mener l'enquête



Une base de données



Des algorithmes informatiques pour séquencer des traces et détecter des arrêts



**Proposition de rendre un DMP comme livrable à l'ANR pour suivre toutes ces données de recherche**

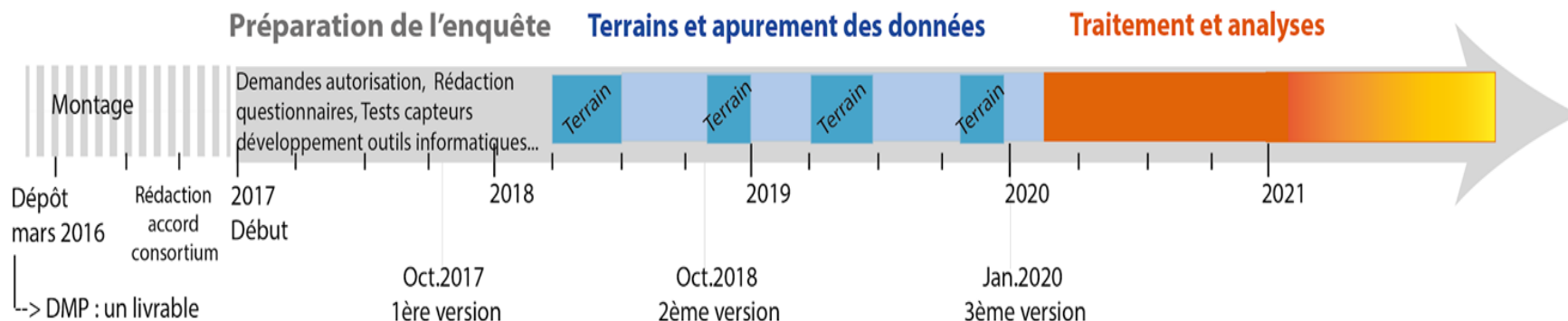
# Sa mise en pratique (notre cuisine)

- Un groupe de travail de 4 personnes au compétences complémentaires
  - droit
  - statistique,
  - géomatique,
  - informatique,
- Base de travail : maquette de DMP de l'Inra (2017)
  - Aujourd'hui: maquettes de DMP en ligne sur DMP Opidor (<https://dmp.opidor.fr/>)
- Une interaction avec le reste de l'équipe
  - Des temps d'échanges entre nous pour constituer le document,
  - Des présentations en séances plénières et des questionnements à traiter avec tous

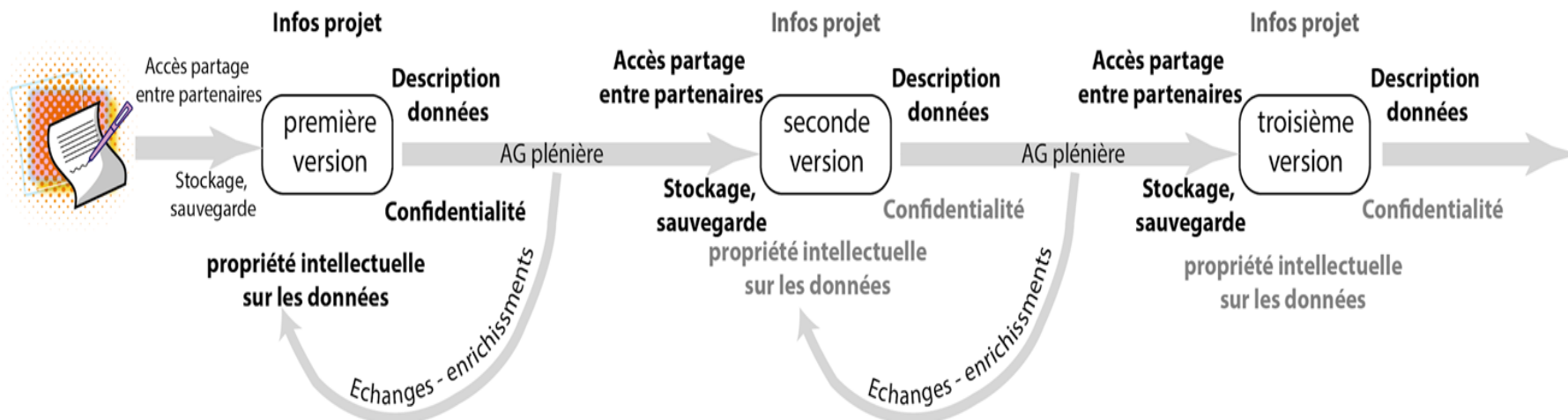


# Suivi du projet ANR MOBIKIDS et de son DMP

## Grandes étapes du projet



## Versions du DMP



# Avantages / Limites

## Nos limites :

- Trouver le bon niveau de rédaction (document général / très précis).  
Difficulté de positionner le curseur sur les questions techniques de sécurité et d'accès au serveur
- Pas de personne compétente dans les métiers de l'IST (pas d'utilisation de métadonnées standardisées)
- Pas anticipé les coûts financiers liés à la réflexion sur l'ouverture (les données collectées sont personnelles)

## Les avantages perçus :

- Avoir une vue d'ensemble sur un projet complexe
- DMP finalement considéré comme un outil de gestion de projet
- Assurer la traçabilité des différents jeux de données
- Percevoir des problèmes techniques et les anticiper (accès lieu de stockage)
- A permis d'anticiper d'éventuels points de tension entre les partenaires
- A favoriser des bonnes pratiques au sein du consortium

# Conclusion

- Importance d'initier des bonnes pratiques le plus en amont de la chaîne de traitement.
- Pour les données personnelles : importance de se conformer au RGPD
  - les personnes connaissent de plus en plus leurs droits, les réputations des laboratoires sont engagées
- Pour les autres données : favorise leur ouverture



Toutes ces réflexions ont été menées depuis plusieurs années avec mes collègues du groupe d'appui méthodologique Ariane de Pacte.

