

Les données à caractère personnel et le cycle de vie

Caroline Buscal

Serda

France

Céline Avignon

Lexing Alain Bensoussan Selas

France

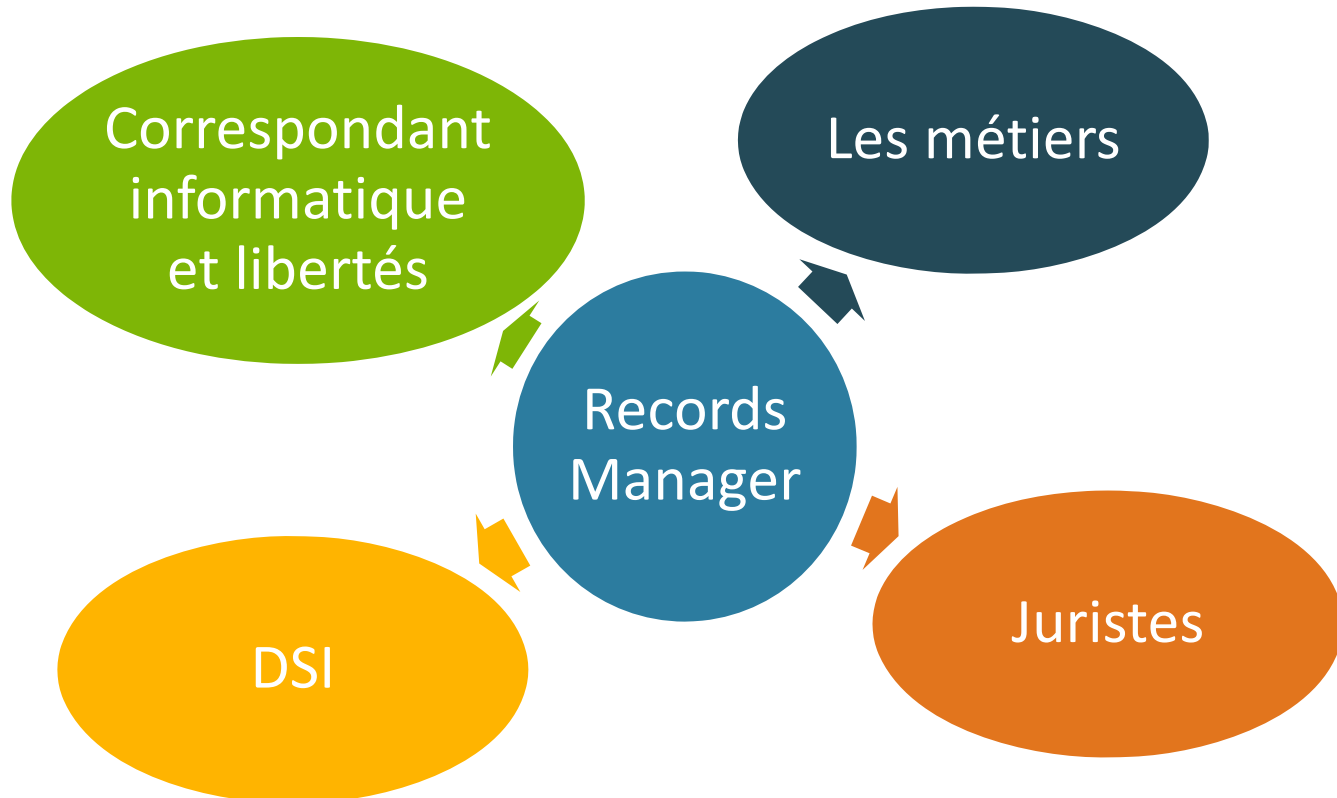
Pourquoi appliquer la loi I&L au cycle de vie ?

- Le champ d'application de la loi :
 - ✓ Les traitements automatisés de données à caractère personnel.
 - ✓ Les traitements non automatisés et les fichiers.

Pourquoi appliquer la loi I&L au cycle de vie ?

- Les principes fondamentaux :
 - ✓ Traitement loyal et licite.
 - ✓ Finalité déterminée, explicitée et légitime.
 - ✓ Données pertinentes, adéquates, non excessives, complètes, exactes et mises à jour.
 - ✓ Formalités auprès de la Cnil (déclaration/autorisation).
 - ✓ Obligation d'information et droits des personnes.
 - ✓ Durée de conservation proportionnée (cf. infra).
 - ✓ Encadrement des flux transfrontières (cf. infra).
 - ✓ Mesures de sécurité et de confidentialité (cf. infra).

Quels interlocuteurs pour le RM sur l'ensemble du projet ?



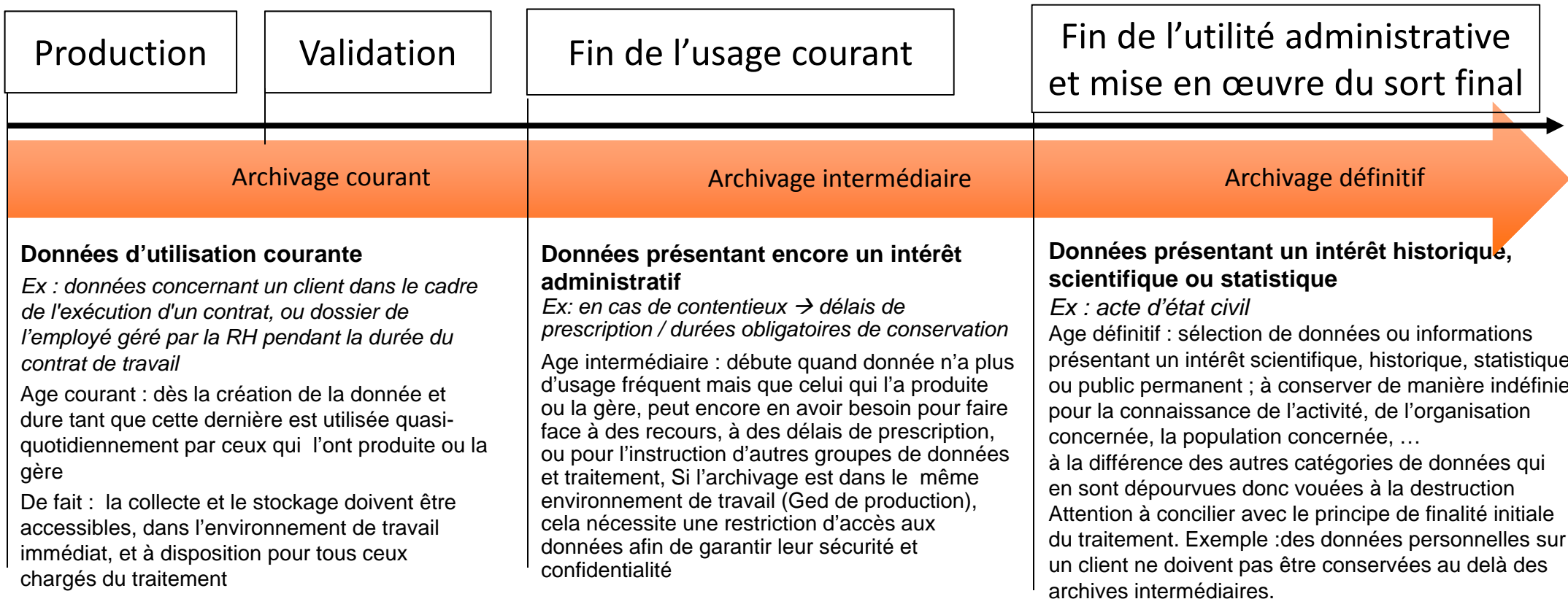
Pourquoi « cycle de vie » ?

- Parce qu'une donnée, une information ou un document, c'est organique : ça naît, ça vit, ça meurt.
- Parce que tout garder de la même façon est source de complexité et de risque : cela ne permet pas de distinguer ce qui est vital, non vital, prioritaire, engageant, etc.
- Parce que le droit à l'oubli devient le devoir d'oubli.
- Parce que les données et les informations sont hybrides (papier, électronique, microfilm).
- Parce qu'il faut adapter les modalités de description, de stockage et d'accès en fonction aussi des obligations.
- Parce que tout garder sur le même plan est coûteux.

Pourquoi « cycle de vie » ?

Quelles sont les étapes du cycle de vie :

elles sont au nombre de 3 : courant ou actif > intermédiaire ou semi actif > définitif



Comment détermine-t-on la durée de la conservation ?

Le référentiel de la Cnil en quelques exemples :

- Norme simplifiée 48 « clients / prospects » :
conservation active pendant la durée de la relation commerciale (+ 3 ans pour les données utilisées à des fins de prospection) + archivage pendant les délais de prescription.
- Norme simplifiée 46 « gestion administrative du personnel » : conservation active pendant la durée du contrat de travail + archivage pendant les délais de prescription.

Comment détermine-t-on la durée de la conservation ?

Les durées de conservation obligatoires :

- C. Com., art. L. 123-22 : 10 ans pour les documents comptables et pièces justificatives.
- C. Consom., art. L. 134-2 : 10 ans pour les contrats conclus par voie électronique > 120 €.

Quelle précaution en présence de flux transfrontières ?

Principe d'interdiction vers un Etat hors Union Européenne sauf :

- Protection équivalente (convention n°108) / adéquate (art. 25 directive 95/46/CE) / suffisante (art. 68 loi I&L).
- Consentement de la personne concernée.
- Exceptions (par exemple, flux nécessaires à l'exécution d'un contrat ou à la sauvegarde de la vie humaine).
- Encadrement contractuel (clauses contractuelles types vers un responsable de traitement ou vers un sous-traitant, BCR / règles internes, contrat ad hoc).

Quelle précaution en présence de flux transfrontières ?

Spécificités :

- Formalités préalables
- Mentions obligatoires

Quelles mesures de sécurité et de confidentialité ?

- Méthode de gestion des risques.
- Protection des archives (sécurisation, intégrité, politique d'archivage, déclaration des pratiques d'archivage).
- Traçabilité (accès, actions, procédure d'exploitation).
- Gestion des violations de données à caractère personnel (détermination des rôles et responsabilité, inventaire, mesures correctrices).
- Sécurisation des échanges avec les tiers.
- Gestion de la continuité d'activité (PCA, PRA, PSI).

le cnam



Quelles mesures de sécurité et de confidentialité ?

- SIF (clause de confidentialité, charte des systèmes d'information).
- Gestion des habilitations (principe du besoin d'en connaître et du moindre privilège, interdiction des comptes génériques, revue annuelle).
- Mécanismes d'authentification adaptés.
- Politique de mot de passe et caractéristiques.
- Lutte contre les codes malveillants (anti-virus, firewall, mises à jour de sécurité).
- Sécurité physique des locaux (accès, incidents).



Conclusion et mode opératoire

