AIDE-MÉMOIRE ARCHIVAGE ET DONNÉES PERSONNELLES

**Synthèse des deux Ateliers L’Oréal pour le CR2PA**

# Les Données personnelles et leur traitement

**Données personnelles**

Toute information se rapportant à une personne physique identifiée ou identifiable directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale;

**Traitement**

Toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que :

|  |  |  |  |
| --- | --- | --- | --- |
| la collecte | la conservation | la consultation | le rapprochement |
| l'enregistrement | l'adaptation | l'utilisation | l'interconnexion |
| l'organisation | la modification | la communication par transmission | la limitation |
| la structuration |  l'extraction | la diffusion ou toute autre forme de mise à disposition | l'effacement ou la destruction |

**Exemples de traitement :**

* Fichier clients (entreprise)
* Fichier usagers (administration)
* Fichier fournisseurs
* Annuaire interne
* Contrôle d’accès (badgeuses)
* Site internet
* Logs de serveurs

**Transfert de données**

* On parle de transfert de données lorsque les données sont transférées depuis le territoire européen vers un pays non membre de l’Union Européenne.
* Le transfert peut s’effectuer par communication, copie ou déplacement de données, par l’intermédiaire d’un réseau (ex. accès à distance à une base de données) ou d’un support à un autre, quel que soit le type de support (ex. d’un disque dur à un serveur).

**Exemples de transferts :**

* Sous-traitance de la maintenance d’un site Web
* Accès en consultation à une base de données à partir d’un pays hors UE

# Le règlement européen

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016. Ce règlement est applicable à compter de mai 2018.

***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***

Il concerne tout « traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier » pour toutes les données personnelles produites en Europe ou passant par des systèmes informatiques européens, soit un périmètre **très très** large.

Il est aussi appelé GDPR (pour « **General data protection regulation** »), et abroge la précédente génération de texte (Directive européenne 95/46/CE de 1995)

Note : Une directive doit être transposée en droit national, un règlement s’applique tel quel !

Le GDPR durcit significativement les obligations des organismes traitant des données personnelles –et les peines applicables en cas de non-conformité : amende pouvant aller jusqu’à 4% du chiffre d’affaire mondial, publication des noms des contrevenants, et surtout en cas de fuite de données personnelles l’information nominative des personnes concernées. Bonjour la réputation…

L’exigence de maîtrise des PII et le renforcement du « droit à l’oubli » sur simple demande des individus imposent en pratique dès mai 2018 une gouvernance de l’information efficace, des processus, une chaîne de responsabilité par traitement et des outils informatiques et workflows humains auditables.

De nombreux éléments restent à définir en pratique avant mai 2018, notamment les cadres d’audit.

# Vocabulaire

* Données personnelles ou DP
* Personal Data ou Personnaly Identifiable Information (PII)
* Règlement européen ou RGPD ou GDPR (General Protection Data Regulation)
* DPD : Délégué à la Protection des données ou DPO : Data Protection Officer, responsable nommé obligatoire à partir d’une certaine taille d’organisation. « Super CIL » (Correspondant Informatique et Libertés)

# Les données personnelles sont-elles des données à part ?

C’est une catégorie de donnée comme une autre, mais liée à une règlementation spécifique et sur laquelle porte un droit de contrôle d’autorités nationales indépendantes : en France, la CNIL.

**Note**. La loi concerne aussi bien les données personnelles sur support papier que dans des bases de données ou dans des documents électroniques. Les risques de partage abusif ou d’usage non prévu sont bien sûrs accrus en cas de support numérique, mais cette non-distinction répond d’une part au souhait d’éthique qui inspire le GDPR et au constat pragmatique qu’il est aujourd’hui très facile de scanner et OCRiser un fichier papier ou un dossier.

**Le principe de base** de la collecte de données personnelles est la proportionnalité : collecter ce qui est nécessaire à l’activité, le conserver en sûreté durant la durée minimale pour cette finalité.

Des sanctions particulières sont prévues en cas de gestion inadaptée :

* Sanctions financières
* Publication dans les journaux : impact sur la réputation de l’entreprise

Du fait ce ces caractéristiques, les Données personnelles ont des particularités fortes pour l’archivage et la gestion en général

* elles doivent être « catégorisées » et identifiées
* ce sont par nature des données engageantes
* il faut les tracer : lieu de conservation, durée de conservation, destruction, droits d’accès

Trois impératifs structurent la gestion d’une donnée personnelle

* + Pas de collecte « au cas où » :
	+ Nécessité de gérer son cycle de vie
		- Elle doit être détruite avant le terme maximal de son échéance
		- Elle doit pouvoir être détruite à la demande de la personne concernée : donc nécessité de savoir où elle est conservée (base de données, documents non structuré…)
	+ Nécessité de protection et de contrôle des accès
		- Seules les personnes qui ont le besoin d’en connaître doivent pouvoir y accéder
		- Des mesures organisationnelles et techniques doivent être mises en place afin de les protéger d’une mauvaise utilisation, de la malveillance ou d’une réutilisation inappropriée

# Exemples de données personnelles

|  |  |
| --- | --- |
| * + Nom
	+ Prénom
	+ Situation familiale
	+ Adresse
	+ Pays
	+ Région
	+ Ville
	+ Données de géolocalisation
	+ Données de connexion (Adresse IP, logs…)
	+ Email
	+ Téléphone
	+ Age
	+ Date de naissance
 | * + Signature
	+ Genre
	+ Ethnie
	+ Informations bancaires
	+ Données biométriques (empreinte digitale, image de la rétine…)
	+ Données biologiques
	+ Habitudes de vie
	+ Type de peau
	+ Type de cheveux
	+ Photos
	+ Vidéos
	+ Données de santé
	+ Voix
 |

# Catégories de personnes concernées par la collecte de leurs données personnelles

* + Salariés
	+ Prestataires externes à l’entreprise
	+ Clients / Consommateurs / Usagers / Adhérents
		- Attention particulière à porter aux mineurs
	+ Patients
	+ Visiteurs
	+ Etudiants / Elèves

# Le GDPR et sa mise en œuvre

Calendrier

* + La règlementation sur les données personnelles en France date de 1978 (loi « CNIL »), avec des contrôles réguliers de la CNIL et de nombreuses affaires de fichiers illégaux ou fuites parues dans la presse (Cdiscount, Boulanger, partis politiques…)
	+ Les audits et sanctions du règlement européen seront applicables dès mai 2018

La mise en œuvre du GDPR implique des cartographies car elles sont nécessaires à la gouvernance :

* Les finalités de collecte
* Les besoins d’usages des métiers ou des opérationnels : les traitements (notamment les transferts)
* Des projets utilisant des données personnelles
* Ces recensements sont variés et doivent être menés en coopération avec l’IT et le service Juridique pour prendre en compte les différentes expertises métiers
	+ Applications et espaces de stockage
	+ Bases de données
	+ Espaces documentaires
	+ Flux
	+ Hébergements des données
	+ Localisation des serveurs

Une maîtrise de la localisation des documents/données (idem que papier)

* + Pour connaître les copies
	+ Pour pouvoir assurer une destruction effective
	+ On voit surgir des exigences croissantes de localisation nationale (« cloud souverain français », demandes russes…) sur fond de protection des consommateurs mais aussi d’enjeux géopolitiques (risque accru de sanctions « exemples »).

Changement majeur du GDPR par rapport aux besoins d’archivage :

* + Obligation de conserver les documents du système de management du DGPR
	+ Obligation de traçabilité du cycle de vie de la données personnelle : de sa collecte à sa destruction, et de son utilisation (quand, comment, par qui et pourquoi)

# Les obligations du GDPR en pratique

Droit des personnes :

• Accès, modification, suppression, opposition

Finalités de traitement :

• Privacy by design

• Questionnaire Métier

• Etude d’impacts (PIA)

Sécurité et confidentialité :

• Localisation des données,

• Protection contre l’intrusion, vol et détournement

• Gestion des droits

• Procédure de sauvegarde et récupération

Sécurité des flux de données intra-groupe et hors UE :

• Inventaire des traitements et des flux

• Procédures de suivi et de contrôles

Relations avec les prestataires et partenaires :

• Imposer des prérequis de conformité

• Obtenir des engagements contractuels forts

• Exiger de la transparence

# Le DPO et l’archivage managérial

Le délégué à la protection des données (DPO) est un nouveau rôle qui n’est pas simplement une nouvelle dénomination des correspondants informatiques et libertés (CIL). Il s’agit d’un acteur majeur dans la gouvernance de l’information en entreprise, avec un poids stratégique plus important et un devoir d’alerte via les PIA (Privacy Impact Assessment) ou études d’impact. Il n’est pas, par contre, un parapluie : le responsable de traitement pourra être tenu responsable de ce qu’il a validé.

Description du DPO sur Wikipedia : <https://fr.wikipedia.org/wiki/D%C3%A9l%C3%A9gu%C3%A9_%C3%A0_la_protection_des_donn%C3%A9es>

En moyenne dans les entreprises représentées au CR2PA, les rôles du CIL, du futur DPO, des Archives et des responsables sécurité Informatique (RSSI/CISO) ne sont pas clairement harmonisés, non plus qu’avec d’autres entités comme le CDO.

* Articulation de règlements et lois distinctes, de différents métiers d’origine
* Pas de lien organigramme. Des discussions existent, parfois des projets, mais peu de coopération étroite
* Nommer un DPO est une obligation, mais beaucoup de recrutements se font à l’extérieur avec des externes qui ne connaissent pas les procédures maison, ou viennent du Juridique et se contentent d’une approche légale parfois assez éloignée du terrain opérationnel
* Les Archives ont un rôle à jouer : spécialistes de la gestion d’info sur le long terme, bonne connaissance des accès à l’info et donc des questions d’accès et d’éliminations
* Les Archives peuvent apporter la garantie de leurs procédures
* Procédures communes -> médiatisation, simplification : il est souhaitable d’éviter les circuits parallèles, redondants.

**En progrès :** la capacité à conduire des projets d’une gouvernance d’information est plus importante qu’il y a quelques années et le GDPR prévoit une certaine liberté dans un cadre rigide : le DPO externe

* Pour les PME, l’appel à une AMOA externe est souvent intéressant, d’autant que le règlement européen prévoit que le DPO peut être mutualisé
* Pour les grands groupes, le connaissance interne des métiers est un + et le DPO interne est une meilleure solution : l’empathie opérationnelle fera toute la valeur de ses recommandations.

Pour les Archives, impliquer le CIL et le DPO dans l’élaboration ou la validation du référentiel de conservation est un atout :

* Position systématique : Conservation/Destruction
* Justification : Pas de collecte « Au cas où »
* Appui réglementaire : justification des durées de conservation, des événements « à partir de » et des catégorisations de données/documents

=> au minimum cela implique des rendez-vous, des présentations réciproques entre les services « archives » et « données personnelles »

Pour le DPO, travailler avec les Archives apporte une meilleure connaissance des workflows

Le DPO est rarement dans le circuit de connaissance pour les documents non structurés qui contiennent de la donnée personnelle car en général ces documents relèvent de la politique d’archivage. D’où la nécessité d’un travail collaboratif du DPO et du responsable archivage pour établir des règles communes de gestion des données perso qu’elles soient structurées ou contenues dans un document non structuré. Le référentiel de conservation élaboré par le responsable archivage permet d’alimenter la cartographie des données personnelles

* L’archivage managérial a la responsabilité : (surtout si il a en charge un service d’archives)
	+ d’élaborer les règles de gestion des documents et des données = politique d’archivage
	+ du processus d’élimination

y compris des données personnelles

* L’archivage managérial peut donner au DPO ou l’aider à élaborer les règles de gestion des données personnelles et peut aussi lui apporter des solutions tant organisationnelles (politique et procédures d’archivage) que techniques (le système d’archivage ou les outils documentaires peuvent peut-être être utilisés pour conserver les données personnelles)
* Complémentarité des missions : le DPO exprime des besoins / la politique d’archivage prescrit des solutions :

|  |  |
| --- | --- |
| **Responsabilités du DPO** | **Responsabilités de l’archivage managérial** |
| S’assurer que seules les données personnelles nécessaires sont collectées  | Identifier les documents et données à conserver dans le cadre des activités de l’entreprise |
| S’assurer qu’elles sont conservées le juste temps nécessaire | Elaborer le référentiel de conservation  |
| Garantir leur protection | identifier les espaces de conservation adaptés, assurer la gestion des droits et la traçabilité des accès |
| Garantir leur destruction | Gérer la destruction à échéance ou à la demande |
| Répondre aux demandes de droits d’accès des personnes concernées par la collecte de leurs données | Assurer l’accès à l’info à toute personne qui en a besoin et qui est habilitée |
| Travailler avec l’IT, le juridique, la fonction archivage si elle existe et les métiers | Travailler avec l’IT, le juridique, le DPO quand nécessaire et les métiers |
| Organiser la mise en conformité de l’organisation avec les lois et règlements | Organiser la mise en conformité de l’organisation avec les lois et règlements |

# IT, systèmes informatiques et données personnelles

La question des cartographies est abordée *supra*

L’IT est un partenaire indispensable par sa maîtrise technique (question du cloud…) des lieux de stockage, de l’administration des outils (question de l’administration « follow the sun » en Europe, Inde et US de bases de données contenant des données personnelles) et des copies (question de l’élimination ciblée dans les sauvegardes…)

Les rapports avec les DSI ne sont pas simples. Dans l’absolu, la DSI devrait avoir pour la gestion des Données personnelles, un rôle de support des politiques et pratiques décidées par le DPO et le référentiel de conservation, mais cela ne correspond pas à l’existant : les opérationnelles métiers attendent trop de la DSI, et lui délèguent (abandonnent) des décisions de politique, notamment la décision de conservation et de destruction.

La question des données personnelle remet donc au cœur du débat la clarification des limites de responsabilité de l’IT : prestataire, partenaire ou décisionnaire souverain ?

La notion de *Privacy by design* a de profonds impacts sur les architectures IT retenues (les sauvegardes, le chiffrage ou la séparation de certaines données personnelles dans des espaces cloisonnés) qui ne doivent pas être sous-estimés en coûts et en temps : la vision doit être partagée avec l’IT, mais aussi la feuille de route pour tendre par itérations progressives vers la maîtrise cible –qui risque de ne pas être atteinte à court terme…

# Sponsoring et communication

Le niveau de risques et l’atteinte potentielle à l’image de l’organisme font de la gestion des données personnelles un sujet majeur dans tout organisme, même pour la Fonction publique.

Le niveau du sponsor doit être en rapport, d’autant que l’ensemble des collaborateurs/agents doit être sensibilisé à la question : digest de sensibilisation, formations pour les « manipulateurs » de PII, communication interne

* Le positionnement dans l’organigramme est un « Elément moteur »
* Le sponsor est essentiel

Arguments : en complémentarité des risques, le lien avec l’éthique et la bonne renommée de l’entreprise dans ses relations avec ses clients est un argument positif fort

* Contrôles, Audits seront réels en 2018 pour les grands groupes et les administrations, ainsi que le testing par des associations de consommateurs
* Les exigences s’accroissent mais aussi la conscience des personnels

=> Levier d’action mais aussi risque de lanceurs d’alerte en cas de pratiques dissimulées

Le stock d’information non maîtrisé est un risque : le sponsor doit en être conscient et prendre une décision de prise de risque ou d’attribution des moyens de liquidation du risque.

# Les réseaux de relais

* Complémentarité au niveau des réseaux de correspondants respectifs DPO / Archives car grande opportunité de synergie (ce point de vue n’est pas partagé par toutes les entreprises : pour certains, le records manager s’appuie sur le réseau des correspondants qualité tandis que le DPO s’adresse aux maîtrises d’ouvrage SI).
* Les juristes peuvent faire remonter des besoins spécifiques, de la veille ou des cas d’exemple, mais portent rarement les déploiements d’outils et de procédures.
* Complémentarité à voir avec les relais IT ou Qualité avec des synergies en terme de management de l’information. Par contre, Le DPO ne s’adresse pas uniquement aux maîtrises d’ouvrage SI car de nombreuses entreprises ont encore du papier : de nombreux consentements clients par exemples. Dans de nombreux cas la dématérialisation du métier pour aboutir à une « Entreprise en ligne » va apporter une réponse, mais souvent l’IT ne peut rien faire pour le DPO car il y a obligation de les conserver papier ou c’est la procédure jugée la plus efficace pour le moyen terme encore.

# Les utilisateurs (internes ou clients externes)

Le GDPR renforce les exigences de consentement éclairé de la personne dont les données personnelles sont utilisées. Elle doit consentir explicitement (souvent double consentement sur Internet) en ayant compris ce qu’elle octroie (question de langue et de clarté de langage, donc d’amélioration des modèles).

Outre le contenu juridique des clauses, il y a un travail à faire sur le graphisme et la concision des explications qui va nécessiter souvent un appel à des graphistes, ou du moins à des compétences non-juridiques.

Le Droit à l’oubli/Suppression des données personnelles est affirmé très fortement, mais il n’est pas forcément opposable systématiquement aux obligations de conservation/Archivage (ex. l’entreprise a besoin de garder des données fiscales sur 3 exercices, et doit donc conserver les preuves durant cette durée).

Il faut par contre maîtriser au plus tôt l’information pour ne pas avoir à détruire de l’information sensible « générale » lorsqu’un individu demande l’application du droit à l’oubli : par ex. un rapport « anonymisé » sur une problématique et des annexes contenant les noms du panel examiné, les photos et habitudes de vies, données biométriques…

=> Trouver des Quick Wins pour les utilisateurs et les responsables de traitement, sans cacher le chemin à parcourir.

# Liens utiles :

* RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016 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)

<http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679&from=FR>

* CNIL – Règlement européen sur la protection des données personnelles : se préparer en 6 étapes

<https://www.cnil.fr/fr/principes-cles/reglement-europeen-se-preparer-en-6-etapes>

* Guidelines on Data Protection Officers (« DPOs”) – 16/EN WP 243 rev.01

<http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083>

* Le CIL et le futur délégué à la protection des données /
	+ [Guide pratique de la prise de fonction du CIL](https://www.cnil.fr/sites/default/files/typo/document/Guide_pratique_Prise_de_fonction_CIL.pdf)
	+ Guide du Correspondant Informatique et Libertés (CIL)
	+ [Délégué à la protection des données (EN)](https://www.cnil.fr/sites/default/files/atoms/files/guidelines_on_dpos_5_april_2017.pdf)

<https://www.cnil.fr/fr/le-cil-et-le-futur-delegue-la-protection-des-donnees>

* CNIL - Les principes clés de la protection des données personnelles

<https://www.cnil.fr/fr/comprendre-vos-obligations/les-principes-cles>

* Pierre Rimbert - Se réapproprier une ressource d’utilité publique - Données personnelles, une affaire politique – Septembre 2016

<http://www.monde-diplomatique.fr/2016/09/RIMBERT/56226>