APDL

Association pour la Protection des Données au Luxembourg

ORIENTATIONS SUR LA CONSERVATION ET LA DESTRUCTION DES DONNEES DANS LE CADRE DU REGLEMENT GENERAL SUR LA PROTECTION DES DONNEES

Version 1.0 du 2 avril 2021

Document élaboré par la Commission Technique :

- Bénédicte d'Allard (ARENDT ARC)
- Sylvie Dessolin (Sopra Steria PSF Luxembourg)
- Guy Isler (CCSS)
- Marie-Emilie Mengal (Juriste spécialisée en TIC et protection des données)
- Miguel Martins (Talkwalker)
- Romain Sabel (BDO Services Luxembourg)
- Philippe Simon (RBC Investor Services)
- Pierre Van Wambeke (Seezam S.A.)

Et relu par les membres de la Commission technique, ainsi que Mme Nathalie Sprauer, Banque Raiffeisen et Maître Cyril Pierre-Beausse, Cabinet /c law

Sommaire

Conservation et destruction des données dans le cadre du RGPD

Après sa publication de 2018 sur les mesures de sécurité (article 32) du Règlement Général sur la Protection des Données 2016/679 (ci-après « RGPD »), la Commission technique a décidé en octobre 2018, selon l'avis de ses membres, de lancer un travail sur la gestion de la rétention et de l'effacement des données (incluant le traitement des données historiques ou d'archives papier, cas rencontrés par beaucoup d'entre nous).

En effet, si plusieurs articles du RGPD posent les principes applicables en matière de conservation de données personnelles, peu d'organismes sont capables de les mettre en œuvre concrètement dans les systèmes à ce jour.

Après un rappel de ces obligations en matière de conservation et de destruction des données, nous allons nous pencher sur la méthodologie. Nous analyserons ensuite comment gérer le cycle de vie des données en tenant compte aussi de leur forme de conservation.

1. Rappel des exigences du RGPD en termes de rétention et destruction

Le RGPD contient plusieurs dispositions ayant trait aux notions de conservation des données à caractère personnel. Selon ces dispositions, le responsable du traitement ne doit pas conserver pour une durée illimitée les données à caractère personnel qu'il recueille et traite dans le cadre de son activité. Cet aspect a souvent été oublié par les responsables du traitement, qui se sont d'abord concentrés sur les urgences opérationnelles, comme les obligations d'identifier les traitements, d'informer et d'assurer l'intégrité, la sécurité et la continuité des traitements de données.

L'article 4, 3° RGPD définit d'emblée la notion de « limitation du traitement » comme étant « le **marquage de données à caractère personnel** conservées, **en vue de limiter leur traitement futur** ». Cette première définition consacre le principe d'une durée de conservation des données à caractère personnel limitée dans le temps associé à la nécessité pour le responsable du traitement de prévoir une matérialisation des critères de conservation associée aux données.

Pour comprendre ces critères, il faut analyser les principes de légitimité du traitement des données à caractère personnel repris à l'article 5, alinéa 1, b) qui dispose que « Les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes, **et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités** ». Cet article ajoute toutefois que le traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques n'est pas considéré comme incompatible avec les finalités initiales.

L'article 5.1.c précise que les « **données doivent être adéquates, pertinentes et limitées** ». Avant de parler de rétention, il faut s'assurer de ne pas collecter plus de données que nécessaire pour la finalité du traitement. En réduisant les données traitées à leur minimum nécessaire, on réduit en même temps l'effort pour les protéger, les conserver et les effacer au bon moment.

Par ailleurs l'article 5, alinéa 1, e) dispose que, dans tous les autres cas, les **données** doivent être « **conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités** pour lesquelles elles sont traitées ». A nouveau, le législateur précise que, dans certains cas, les données à caractère personnel peuvent être conservées pour des durées plus longues, pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises par cet article (limitation de la conservation).

L'article sur l'information obligatoire des personnes concernées (article 13) prévoit aussi en son alinéa 2a que l'on communique aux personnes concernées « la durée de conservation des données à caractère personnel ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée.

Enfin, l'article 18 du RGPD précise que la « personne concernée a le droit d'obtenir du responsable du traitement la limitation du traitement » dans certains cas spécifiques énumérés de a) à d).

N'oublions pas en outre l'article 17 qui donne aux personnes concernées un droit à l'oubli difficile à respecter si, lors de la conception du traitement et de la méthode de conservation des données, cet aspect n'a pas été pris en compte. L'effacement sélectif pour une personne concernée peut être un défi technique si les archives ne sont pas organisées correctement. Le droit à l'oubli n'étant pas absolu, il faut statuer sur les demandes au cas par cas.

Comme l'article 25 impose la protection des données dès la conception et par défaut, il est évident que la question de l'effacement possible doit être traitée dès la mise en place du traitement afin de respecter les droits de la personne concernée.

En résumé, le responsable du traitement est autorisé à conserver les données personnelles tant que les finalités du traitement sont d'actualité.

Les finalités du traitement et, dans la mesure du possible, les délais prévus pour l'effacement des différentes catégories de données, doivent être repris dans le registre des activités de traitement tenu par le responsable du traitement conformément à l'article 30 du RGPD. Cela paraît évident compte tenu du fait que ces deux notions sont étroitement liées. N'oublions pas non plus que la conservation des données est un traitement en soi, qui doit donc avoir une base légale.

Pas de traitement de données à caractère personnel sans finalités et, dès lors, **pas de conservation de ces données sans subsistance de ces finalités déterminées, explicites et légitimes.**

Le RGPD prévoit également des hypothèses spécifiques.

La première a trait à la conservation des données à caractère personnel traitées par le responsable du traitement pour assurer l'exécution de ses missions (publiques pour les acteurs publics, commerciales, contractuelles mais aussi de leurs obligations légales pour les acteurs privés) dans le cadre de finalités déterminées, explicites et légitimes pour une durée limitée correspondant à la durée de subsistance de cette finalité.

La seconde a trait à la conservation des données à caractère personnel traitées par le responsable du traitement, dans le cadre de ses missions de recherches (scientifique, historique ou statistique) ou dans le cadre de ses obligations légales découlant de la règlementation en matière d'archivage dans l'intérêt public, pour une durée limitée correspondant à la durée de subsistance de ces finalités particulières. Ce cas se rencontre principalement dans le secteur public (administrations, services d'archives publics, …).

D'autres hypothèses sont à considérer dans le contexte de la rétention des données à caractère personnel, notamment celle de la sous-traitance. Ainsi l'article 28.g du RGPD prévoit que « selon le choix du responsable du traitement, le sous-traitant supprime toutes les données à caractère personnel ou les renvoie au responsable du traitement au terme de la prestation de services relatifs au traitement, et détruit les copies existantes, à moins que le droit de l'Union ou le droit de l'Etat membre n'exige la conservation des données à caractère personnel ». Il en résulte que le sous-traitant doit lui aussi organiser les données retenues pour le compte d'un responsable du traitement, de telle sorte qu'il soit capable de les extraire ou de les détruire. Rappelons dans ce contexte que le sous-traitant doit également aider le responsable du traitement à être conforme au RGPD, et qu'il doit donc aussi veiller aux méthodes de rétention choisies, afin de pouvoir assister le cas échéant le responsable du traitement à répondre aux différentes demandes de personnes concernées.

Finalement, de plus en plus de lois récentes définissent des durées légales de conservation de données à caractère personnel. C'est notamment le cas de la loi du 23 juillet 2016 sur la réorganisation du casier judiciaire.

Après un rappel des obligations, nous allons nous pencher sur la méthodologie. Nous analyserons ensuite comment gérer le cycle de vie des données en tenant compte aussi de leur forme de conservation.

2. « Par où commencer ?» - une méthodologie : l'apport du Records Management

Face à toutes ces obligations, par où commencer ? Par chance, les responsables de la protection des données vont recevoir l'aide des « *Records Managers* » et bénéficier de l'apport de cet autre domaine de la gestion de l'information (le « *Records Management* », qui consiste à gérer les données et documents dans une optique de valeur probante et d'efficience).

En effet, il existe un ensemble de bonnes pratiques pour le « *Records Management* », codifiées par une série de normes ISO[1], qui aident à définir les durées de rétention et à gérer conservation et effacement des données, quel que soit leur support.

2.1. Analyser les processus

L'analyse des processus pour le *Records Management*, consiste à identifier les exigences légales, réglementaires, contractuelles, commerciales et opérationnelles applicables concernant la conservation des données. Autrement dit, les obligations légales et les besoins métiers de conservation. Ceux-ci sont extraits des différents règlements applicables et des règles internes.

Cette méthode va donc permettre de :

- compléter le registre des traitements qui doit indiquer les délais prévus (art. 13.2.a du RGPD) dans la mesure du possible pour l'effacement des différentes catégories de données (art. 30.f du RGPD) et les différents documents de *compliance* (notice d'information des personnes concernées, etc.), et
- de mettre en œuvre les rétentions et destructions nécessaires[2].

Cette analyse, comme celle conduite pour identifier les traitements de données à caractère personnel et les recenser dans le registre, va être menée via une approche par « processus métier ». L'avantage de cette approche est qu'elle recoupe celles généralement utilisées notamment en matière de management de la qualité (ISO 9000) ou de sécurité de l'information (ISO 27000). L'analyse et la modélisation des processus métiers sont ainsi largement pratiquées et beaucoup d'organismes de différents secteurs et de toutes tailles disposent généralement déjà d'une base documentaire les décrivant.

Cela permet au DPO et aux équipes qui accompagnent la conformité au RGPD de prendre rapidement connaissance des activités de l'organisme, de conduire de manière rapide et exhaustive l'identification des traitements (puisque l'on peut passer en revue tous les processus, et pour chacun questionner l'existence de traitements de Données Personnelles), et de construire le registre de traitements RGPD.

2.2. Identifier les obligations et les durées de rétention

En même temps que l'on identifie les traitements et les données en jeu et que l'on établit la licéité du traitement, on va rechercher **les textes légaux (ou réglementaires) applicables**, ainsi que **la durée de rétention** qui peut être

[1] Les normes ISO sur le *Records Management*, issues des meilleures pratiques des pays anglo-saxons, mais aussi d'une longue tradition des administrations européennes, ont été élaborées à partir de 1998 par une Commission ISO à laquelle le Luxembourg participe, via un Comité ILNAS, TC46SC11, Archives et *Records Management*. Voir :
https://www.archimag.com/archives-patrimoine/2017/06/01/records-management-comment-construire-politique-gouvernance
https://www.iso.org/fr/committee/48856/x/catalogue/p/1/u/0/w/0/d/0

[2] Cette analyse des exigences va également permettre de justifier la conservation des données (qui en elle-même constitue un traitement)

explicite dans le texte : l'**obligation de conserver une information pendant un certain nombre d'années**, ou au contraire **l'obligation de détruire** après une certaine durée (casier judiciaire par exemple), ainsi que le « *trigger* » (la borne, ou littéralement l'« événement déclencheur » à partir duquel court la durée de rétention).

Par exemple, la loi du 12 novembre 2004 relative à la lutte contre le blanchiment et contre le financement du terrorisme comporte dans son article 3 (« Obligations de vigilance à l'égard de la clientèle ») un ensemble de dispositions relatives à la conservation et à la protection des données précisant les durées de rétention et l'obligation d'effacement[3].

Extraits :
« (6) « Les professionnels sont ***tenus de conserver les documents, données et informations*** *ci-après aux fins de prévention et de détection d'un éventuel blanchiment ou d'un éventuel financement du terrorisme et des enquêtes en la matière menées par les autorités luxembourgeoises responsables de la lutte contre le blanchiment et contre le financement du terrorisme :*
a) en ce qui concerne les mesures de vigilance à l'égard du client, une copie ou les références des documents, des données et informations qui sont nécessaires pour se conformer aux obligations de vigilance à l'égard de la clientèle prévues aux articles 3 à 3-3, « y compris, le cas échéant, les données obtenues par l'utilisation de moyens d'identification électronique, des services de confiance pertinents prévus par le règlement (UE) nº 910/2014, ou tout autre processus d'identification sécurisé, électronique ou à distance, réglementé, reconnu, approuvé ou accepté par les autorités nationales compétentes, les livres de comptes, la correspondance commerciale, ainsi que les résultats de toute analyse réalisée, » ***pendant cinq ans après la fin de la relation d'affaires avec le client ou après la date de la transaction conclue à titre occasionnel*** *;*
b) les pièces justificatives et enregistrements de transactions qui sont nécessaires pour identifier ou reconstituer des transactions « individuelles afin de fournir, si nécessaire, des preuves dans le cadre d'une enquête ou instruction pénale », ***pendant cinq ans après la fin de la relation d'affaires avec le client ou après la date de la transaction conclue à titre occasionnel.*** *(Loi du 25 mars 2020)*
(…)
Les professionnels sont également tenus de conserver les informations relatives aux mesures qui ont été prises afin d'identifier les bénéficiaires effectifs au sens de l'article 1er, paragraphe (7), point a), sous-points i) et ii).
Sans préjudice des délais de conservation plus longs prescrits par d'autres lois, les professionnels sont tenus d'effacer les données à caractère personnel à l'issue des périodes de conservation visées à l'alinéa 1er.
Les autorités de contrôle peuvent exiger, dans des affaires spécifiques, lorsque cela est nécessaire à l'accomplissement de leurs missions au titre de la présente loi, qu'un professionnel conserve les données pendant ***une période supplémentaire qui ne peut excéder cinq ans****.*
Par dérogation à « l'alinéa 4 », les professionnels « conservent » les données à caractère personnel pendant une période supplémentaire de cinq ans lorsque cette conservation est nécessaire pour la mise en œuvre efficace des mesures internes de prévention ou de détection des actes de blanchiment de capitaux ou de financement du terrorisme. » (Loi du 13 février 2018) «

Parfois il faut aussi tenir compte de la durée d'un éventuel procès en cas de litige ou de contestation (« *litigation hold* » qui s'ajoute à la durée légale, car on ne va pas pouvoir détruire les preuves pendant toute la durée du contentieux). Il convient de suspendre le délai en cas de contentieux jusqu'à ce que la décision ne soit plus susceptible de recours et dite « de force de chose jugée ».

Si l'on n'a pas de texte applicable, on va considérer la guidance des administrations, des associations professionnelles, les normes métiers, les référentiels de certification (systèmes de management de la qualité ou de sécurité des systèmes d'information, qui tous exigent d'identifier les « *assets* informationnels à gérer » - données et documents - et de fixer les durées et modalités de rétention). Enfin, il y a les besoins du métier, par exemple les besoins contractuels, qui doivent bien sûr prendre en compte les exigences du RGPD : uniquement la durée nécessaire au traitement.

[3] https://www.cssf.lu/wp-content/uploads/L_121104_blanchiment_upd250320.pdf

Les Archives Nationales de Luxembourg et la CNIL publient également des référentiels applicables à différents secteurs (cf. exemples en annexe 3)

2.3. Formaliser les durées dans le registre et dans les procédures

Les obligations et durées de rétention ainsi identifiées sont reportées, pour les besoins du RGPD, dans le registre (cf. annexe 1). Il peut être utile d'indiquer le texte légal applicable, la durée de rétention ainsi que son point de départ (le « *trigger* »). Les organismes les plus avancés en matière de protection des données pourront en faire part aux personnes concernées, comme requis par le règlement, en même temps qu'ils informeront ceux-ci sur les traitements. Une procédure de rétention spécifique, accompagnée d'un tableau en annexe (*cf*. exemple en annexe 2) ou d'une base de données devrait être mise en place, surtout s'il y a un grand nombre de type de données et d'exigences quant à leur conservation.

NB : le *Records Management* ne se limite pas aux données personnelles, mais concerne, comme on l'a vu, l'ensemble des « *assets* informationnels ». Dans le cadre du déploiement par l'organisme d'une démarche plus globale de maîtrise ou de gouvernance de l'information, il sera donc possible d'élaborer une procédure et un référentiel général de conservation portant sur l'ensemble des activités, processus et traitements, et donc l'ensemble des données et documents.

Il est essentiel de rappeler qu'il revient à chaque organisme de vérifier, en fonction de la nature de son activité, de son statut juridique et des règles qui lui sont applicables, quelles données doivent être conservées, pendant quelle durée et dans quelles conditions. L'organisation doit effectuer une « *due diligence* » et maintenir une veille sur les dispositions légales qui lui sont applicables, et ne pas utiliser (sans une relecture attentive et les vérifications qui s'imposent) les listes de rétention toutes faites qui sont parfois circulées ou disponibles sur internet.

2.4. Gérer le cycle de vie: mettre en œuvre et gérer la rétention et la destruction dans le temps

De la même manière quand les traitements sont identifiés, on va s'intéresser aux systèmes où les données sont utilisées, stockées, et il faut mettre en place les mesures de sécurité telles que le chiffrement, la gestion des accès[4]. **Il s'agit, une fois les durées de rétention définies, de les mettre en œuvre dans les systèmes**.

Il arrive que la durée du traitement soit assez longue en soi (par exemple, pour le patient d'un établissement de santé, le client d'une société d'assurance ou d'une banque, elle peut aller de 10 à 30 ans, voire au-delà selon les cas) et que s'y ajoute une durée de conservation légale, par exemple de 10 ans après la fin de la relation avec un client (c'est ce que l'on appelle « l'archivage intermédiaire » notamment dans le secteur public). Il est dès lors nécessaire de **gérer la durée de rétention durant tout le cycle de vie et de protéger les données à toutes les étapes, quel que soit le support**.

Ainsi, on va souvent conserver en base active les données les plus récentes ou les plus utilisées, et placer celles moins couramment mises en jeu dans des systèmes de stockage intermédiaire. De même, les dossiers papiers les plus récents sont conservés à portée de main, tandis que les plus anciens sont souvent placés dans des locaux de stockage, ou confiés à un prestataire de service de dématérialisation et/ou de conservation. En effet, la conservation numérique ou papier peut être confiée à des sous-traitants spécialisés, dont certains peuvent être certifiés « PSDC », prestataire de service de dématérialisation et/ou conservation[5].

[4] Voir notre publication de 2018 REGLEMENT GENERAL SUR LA PROTECTION DES DONNEES – RGPD-ORIENTATIONS SUR L'IMPLEMENTATION DE L'ARTICLE 32 DU RGPD (« Sécurité du Traitement »)
[5] https://portail-qualite.public.lu/fr/confiance-numerique/archivage-electronique.html

Il arrive également que l'information change de support : un document papier peut être numérisé au cours du processus. Pour chaque système servant à traiter les données, il faudra mettre en œuvre les mesures de protection et de sauvegarde appropriées. A l'issue de la période de rétention, les données doivent être détruites ou, dans certains cas prévus pour le secteur public, conservées comme archives définitives.

Il pourra être utile de rédiger des procédures annexes à la politique de rétention précisant la mise en œuvre des règles dans les différents systèmes.

Tous ces aspects concrets seront développés dans la section suivante, en s'attachant à décrire les bonnes pratiques de gestion, selon les différents systèmes et étapes du cycle de vie, et selon les supports.

3. Gérer les données et documents tout au long du cycle de vie

Bien gérer la durée de rétention des données à caractère personnel, c'est les protéger tout au long de leur cycle de vie, de la collecte à la destruction.

Où se trouvent les données personnelles ? Elles sont souvent dispersées à travers l'ensemble des données de l'organisme, qui elles-mêmes sont stockées et dupliquées sur des supports différents, dans des environnements multiples. Nous apporterons d'abord quelques éléments d'information sur le stockage des informations (leur organisation, leur support, les différents environnements d'utilisation), avant d'aborder leur destruction et leur conservation.

Les données peuvent prendre des formes variées, qui influenceront également leur gestion. Nous avons choisi de distinguer entre les données nativement numériques et les données papier.

3.1. Les données nativement numériques

Avec la numérisation, la plupart des données sont aujourd'hui numériques dès leur création. Les données numériques constituent ainsi la majorité des données personnelles à traiter, aussi leur bonne gestion est-elle particulièrement importante. Leur forme facilite un traitement de masse partiellement ou totalement automatisé.

Pour gérer les changements de statut des données ou documents numériques, il faut créer dans les systèmes, si elle n'existe pas, la notion de déclencheur (*trigger*) et gérer les données en bases selon leur durée de rétention prévue. Il conviendrait de déployer un algorithme qui, à la date échue, fait basculer les données dans un système hors production, puis à terme applique les règles de destruction.

Malheureusement, il n'existe la plupart du temps ni un tel déclencheur, ni de durée de rétention programmée dans les systèmes actuellement en production ou ceux disponibles sur le marché. Dans certains cas, lorsque ces variables existent, elles ne peuvent être utilisées en pratique, pour des raisons techniques ou autres. Que faire alors avec les stocks de données anciennes ?

Rechercher une solution 100 % conforme est peu réaliste. Néanmoins un certain nombre de mesures peuvent être prises :

- Créer les déclencheurs au plus vite pour l'avenir dans les systèmes actuels, y compris dans les environnements non structurés (messageries, documents bureautiques...)
- Pour l'arriéré, effectuer si possible une revue individuelle des enregistrements ou au moins d'un échantillon pour voir si en majorité les données/documents sont encore nécessaires

- Déterminer le sort et la durée à appliquer en fonction de cette revue ou de cet échantillonnage : conserver jusqu'en xxxx et veiller à la destruction à terme ; ou détruire (éventuellement après extraction de certaines données encore à conserver).

Examinons plus en détail la gestion, l'archivage et la destruction des documents numériques.

3.1.1. La gestion des données numériques

Les données sont « rangées » dans des **fichiers** ou des **bases de données** s'appuyant sur plusieurs fichiers. L'utilisation d'index simplifie et accélère les opérations de recherche, de tri ou d'agrégation. Les **index** sont constitués à partir d'une copie des données à accéder. Par exemple, le nom des personnes se trouve dans une table ou un fichier et l'on facilite et accélère leur recherche en construisant un index. Cet index contiendra alors lui aussi les noms des personnes. La même donnée se retrouve donc à plusieurs endroits.

De nombreuses données existent cependant sous une forme non structurée : messagerie, GED, fichiers contenant des notices ou textes non structurés, enregistrements vidéo ou téléphone, etc. Parfois nous disposons de métadonnées permettant de classifier néanmoins ces informations.

*Une **métadonnée** est une information à propos d'une donnée. A titre d'exemple, on peut citer la date et l'heure à laquelle la donnée a été produite, le nom de la personne qui l'a enregistrée, ou encore les coordonnées GPS de l'endroit où une photo a été prise. Les métadonnées sont indispensables pour, selon les cas, authentifier, gérer, classer et retrouver les informations et les documents. Certaines métadonnées peuvent servir à calculer une date de rétention ou servir de déclencheur pour une action de destruction ou d'archivage. Attention : la métadonnée peut en elle-même constituer une donnée personnelle (par exemple, en identifiant l'auteur ou le sujet de la donnée concernée).*

Les données sont localisées sur des **supports qui peuvent être divers**. Ces supports influencent les techniques de conservation et de destruction à appliquer.

- Le **disque dur** est le support de données électronique par excellence. Tous les ordinateurs actuels utilisent un disque dur pour stocker les données. Il en existe deux grandes familles:
  - le disque dur à plateaux magnétiques : les informations sont stockées sur un ou plusieurs plateaux (verre ou alliage d'aluminium) recouvert d'une couche métallique.
  - le disque dur SSD : les informations sont stockées dans des puces électroniques composées de transistors. Ils sont bien plus rapides que les disques à plateau, et aucune pièce n'est en mouvement. La technologie évolue rapidement sur ce type de support, mais sa durée de vie est toutefois moindre que celle du disque à plateaux magnétiques car chaque cellule ne peut être écrite qu'un nombre limité de fois.

  Il existe des disques durs magnétiques hybrides, dotés des 2 technologies. Ce sont des disques à plateaux magnétiques traditionnels auxquels des puces de mémoire SSD ont été ajoutées, le but est d'accélérer les accès au disque à plateaux magnétiques en se servant de la SSD comme cache.

  Le disque dur peut être local, placé directement dans le boîtier de l'ordinateur ou du serveur, ou dans une baie dédiée contenant plusieurs disques et relié à l'ordinateur ou au serveur (SAN Storage Area Network ou NAS Network Attached storage).

  Il peut aussi être externe et transportable, relié à l'ordinateur lorsque l'utilisateur l'y connecte. Il peut être distant, situé à l'extérieur des locaux, relié par un réseau.

  Les disques durs n'étant pas à l'abri de problème, les données sont souvent copiées sur plusieurs disques en même temps afin d'assurer une redondance des données et faciliter leur récupération : en cas de

problème survenant sur l'un des disques, on pourra toujours utiliser les données stockées sur les autres disques (système RAID).

- Les **bandes ou cassettes magnétiques** sont encore utilisées de nos jours car elles permettent d'enregistrer une très grande quantité de données pour un coût faible. C'est un support magnétique effaçable et réutilisable. C'est un support lent qui est réservé aux copies de sauvegardes et aux archives. Il est courant d'organiser les sauvegardes sur plusieurs périodes : journalière, hebdomadaire, mensuelle… La même donnée se retrouvera donc sauvegardée plusieurs fois et sur plusieurs bandes. Contrairement au disque dur, on ne travaille pas directement avec les données d'un support magnétique. On doit d'abord enregistrer les données du support magnétique sur un disque dur pour pouvoir les traiter. Des robots (juke-box) permettent d'éviter les manipulations manuelles des supports magnétiques. Il faut les relire de temps en temps afin de les re-magnétiser et s'assurer que l'information reste disponible en cas de besoin.

- Les **CD-ROM et DVD-ROM** sont utilisés lorsque les données doivent être conservées sans pouvoir être effacées ou modifiées. Les supports en plastique ont une durée de vie limitée à quelques années seulement alors que les supports non réinscriptibles en verre sont garantis 100 ans.

- Les **clés mémoire de type USB** sont constituées de puces composées de transistors et fonctionnent comme les disques SSD, avec cependant moins de sécurité (et donc de résistance dans le temps). En dépit de cette faiblesse, leur facilité d'utilisation explique la généralisation de leur usage. Toutefois, il ne faut pas oublier qu'il s'agit d'un support amovible, transportable très facilement, et donc exposé. En cas d'utilisation il faut donc prévoir au départ sa sécurisation (par exemple son chiffrement) en cas de vol ou de perte.

- Les **microfiches ou microfilms** sont des supports anciens qui peuvent encore être rencontrés. L'information est contenue sur un support plastique photographique, elle est réduite d'un facteur 24 par rapport à l'original. Une seule microfiche au format A6 (environ 10 cm x 15 cm) contient entre 100 et 130 pages. Les microfilms noir et blanc se conservent plus facilement et plus longtemps (100 ans) que les microfilms couleurs qui doivent se conserver au noir et au froid. Ce support s'apparente et se gère à la façon des archives papiers.

- Les **supports obsolètes** tels que les **disquettes souples** au format 3 pouces et demi, ou 5 pouces et quart, ou 11 pouces souffrent des problèmes évoqués pour les supports magnétiques (bandes ou disque dur). Les cartes perforées en papier cartonné sont citées pour mémoire, avec une moindre chance d'être rencontrés.

Quels qu'ils soient, les supports doivent être stockés de façon à être protégés du feu, des inondations, de l'humidité, des vols, et ne doivent être accessibles qu'à des personnes autorisées. Pour éviter les conséquences d'un problème grave survenant dans le bâtiment principal, des copies devraient se trouver dans un autre bâtiment situé à distance et protégé de la même façon. Pour éviter les fuites de données les supports devraient tous être chiffrés.

Un organisme utilise **plusieurs environnements de travail**, chacun contenant des données particulières et ayant un but spécifique.

- L'**environnement de production** ou **base active** contient les données traitées ainsi que les programmes de traitement. C'est l'environnement de travail principal utilisé par les employés pour effectuer les différents traitements.

- L'**environnement d'acceptation** (aussi appelé pré-production ou test) est constitué d'une copie de l'environnement de production, des programmes et des données. Il est utilisé pour tester et valider que les nouveaux programmes, les mises à jour et toute modification effectuée sur un programme fonctionne

correctement avant son utilisation dans l'environnement de production. Un programme nouveau ou modifié qui perturbe le fonctionnement du système ou qui ne fonctionne pas comme prévu ne sera pas transféré dans l'environnement de production qui reste ainsi préservé et opérationnel. Cet environnement d'acceptation contient souvent une copie des données de production. Si les données copiées ne sont pas anonymisées[6], il faut appliquer les mêmes règles strictes de limitation d'accès que pour l'environnement de production.

- L'**environnement de développement et de test** est utilisé pour développer/modifier les programmes. En général il contient un jeu réduit de données, souvent créé sur mesure pour réaliser des tests réduits. Il ne devrait donc pas contenir de données personnelles.

- D'**autres environnements** peuvent s'ajouter : environnement dédié à la production de rapports, multiples environnements d'acceptation, environnement de formation...

Les différents environnements sont sauvegardés régulièrement. Une sauvegarde (*backup* en anglais) est une copie des données et des programmes de l'environnement et servira à restaurer l'environnement sur un autre matériel en cas de panne de celui habituel, ou à revenir à une version précédente en cas de problème de logiciel ou de matériel.

Une archive est une copie des données qui doivent être conservées dans le temps pour un besoin de consultation dans le futur. Une archive est donc différente d'une sauvegarde, tant dans son contenu que dans son but. Le format des données archivées et leur support doit être pensé : disposera-t-on des logiciels/appareils pour lire ces données plusieurs années après compte tenu de l'évolution rapide des technologies ?

Qu'il s'agisse de données actives sur lesquelles des traitements sont effectués régulièrement ou de données archivées ou sauvegardées, toutes doivent être protégées correctement.

Le premier principe à appliquer est la gestion correcte des accès. Basés sur le principe du moindre privilège, les accès doivent être limités aux seules personnes en ayant vraiment besoin. Si ce principe est souvent mis en place pour les données actives, il est parfois plus difficile à respecter pour les données archivées et sauvegardées. Notamment en cas de restauration de données sauvegardées, il peut arriver que des droits d'accès historiques réapparaissent, qui ne sont plus justifiés et qui ont d'ailleurs été modifiés sur la base active.

Les supports amovibles constituent un autre risque pour la confidentialité des données. En effet, les copies réalisées, parfois à l'insu du responsable du traitement par les employés d'un service, peuvent plus facilement être réutilisées, voire déplacées. Des mesures spécifiques sont donc à mettre en place pour garantir la restriction d'utilisation de ces données et éventuellement une traçabilité de cette utilisation : ces mesures seront particulièrement utiles en cas de violation de données personnelles. Plus facilement volés ou perdus, les supports amovibles nécessitent également une meilleure protection, qu'elle soit physique (enfermés correctement) ou logique (chiffrement des données).

3.1.2. L'archivage des données numériques

Le cycle de conservation des données à caractère personnel peut être divisé en trois phases successives distinctes:

1. La base active,
2. L'archivage intermédiaire,
3. L'archivage définitif.

[6] L'anonymisation n'est pas facile à réaliser (voir 3.1.3)

1ère phase : La base active.

C'est la durée d'utilisation courante des données ou autrement dit, la durée nécessaire à la réalisation de la finalité initiale du traitement.

2ème phase : L'archivage intermédiaire

Il peut être justifié que les données personnelles soient conservées en archivage intermédiaire distinctement de la base active, avec accès restreint, dans la mesure où :

- Il existe une obligation légale de conservation de données pendant une durée fixée (*cf*. ci-dessus 2.2 détermination des durées de rétention) ;
- En l'absence d'obligation de conservation, ces données présentent néanmoins un intérêt administratif, notamment en cas de contentieux, justifiant de les conserver le temps des règles de prescription/forclusion applicables, notamment en matière commerciale, civile et fiscale ;
- Enfin, sous réserve de garanties appropriées pour les droits et libertés des personnes concernées, certaines données peuvent être traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques.

Par exemple, une fois une transaction bancaire effectuée, les pièces justificatives et enregistrements de transactions qui sont nécessaires pour identifier ou reconstituer des transactions « individuelles afin de fournir, si nécessaire, des preuves dans le cadre d'une enquête ou instruction pénale », seront conservées pendant cinq ans après la fin de la relation d'affaires avec le client ou après la date de la transaction conclue à titre occasionnel (loi du 25 mars 2020).
*A ce délai on peut ajouter 5 ans supplémentaires pour d'éventuels contrôles de la CSSF (*cf. *ci-dessus, art. 3 paragraphe 6 de la loi du 12 novembre 2004 relative à la lutte contre le blanchiment et le financement du terrorisme).*

3ème phase : l'archivage définitif

Enfin, dans les conditions de la loi du 17 août 2018 sur l'archivage, l'intérêt public peut parfois justifier que certaines données du secteur public ne fassent l'objet d'aucune destruction : c'est l'archivage définitif. Ces archives sont gérées par les services d'archives publics compétents.

a. Un archivage sélectif

Dans le cas d'un archivage intermédiaire, le responsable du fichier doit veiller à ne conserver que les données nécessaires au respect de l'obligation prévue ou lui permettant de faire valoir un droit en justice : un tri doit donc être effectué parmi la totalité des données collectées pour ne garder que les seules données indispensables.

Attention : les données ainsi archivées ne peuvent pas continuer à être utilisées par les services opérationnels dans leur travail quotidien. Ces données ne sont désormais conservées que dans une optique contentieuse et ne sont accessibles que de façon restreinte. Le nombre d'utilisateurs ayant accès doit être limité et cet accès ne doit se faire que pour les cas prévus et selon des règles définies.

b. Un archivage limité dans le temps

Les données archivées ne sont conservées que le temps nécessaire à l'accomplissement de l'objectif poursuivi : elles doivent donc être supprimées lorsque le motif justifiant leur archivage n'a plus raison d'être.

Par exemple, des données archivées pour se prémunir d'une action en justice durant le temps d'une prescription ou d'une forclusion doivent être supprimées lorsque cette action est prescrite ou forclose.

c. Les modalités techniques d'archivage

Pour les archives intermédiaires, le choix du mode d'archivage est laissé à l'appréciation du responsable du fichier. Des données peuvent ainsi être archivées :

- dans une base d'archive spécifique, distincte de la base active, avec des accès restreints aux seules personnes ayant un intérêt à en connaître en raison de leurs fonctions (par exemple, le service du contentieux) ;
- ou dans la base active, à condition de procéder à un isolement des données archivées au moyen d'une séparation logique (gestion des droits d'accès et des habilitations) pour les rendre inaccessibles aux personnes n'ayant plus d'intérêt à les traiter.

Pour les archives définitives (c'est-à-dire les données conservées dans l'intérêt public), il est recommandé de les conserver sur un support physique indépendant, non accessible par les systèmes de production, n'autorisant qu'un accès distinct, ponctuel et précisément motivé auprès d'un service spécifique seul habilité à les consulter (par exemple, la direction des archives lorsqu'elle existe).

d. Un archivage sécurisé

Des mesures techniques et organisationnelles doivent être prévues pour protéger les données archivées (destruction, perte, altération, diffusion ou accès non autorisés). Ces mesures doivent assurer un niveau de sécurité approprié aux risques et à la nature des données.

Lorsque l'archivage est confié à un sous-traitant, le responsable du traitement doit s'assurer que son prestataire présente des garanties suffisantes en matière de sécurité et la confidentialité des données qui lui sont confiées.
Quel que soit le type d'archive, la consultation des données archivées doit être tracée.

Une personne qui exerce son droit d'accès doit obtenir la communication de l'intégralité des données la concernant, qu'elles soient stockées en base active ou archivées.

3.1.3. La destruction des données numériques

a. L'Anonymisation

Une donnée anonymisée est une donnée qui ne permet plus d'identifier la personne concernée. Cette donnée sort donc du périmètre du RGPD. L'anonymisation permet de traiter les données en protégeant les personnes concernées. C'est une opération doit être irréversible et n'est donc pas toujours facile à réaliser. Plusieurs types d'anonymisation existent. Un exemple simple est celui de l'anonymisation par agrégat (aussi appelée méthode de dilution) : l'information est agrégée pour ne plus être reliée à une personne en particulier. Exemple de l'âge que

l'on agrège par tranche : 0-10 ans, 10-20 ans, 20-30 ans… Si on conserve uniquement la tranche d'âge et non plus l'âge réel (ou la date de naissance), on empêche (ou du moins on rend plus difficile) la liaison de cette information avec un individu précis. On répète ce processus avec chaque information personnelle que l'on souhaite conserver.

Les agrégats doivent être choisis avec soin pour, d'une part, conserver des données pertinentes en vue des futures questions que l'on voudra poser et, d'autre part, conserver l'anonymat des personnes. Afin de garantir celui-ci, il doit y avoir un nombre suffisant de personnes par agrégat (p. ex. par tranche d'âge). Du « bruit » peut également être ajouté au contenu (on parle de randomisation), avec l'introduction de données aléatoire dans les champs de données.

Un travail d'analyse est donc nécessaire pour chaque ensemble de données pour éviter toute possibilité de ré-identification des personnes. Une assurance supplémentaire d'une bonne anonymisation est le cumul des différentes techniques citées précédemment. Il est bon de savoir que des techniques de ré-identification comme l'individualisation (retrouver les données d'une personne suite à une mauvaise anonymisation), de corrélation (sur base d'une relation entre personnes), ou d'inférence (retrouver un attribut à partir d'autres attributs) existent et pourraient réduire à néant une anonymisation que l'on pensait adéquate[7].

b. L'effacement courant n'est pas sûr

On ne parle pas ici de déplacer un fichier dans la corbeille, qui n'est pas un véritable effacement, mais simplement le déplacement du fichier d'un répertoire de l'utilisateur vers le répertoire 'corbeille' géré par le système. On aborde ici le fait de vider la corbeille, ou de supprimer un fichier sans le mettre dans la corbeille.

Or, l'effacement d'un fichier dans un ordinateur n'est pas vraiment l'effacement de son contenu.

Sur un disque dur, quel que soit son type (SSD ou vrai disque rotatif), un fichier occupe une certaine place référencée par une adresse. Un index répertorie la liste des fichiers enregistrés et leur adresse. Pour accéder à un fichier, le système lit l'index pour y trouver son adresse, puis se rend à cette adresse et lit son contenu.

Pour « supprimer » un fichier, il suffit de le supprimer de l'index, et d'indiquer que l'adresse du fichier supprimé est à nouveau disponible pour l'enregistrement du prochain nouveau fichier. Pour l'utilisateur et pour le système, le fichier disparaît. Cependant sur le disque les données restent présentes jusqu'à ce qu'elles soient écrasées par un nouveau fichier. Les nouveaux systèmes de gestion de fichiers historisés inclus dans les systèmes d'exploitation (comme « ZFS Copy on write » par exemple) n'effacent pas le fichier mais créent un second fichier et n'écrasent pas le précédent. Ceci génère de multiples copies des mêmes données au sein du disque dur avec par conséquent des risques plus importants de récupérer un fichier. Des outils spécialisés permettent en outre de retrouver les adresses des fichiers effacés et de les réintroduire dans l'index.

Le fonctionnement est identique dans une base de données. Les enregistrements effacés sont simplement marqués comme étant supprimés. Les programmes lisant les données ne « voient » que les enregistrements n'étant pas marqués comme supprimés. Les enregistrements supprimés logiquement restent dans la base de données tant qu'elle ne sera pas réorganisée. Là encore des programmes spécialisés peuvent « dé-marquer » un enregistrement marqué comme effacé pour le restaurer et le rendre lisible à nouveau.

[7] Pour aller plus loin, consulter l'**Avis WP-2016 du G29 sur les techniques d'anonymisation (FR)** (CNIL)

Le problème des supports à enregistrement magnétiques : sur un disque dur classique, l'effet consistant à enregistrer une information s'exerce magnétiquement sur une zone définie du disque. Après un « effacement » de cette donnée il subsiste toutefois en périphérie de cette zone une légère persistance de l'information initiale (due à l'effet de rémanence magnétique). Certains programmes informatiques spécialisés permettent de relire ces informations de périphérie et de retrouver les anciennes données.

Ce problème ne se rencontre pas avec les disques SSD qui ont une autre faiblesse : pour ne pas user prématurément les cellules mémoires qui n'ont qu'un nombre d'écritures possibles défini, le contrôleur de gestion évite de réécrire toujours au même endroit mais répartit les écritures sur l'entièreté du disque. Potentiellement, une information « effacée » n'est donc recouverte par une autre information que longtemps après.

Le reformatage d'un disque ne donne pas un niveau de sécurité plus élevé. En fait, il s'agit d'effacer l'index du système de fichier, et non pas d'initialiser comme à l'origine les pistes et secteurs du disque. Des programmes spécialisés dans la récupération des données permettent là encore de retrouver une partition effacée.

On doit également se souvenir que les imprimantes laser professionnelles contiennent des disques durs enregistrant chaque impression, il conviendra de penser à détruire son disque dur lors du remplacement d'une telle imprimante. Il en est de même pour les photocopieurs professionnels qui possèdent dorénavant presque tous un disque dur interne pour la réimpression ou la numérisation de documents.

c. Effacement sécurisé

A l'inverse, il existe des outils logiciels spécialisés dans la sécurité qui permettent de garantir un effacement sécurisé. Pour effacer un fichier, l'outil lit l'index pour trouver l'adresse du fichier et va effectivement réécrire le disque à l'emplacement du fichier, selon une ou plusieurs des nombreuses méthodes possibles (à choisir par l'utilisateur), ceci une ou plusieurs fois de suite (plusieurs passes), afin que de s'assurer que la lecture de périphérie et la restauration deviennent réellement impossibles. L'index est lui aussi traité pour rendre l'emplacement du fichier disponible, ainsi que les parties cachées du disque.

Un grand nombre de normes gouvernementales ou industrielles existent pour l'effacement sécurisé des données. Pour ne citer que quelques exemples, outre la **certification de l'ANSSI** en France et le GISA en Allemagne :

- British HMG IS5 Enhanced , U.S. DoD 5220.22-M
- U.S. DoE M 205.1-2, U.S. Army AR380-19,
- NAVSO P-5239-26, Canadian RCMP TSSIT OPS-II, German BCI/VSITR
- Russian GOST R 50739-95, Bruce Schneier's 7-passes, Peter Gutmann's 35-passes

Les bandes magnétiques sont sujettes aux mêmes problèmes que ceux mentionnés à propos des disques durs magnétiques. En cas de volonté de réutilisation, les mêmes contraintes d'effacement s'imposent.

d. Destruction physique

Si leur réutilisation n'est pas souhaitée, la destruction physique des supports de données électronique tels que les disques durs, SSD, bandes, clés USB reste le moyen le plus sûr et le plus efficace. Le pilon et le broyeur permettent de détruire physiquement les disques en interdisant tout accès à ces données (à la condition que l'on puisse s'assurer que personne n'accédera à leur contenu avant leur destruction physique). Pour les SSD, il faut s'assurer

qu'à la sortie du broyeur les miettes sont d'une taille plus petite que celle d'une puce mémoire contenant des données. Pour les bandes magnétiques, l'assurance d'un passage sur un appareil de démagnétisation avant le passage au broyeur assure l'effacement. Plusieurs sociétés sont spécialisées dans ce genre de destruction.

La destruction physique est la seule à envisager pour les microfiches ou microfilms. Elle est aussi recommandée pour tout support de stockage arrivant en fin de vie.

e. Pseudonymisation n'est pas destruction !

La pseudonymisation est une technique qui consiste à remplacer un identifiant (ou une donnée à caractère personnel) par un pseudonyme. Il faut rappeler que la pseudonymisation n'est pas une destruction d'information mais une mesure de protection : une donnée pseudonymisée est une donnée personnelle au sens du RGPD (contrairement à une donnée anonymisée). L'identifiant ou la donnée personnelle est stockée à part et protégée. Cette technique permet la ré-identification en cas de besoin particulier, elle est donc réversible.

Exemple : Une pseudonymisation efficace peut être effectuée en générant une clé secrète longue et difficile à mémoriser (une combinaison de caractères aléatoires), puis en appliquant une fonction dite à sens unique sur la partie des données identifiant une personne (par exemple, un algorithme de hachage à clé secrète tel HMAC).

La pseudonymisation comporte des risques à ne pas négliger. Utiliser la même clé d'identification sur des bases de données différentes peut faciliter l'identification de la personne. En effet, en regroupant des données de plusieurs bases pseudonymisées on peut de nouveau disposer de suffisamment de données pour identifier une personne. Il convient de ne pas oublier d'appliquer une sécurité maximale aux données qui restent stockées en clair et qui permettront de retrouver les données initiales. Des algorithmes de *Business Intelligence* peuvent conduire à une ré-identification même sans disposer de la clé.

3.2. Les documents papier

Les principes applicables aux données nativement numériques sont évidemment aussi applicables aux données papier. Bien que l'on parle aujourd'hui beaucoup de numérisation et de digitalisation, le papier n'a pas entièrement disparu, en particulier dans les locaux d'archives ou chez les prestataires de stockage.

3.2.1. La gestion des données papier

Le papier continue à circuler et peut contenir des données personnelles.

Malgré l'évolution de la législation qui reconnait la valeur probante des documents numériques et des signatures électroniques, de nombreux documents papier continuent à circuler dans nos organismes.

En outre, les documents digitaux peuvent, après impression, se re-matérialiser en documents papier.
Il faut également protéger les données à caractère personnel qu'ils contiennent. Or, les documents imprimés ne sont pas toujours utilisés de manière temporaire et détruits.

D'autre part, la digitalisation progresse rapidement. Les documents numérisés évitent en principe les soucis de la gestion des données personnelles sur support papier, pour autant que la destruction de l'original soit gérée correctement.

Il faut donc distinguer le cas de la numérisation avec conservation des documents papier pour des raisons de sécurité juridique, du cas de la transformation du papier en document électronique selon les règles de l'archivage électronique, donnant valeur probante à la copie digitale et permettant alors la destruction de l'original papier.

Si des archives papier subsistent, il faut veiller à protéger correctement les données à caractère personnel qu'elles contiennent.

3.2.2. L'archivage des données papier

Tout comme pour les données électroniques, il existe un cycle de vie pour les documents papier :

- Les documents se trouvent d'abord dans des **dossiers actifs**, conservés à portée de main, afin de pouvoir être consultés rapidement. Dans des organisations plus grandes, il existe souvent plusieurs copies à des endroits différents, l'accès aux documents dans un autre service étant moins facile que pour les données numériques.
- Après un certain temps les documents sont généralement archivés, le plus souvent dans l'établissement, mais dans des locaux différents. Souvent, l'accès à ces locaux d'archivage est plus restrictif que l'accès aux dossiers actifs. Il s'agit des **archives intermédiaires** qui contiennent les documents consultés moins souvent, mais qui peuvent encore être consultés de temps en temps.
- Finalement, les documents sont transmis aux **archives définitives**. Ces archives sont souvent à un endroit géographique différent ou chez un professionnel de l'archivage. Ressortir des documents de ces archives nécessite plus d'effort et reste en général l'exception.

Pour autant que les documents papiers ne soient pas digitalisés, ils sont généralement stockés dans les bureaux où le traitement a lieu. Tout comme pour les données électroniques, l'accès doit être réglementé. Concrètement cela veut dire qu'en fonction de la sensibilité des données, les dossiers doivent être mis sous clés et l'accès doit être limité aux personnes en ayant besoin.

Notamment en-dehors des heures de bureau, une « *clean desk policy* » est nécessaire pour ne pas exposer les dossiers aux risques de destruction ou de vol.

En fonction du traitement, il peut être nécessaire de créer plusieurs copies des documents papier. Dans ce cas, il faut veiller à ce que la conservation et surtout la destruction ne concernent pas uniquement l'original, mais aussi les différentes copies.

A ce stade, la question de digitaliser les documents pour effectuer les traitements à des endroits différents peut être pertinente. Il sera probablement plus facile de tracer l'utilisation de documents électroniques.

Lorsque les documents papier ne sont plus utilisés pour le traitement courant, ils sont archivés. Là encore les durées de rétention vont jouer.

Pour pouvoir passer des documents ou des dossiers en archives intermédiaires, puis définitives, ou les détruire à terme, il faut les classer ou les indexer selon une méthode, qui permettra d'appliquer les règles de rétention définies. Par Exemple, un classement chronologique de factures permettra de les détruire plus facilement à terme. Tandis que le classement de résultats d'analyses médicales et autres données par patient (et non

chronologiquement) permettra de conserver les données pendant toute la durée de vie de la personne, ou de sa prise en charge par l'établissement de santé, plus dix ans.[8]

La destruction ne sera possible qu'en se basant sur une indexation adaptée. Souvent, une base de données comportant les métadonnées clés est le seul moyen de gérer les destructions selon les critères définis. Toutefois, en créant une telle base de données, on crée de nouveau des données personnelles digitales, qu'il faudra gérer à leur tour (effacer aussi les enregistrements dans la base contenant des données personnelles quand les données papier sont effacées).

3.2.3. La destruction des données papier

La règle d'or à appliquer est de ne pas utiliser les poubelles « normales » pour jeter des documents papier contenant des données personnelles. Ces poubelles, même si elles sont réservées au papier, ne sont en général pas protégées et à un moment donné le contenu peut se retrouver dans des bacs non fermés, sur la voie publique en attente de la collecte des ordures, ou dans une décharge à ciel ouvert. A trop d'endroits, il suffit de fouiller les poubelles pour récupérer des données confidentielles.

Les documents concernés doivent donc être déchiquetés sur place, en veillant à ce que les restes ne puissent pas être recomposés facilement.

Alternativement, il est possible d'utiliser des containers fermés pour collecter ces documents. Il faut veiller à ce qu'il soit impossible de ressortir ces documents, sauf par une personne autorisée, qui dispose de la clé du container. Ces containers doivent ensuite être enlevés par une firme spécialisée, qui garantit la destruction du papier de manière à ce qu'il ne reste plus d'information exploitable. Il convient d'établir un contrat en bonne et due forme engageant la responsabilité du prestataire.

Il existe donc des techniques faciles à mettre en place. Le défi est souvent la méthode d'archivage.

Les modalités choisies pour la destruction des documents papier doivent donc être décrites au sein d'une procédure interne à l'organisme, à côté des règles de création et indexation décrites plus loin dans le document.

Mais que faire face à un vrac ou arriéré d'archives papier non classé, ou dont le classement ne permet pas d'appliquer une durée de rétention pour le transfert à l'étape suivante de l'archivage ou la destruction définitive. Là encore, il faut prendre des mesures pour améliorer la situation pour le futur :

- Créer au plus vite pour l'avenir un classement/une indexation adaptés permettant d'appliquer la durée de rétention à l'avenir
- Pour l'arriéré, effectuer si possible une revue individuelle des documents ou au moins d'un échantillon pour voir si en majorité les données/documents sont encore nécessaires
- Déterminer le sort et la durée à appliquer en fonction de cette revue ou de cet échantillonnage : conserver jusqu'en xxxx et veiller à la destruction à terme ; ou détruire (éventuellement après extraction de certains documents encore à conserver)

[8] Article 15 de la loi du 24 juillet 2014 relative aux droits et obligations du patient (10 ans à compter de la fin de la prise en charge)

4. La gestion de la sous-traitance

Dans le cas où le responsable du traitement fait appel à un sous-traitant, il est important de rappeler l'article 28.3.g du RGPD, qui exige que le sous-traitant, au choix du responsable du traitement, retourne les données ou les supprime au terme du contrat. L'application de cette clause doit être adaptée, notamment dans le cas des contrats tacitement renouvelés.

Il n'est pas inutile de rappeler aussi que le sous-traitant doit respecter tous les principes de conservation. La sécurité des données doit donc être assurée, tout comme la limitation des accès (ainsi que leur traçabilité et auditabilité, en cas de violation des données).

Par ailleurs, en cas de nécessité d'effacer les données, soit suite à une demande justifiée, soit parce que la fin de la période de rétention est atteinte, le sous-traitant doit pouvoir exécuter cette opération de destruction. Il doit donc lui aussi avoir mis en place des systèmes lui permettant l'effacement selon certains critères.

A noter que le sous-traitant peut avoir une obligation légale ou un intérêt légitime à ne pas effacer toutes les données personnelles à la fin du contrat. Il peut être obligé par la loi à garder une trace des activités réalisées pour compte d'autrui. Il peut aussi avoir un intérêt légitime à conserver certaines données, afin de pouvoir prouver la bonne exécution de sa tâche tant qu'une action judiciaire dans le cadre de sa responsabilité peut être entamée par le responsable du traitement.

Tout ceci devra être réglé par des clauses contractuelles détaillées, ainsi que des instructions documentées (tel que requis par l'article 28 du RGPD).

5. Procédures à mettre en place

Ainsi, il est nécessaire de gérer les données à caractère personnel, les bases de données et les documents, qu'ils soient digitaux ou sous format papier, tout au long de leur cycle de vie. Afin d'y parvenir, des méthodes doivent être appliquées et des procédures doivent être mises en place.

Le *Records Management* fournit une méthodologie et des procédures qui vont répondre à ces besoins. Le RGPD introduit également un principe important : le « *Privacy by design/by default* ». Celui-ci pose que, dès le début de la mise en place d'un traitement de données personnelles, il faut étudier les différents aspects, dont la rétention et l'effacement, et prendre les mesures nécessaires dès la conception.

Le *Privacy by Design* requiert que le responsable de traitement veille à ce que des mesures techniques et organisationnelles appropriées soient mises en place, tant au moment de la conception d'un processus (« la détermination des moyens de traitement ») que lors du traitement lui-même. En d'autres termes, les principes de protection des données, y inclus les obligations en matière de conservation et destruction, doivent être établis dès la conception d'un nouveau processus. Sur la base des conclusions de l'analyse effectuée dans le cadre du *Privacy by Design*, le responsable du traitement doit établir les règles minimales qui, à la création d'un enregistrement, ou document papier ou électronique, lui permettent de suivre aisément la durée de rétention et la date requise de destruction. En fonction du type de donnée/document, l'information clé (par exemple, à indiquer dans les noms/propriétés du document, ou dans le dossier dans lequel le document est stocké) pourra être la date de création document ou de la collecte de la donnée, la date d'établissement d'une relation avec une contrepartie ou de signature du contrat, ou encore la date de fin de ceux-ci. D'où l'intérêt des déclencheurs décrits plus haut. Il est donc important qu'une réflexion ait lieu en amont, au niveau de l'organisme et/ou des équipes, afin de définir les nomenclatures et classifications nécessaires au suivi correct des périodes de conservation.

Sur base des règles et bonnes pratiques susmentionnées, une ou plusieurs procédure(s) interne(s) doi(ven)t, en fonction des choix faits par l'organisme, établir les règles à respecter par chaque employé en matière de conservation et de destruction des données. Deux procédures sont à notre avis indispensables.

5.1. La procédure de rétention

Cette procédure doit définir comment respecter la politique de rétention. Elle décrira la manière d'assurer la conservation et protection correctes des données et des documents nécessaires. Elle doit aider les employés à comprendre leurs obligations en matière de conservation d'enregistrements papier et de documents électroniques. Il est donc important que la procédure communiquée soit compréhensible par tous.

La procédure doit contenir un tableau (ou base de données) des durées de conservation des données, pour que chaque employé puisse se référer aux obligations légales et réglementaires applicables. En outre, ces informations doivent figurer également dans le registre des traitements de données à caractère personnel, de manière à ce que chaque employé retrouve les règles à respecter dans le cadre de son traitement. Dans le cas d'une petite organisation avec très peu de traitements de données personnelles, il peut être suffisant de documenter ces informations de manière exhaustive uniquement dans le registre des traitements. Ces durées de rétention (ou du moins les principes qui les sous-tendent) doivent aussi être communiquées aux personnes concernées, en application des articles 13 et 14 du RGPD.

5.2. La procédure d'effacement

Une fois la procédure de rétention mise en place, il est tout aussi important de définir la procédure d'effacement des données. Nous l'avons vu à plusieurs reprises, le responsable du traitement n'a pas seulement une obligation de conserver les données correctement. Il doit aussi les effacer une fois que la finalité du traitement n'est plus donnée.

Le responsable de traitement doit donc définir le processus d'effacement des données ainsi que la gouvernance associée. Un défi de cette procédure est la documentation de l'effacement. Notamment en cas de demande d'une personne concernée il est utile de pouvoir démontrer que ses données ont été effacées. Or, il n'est pas possible de garder une trace détaillée des effacements contenant de nouveau les données personnelles. Ainsi, documenter que le CV de tel candidat non retenu a été effacé à telle date serait de nouveau une donnée personnelle, permettant de savoir que la personne concernée avait envoyé une candidature.

Le seul moyen de documenter que les effacements sont effectués correctement est donc la description de la procédure d'effacement et la preuve que cette procédure est exécutée correctement, sans conserver le détail des données effacées.

La procédure d'effacement est souvent en partie manuelle. Idéalement les déclencheurs définis permettent d'automatiser l'effacement, au moins des données numériques.

5.3. Le suivi des procédures

Les procédures doivent être revues sur une base annuelle pour s'assurer de leur efficacité et de leur pertinence. En outre, de plus en plus d'organismes nomment une personne en charge de la conservation des données ou un *Records Manager* (cette fonction pouvant être cumulée avec une ou plusieurs autres fonctions) pour faciliter le suivi de la gestion de la conservation des données et être identifié comme point de contact sur le sujet.

N'oublions pas non plus que, dans les organisations ayant désigné un DPO, ce dernier devrait vérifier la bonne exécution des procédures en place.

Annexe 1 : Exemple de Fiche registre avec durées et textes de référence

D'après le modèle de registre CNIL disponible sur **https://www.cnil.fr/sites/default/files/atoms/files/registre-traitement-simplifie.ods** (avec ajout des textes de référence)

Finalité(s) du traitement effectué			
Finalité principale	Gestion de la paie		
Sous-finalité 1	Calcul des rémunérations		
Sous-finalité 2	Calcul du montant des versements adressés aux organismes sociaux		
Sous-finalité 3	Ordre de virement à la banque		
Catégories de données personnelles concernées	Description	Durée de conservation	Texte de référence
État civil, identité, données d'identification, images...	Noms, prénoms, adresses	5 ans à compter du versement de la paie	Article L3243-4
Informations d'ordre économique et financier (revenus, situation financière, situation fiscale, etc.)	RIB	5 ans à compter du versement de la paie	Modifié par LOI n°2009-526 du 12 mai 2009 - art. 26
Numéro de Sécurité Sociale (ou NIR)	Numéros de sécurité sociale des salariés	5 ans à compter du versement de la paie	L'employeur conserve un double des bulletins de paie des salariés ou les bulletins de paie remis aux salariés sous forme électronique pendant cinq ans.
Catégories de personnes concernées	Description	Précisions	
Catégorie de personnes 1	Salariés		

Annexe 2 : Exemple de tableau annexé à une procédure de rétention

3 - PROCESSUS RESSOURCES HUMAINES					
	SOUMIS À LA RÉGLEMENTATION SUR LA PROTECTION DES DONNÉES A CARACTERE PERSONNEL :				
Données et documents visés	Personnes concernées	Types de données concernées	Texte légal	Durée de conservation	Début de la durée de conservation
PROCESSUS RECRUTEMENT					
Recrutement : extrait de casier judiciaire, certificat de bonnes vie et mœurs,...	-Candidats à l'embauche (recrutés ou non) -Salariés	Données : -d'identification ; condamnations	Art. 8-5 (2) de la Loi du 23/07/ 2016 relative à l'organisation du casier judiciaire	1 mois	A partir de la conclusion du contrat de travail
PROCESSUS GESTION ET ADMINISTRATION des RH					
(...)					
SALAIRES					
Documents relatifs aux salaires dont les bulletins de paie, impôts, sécurité sociale, rémunération des heures supplémentaires, primes, avantages en nature, etc.	-Salariés	Données : -d'identification ; -financières	-Prescription des actions en paiement de salaires de toute nature est de 3 ans (article 2277 du CCivl et Art. L 221-2 du Code du travail) -Conservation des bulletins de paie (=pièces justificatives) pour une durée de 10 ans :Art. 14, 16 et 189 du CCom)	10 ans	à compter de la clôture de l'exercice social de référence

NB : Exemple donné à titre purement indicatif et n'ayant pas vocation de référentiel. Comme indiqué précédemment, il incombe à chaque organisme de réaliser sa propre analyse en identifiant les textes applicables à son activité ainsi que les éventuels référentiels le concernant.

Annexe 3 : Exemples de référentiels

Extrait du TABLEAU DE TRI DES DOCUMENTS ET DES ARCHIVES DE L'INSTITUT NATIONAL DE LA STATISTIQUE ET DES ÉTUDES ÉCONOMIQUES, Archives Nationales de Luxembourg, juin 2020
https://anlux.public.lu/dam-assets/pdf-statiques/STATEC-Convention-tableau-de-tri-V01-01.pdf
Référentiel applicable au STATEC, et pouvant inspirer d'autres organismes, sous réserve de vérification par eux que les textes référencés s'appliquent à leur cas.

Ensemble des tableaux de tri des Archives Nationales : **https://anlux.public.lu/fr/gerer-ses-archives/tableaux-de-tri.html**

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Archives nationales

Code série	Série	Liste des documents	DUA	Élément déclencheur de la DUA	Sort final	Remarques
R2-02	Recrutement et carrière - documents opérationnels ou doublons du dossier du CGPO	- Feuille de renseignement, copie des diplômes, questionnaire ou test précédant l'embauche et ses conclusions, lettre d'embauche, attestation de prise de connaissance du règlement intérieur, document attestant de la situation personnelle et familiale, certificat d'aptitude lors de l'embauche, extrait d'acte d'État-civil, relevé d'identité bancaire, lettre de démission et réponse, reconstitution de carrière et état des services, accusés de réception (clefs et badges d'accès au bâtiment), copie des arrêtés, attestation de prise de connaissance du document de l'organisation interne, de la politique de sécurité de l'information et de la charte de confidentialité, accord de confidentialité **- Extrait de casier judiciaire*** **- Affaires disciplinaires mineures** (avertissement, réprimande et amende ne dépassant pas le 5ème d'une mensualité brute du traitement de	75	Date de naissance de l'agent	D	**Justification de la DUA et du sort final :** Ces documents sont détruits car le dossier de carrière des agents est conservé auprès du CGPO *** Destruction au bout d'1 mois si candidature retenue** - Lettre circulaire du 17 mai 2019 relative aux délais de conservation des casiers judiciaires - Loi modifiée du 29 mars 2013 relative à l'organisation du casier judiciaire et aux échanges d'informations extraites du casier judiciaire entre les États membres de l'Union européenne, art. 8-5 **** Destruction (mention rayée dans le dossier) après 3 ans** à compter de la décision sanctionnant l'agent si, dans les 3 ans qui suivent la décision disciplinaire, le fonctionnaire n'a encouru aucune nouvelle sanction disciplinaire - Loi modifiée du 16 avril 1979 fixant le statut général des fonctionnaires de l'État, art. 54 §5

Extrait du Référentiel des durées de conservation dans le domaine de la recherche en santé, CNIL, juin 2020 https://www.cnil.fr/sites/default/files/atoms/files/referentiel_-_recherches_dans_le_domaine_de_la_sante.pdf

Activités de traitement	Détails du traitement	Durées de conservation en base active	Durées de conservation en archives intermédiaires	Fondements juridiques Textes de références
Recherches impliquant la personne humaine (RIPH) et recherches nécessitant le recueil du consentement de la personne concernée : - Les recherches interventionnelles, y compris les recherches à risques et contraintes minimes ; - Les essais cliniques de médicaments à l'exception des essais cliniques par grappes ; - Les recherches nécessitant la réalisation d'un examen des caractéristiques génétiques;	**Recherche conforme à la MR[1]-001** *Données des personnes se prêtant à la recherche*	Conservation dans les systèmes d'information du RT, du centre investigateur ou du professionnel intervenant dans la recherche **jusqu'à la mise sur le marché du produit étudié** ou **jusqu'à 2 ans** à compter de la dernière publication des résultats de la recherche. En l'absence de publication : conservation **jusqu'à la signature du rapport final de la recherche**.	Archivage sur support papier ou informatique pour une **durée conforme à la réglementation en vigueur**	MR-001 Délibération n° 2018-153 du 3 mai 2018 Réglementation sectorielle applicable : code de la santé publique, arrêtés (ex : arrêté du 8 novembre 2006, bonnes pratiques cliniques, règlement n°536/2014)
	Recherche conforme à la MR-001 *Données des professionnels intervenant dans la recherche*	**15 ans** au maximum après la fin de la dernière recherche à laquelle les professionnels ont participé	Archivage sur support papier ou informatique pour une **durée conforme à la réglementation en vigueur**	MR-001 Délibération n° 2018-153 du 3 mai 2018 Réglementation sectorielle applicable : code de la santé publique, arrêtés (ex : arrêté du 8 novembre 2006, bonnes pratiques cliniques, règlement n°536/2014)

Pour aller plus loin :

Ces orientations qui se veulent simples et pratiques, ont été rédigées par les membres de la Commission technique en 2019-2020, en réponse aux nombreuses questions de nos membres sur le sujet. Depuis, la CNIL a publié une guidance sur le sujet, ainsi que ses référentiels sectoriels, qui pourront être utiles à tout professionnel de la protection des données souhaitant approfondir le sujet : **https://www.cnil.fr/fr/les-durees-de-conservation-des-donnees**.

DISCLAIMER

Les droits de propriété intellectuelle attachés au présent document ainsi que les logos, dessins, designs, titres et intérêts qui en découlent appartiennent exclusivement à l'APDL. L'APDL et éventuellement des tiers titulaires de droits sur ces éléments sont seuls habilités à les exploiter et les modifier. Vous disposez d'un droit de diffusion de ces éléments sans possibilité d'en modifier le contenu ou le formatage et à condition que cette diffusion soit conforme aux bons usages, qu'elles ne poursuivent pas un but de lucre et qu'elle ne porte pas atteinte ni à l'œuvre ni à son exploitation.

Lors de la diffusion de ces éléments ou d'extraits de ces éléments et conformément à la législation applicable aux droits d'auteur, vous vous engagez à conserver les logos et le nom de l'APDL et à indiquer la source et l'auteur.