VADE-MECUM

Unaf
UNIS POUR LES FAMILLES

COMMENT METTRE EN PLACE LE RGPD DANS LES SERVICES ?

POUR MIEUX PROTÉGER LES PERSONNES ACCOMPAGNÉES

MARS 2021

De la collecte à la conservation des données personnelles !

Ce guide a été créé par l'Unaf, avec la participation des Udaf et d'experts en archivage (Françoise COHEN-CASSUTO, *Un dossier Une place*) et du RGPD (Maitre Alexandre TESSONNEAU, *Squadra Avocats*). Il relève de la propriété de l'Unaf mais a vocation à être mis à disposition auprès d'autres acteurs concernés.

Il a fait l'objet d'une relecture approfondie par la CNIL, lui conférant ainsi un gage de qualité et de fiabilité.

Il a pour but de rappeler le cadre juridique en matière d'archivage et de RGPD, et donner des repères en termes d'organisation, de pratiques professionnelles et de réflexions éthiques.

Les illustrations proviennent toutes du site freepik.com et flaticon.com

AVANT-PROPOS

Un règlement général sur la protection des données pour mieux garantir le respect des droits et de la vie privée des citoyens, a fortiori pour les plus vulnérables

Entré en application le 25 mai 2018, le règlement général sur la protection des données (RGPD) s'inscrit dans la continuité de la loi « Informatique et Libertés » de 1978. Il a harmonisé les règles en matière de protection des données à caractère personnel sur le territoire de l'Union européenne, permettant aux citoyens et aux professionnels de bénéficier d'un cadre juridique unique.

Ainsi tout organisme, quels que soient sa taille, son pays d'implantation ou son activité, est concerné par le RGPD et doit s'inscrire dans une démarche de conformité. Pour y arriver, les professionnels doivent mettre en place des procédures et des actions destinées à assurer le respect des principes du RGPD.

Le secteur social et médico-social n'échappe bien sûr pas à cette évolution. Eu égard aux volumes conséquents de données collectées et traitées, souvent sensibles, concernant les familles et les personnes accompagnées, de nouvelles organisations et des changements de comportements individuels se mettent en place, concernant tant les salariés que les personnes accompagnées.

Cette mise en conformité constitue donc une étape incontournable pour l'ensemble du secteur, mais peut parfois se révéler délicate au regard de l'environnement juridique complexe que représentent le Code de l'action sociale et des familles et le Code de la santé publique.

Un guide pratique utile pour l'ensemble des acteurs du secteur social et médico-social

C'est pourquoi la CNIL salue pleinement l'initiative commune de l'Unaf et des Udaf, ainsi que la grande qualité de ce guide pratique. Cette démarche d'accompagnement rejoint pleinement celle de la CNIL qui a adopté un référentiel relatif aux traitements des données à caractère personnel, dans le cadre de l'accueil, l'hébergement et l'accompagnement social et médico-social des personnes âgées, des personnes en situation de handicap et de celles en difficulté.

Ce guide, à la fois théorique et pratique, sera incontestablement utile aux acteurs du secteur social et médico-social qui, à n'en pas douter, sauront rapidement se « l'approprier » afin de garantir le respect des droits et libertés des personnes qu'ils accompagnent.

Marie-Laure DENIS
Présidente de la CNIL

ÉDITO

Pour mieux protéger les personnes accompagnées : un « vade-mecum » sur le RGPD, de la collecte à la conservation des données personnelles

Avec ce guide, l'Unaf souhaite rappeler les notions clés et les règles en vigueur. Il est illustré d'exemples concrets issus des Udaf. Il propose également des recommandations pour que les pratiques professionnelles protègent les droits des familles et des personnes accompagnées. Vous y trouverez ainsi les différentes étapes de mise en conformité au RGPD : de la collecte à la conservation des données. Nous espérons qu'il facilitera au plus grand nombre l'adaptation aux changements et permettra aux professionnels des Udaf ou de toute autre structure, de répondre à leurs questionnements et d'assumer au mieux leurs responsabilités.

In fine, l'objectif est bien celui d'améliorer sans cesse la qualité des services rendus aux personnes et aux familles. Nous gagnerons ainsi collectivement en sécurité et en efficacité et surtout nous répondrons à un enjeu de transparence, condition de la relation de confiance nécessaire pour les accompagner avec bientraitance.

Aussi, ce vade-mecum constitue une première étape de sensibilisation, dans un esprit pédagogique et très pratique. Ancré dans plusieurs champs d'intervention, il prend en compte différentes approches : le régime des archives publiques, le RGPD, les spécificités légales des secteurs d'activité comme celui de la protection juridique des majeurs, mais aussi les réalités du terrain. Au-delà de ce guide, l'Unaf entend poursuivre sa démarche pour aider au mieux les professionnels à conforter leurs pratiques.

Un outil conçu par et pour de nombreux acteurs

Cet outil est le fruit d'une collaboration active entre l'Unaf et les Udaf, avec l'appui d'experts : une archiviste professionnelle et un cabinet d'avocats. Plus d'une trentaine d'Udaf ont ainsi participé à ce travail, à travers l'organisation de nombreux échanges et réunions.

Nous remercions particulièrement la CNIL pour ses encouragements et son précieux soutien au travers de l'engagement de sa Présidente et de la collaboration à notre démarche des équipes de la CNIL. Leur travail de relecture, leurs suggestions d'améliorations et leurs amendements confèrent à cet outil un gage de qualité et de fiabilité.

Nous remercions toutes les personnes extérieures ou membres de notre réseau qui ont participé à ce travail, sans qui il n'aurait pu aboutir.

Ce guide peut être utile à toutes les associations porteuses des mêmes services, en particulier les services mandataires judiciaires à la protection des majeurs (MJPM) et les services délégués aux prestations familiales (DPF), mais également à toute organisation concernée par le traitement des données personnelles des personnes accompagnées.

La protection des données est un sujet primordial qui offre la possibilité de multiples collaborations et l'Unaf avance dans la perspective de tout nouveau partenariat profitable à l'intérêt des personnes vulnérables.

Guillemette LENEVEU
Directrice Générale de l'Unaf

Marie-Andrée BLANC
Présidente de l'Unaf

SOMMAIRE

INTRODUCTION 7

PROMOUVOIR LES DROITS DES PERSONNES EN CONCILIANT LE RGPD ET LE RÉGIME DES ARCHIVES PUBLIQUES 7
LES TRAVAUX DE L'UNAF SUR L'ARCHIVAGE ET LA PROTECTION DES DONNÉES DES PERSONNES ACCOMPAGNÉES 8

CHAPITRE I : LES NOTIONS DU RGPD 13

1. LES DONNÉES PERSONNELLES 14
2. LE TRAITEMENT DES DONNÉES PERSONNELLES 15
3. LE RESPONSABLE DE TRAITEMENT 16
4. LES SOUS-TRAITANTS 16

CHAPITRE II : LES PRINCIPES DE LA PROTECTION DES DONNÉES 17

1. LE PRINCIPE DE LICÉITÉ : DÉFINIR LA BASE LÉGALE D'UN TRAITEMENT DE DONNÉES 18
2. LE PRINCIPE DE FINALITÉ 21
3. LE PRINCIPE DE PROPORTIONNALITÉ ET DE PERTINENCE 22
4. LE PRINCIPE D'UNE DURÉE DE CONSERVATION LIMITÉE 29
5. LE PRINCIPE DE CONFIDENTIALITÉ 33
6. LE PRINCIPE DE SÉCURITÉ 38

CHAPITRE III : L'INFORMATION ET LES DROITS DES PERSONNES 45

1. LE DROIT À L'INFORMATION 48
2. LE DROIT D'ACCÈS 52
3. LE DROIT DE RECTIFICATION 58
4. LE DROIT D'OPPOSITION 58
5. LE DROIT À L'OUBLI 59
6. LE DROIT À LA LIMITATION DU TRAITEMENT 60
7. LE DROIT À LA PORTABILITÉ DES DONNÉES 61

CHAPITRE IV : LES ETAPES DE MISE EN CONFORMITÉ AU RGPD 63

1. DÉSIGNER UN DÉLEGUÉ À LA PROTECTION DES DONNÉES (DPO) 65
2. CRÉER ET METTRE À JOUR UN REGISTRE DE TRAITEMENT 67
3. CONSTRUIRE UN PLAN D'ACTION VERS LA CONFORMITÉ 68
4. MENER UNE ANALYSE D'IMPACT RELATIVE À LA PROTECTION DES DONNEES 69
5. ORGANISER DES PROCESSUS EN INTERNE 71
6. DOCUMENTER LA CONFORMITÉ 72

ANNEXES _____ 73

RÉFERÉNCES JURIDIQUES _____ 89

FOIRE AUX QUESTIONS _____ 93

POUR ALLER PLUS LOIN _____ 99

LISTE DES SIGLES _____ 103

GLOSSAIRE _____ 105

REMERCIEMENTS _____ 113

INTRODUCTION

PROMOUVOIR LES DROITS DES PERSONNES EN CONCILIANT LE RGPD ET LE RÉGIME DES ARCHIVES PUBLIQUES

Le secteur social et médico-social n'échappe pas à la transition numérique que traverse notre société. Les modes de vie de la population évoluent et les fonctionnements des organisations aussi. La dématérialisation accrue, notamment pour les démarches d'ouverture et de maintien des droits, nécessite une adaptation des actions auprès des personnes accompagnées. Si les usages de l'informatique se généralisent, il convient de s'interroger sur la place des personnes qui en sont privées.

Par ailleurs, nous savons que l'essor du numérique renforce la reconnaissance de certains droits fondamentaux tels que la liberté d'expression, mais qu'il peut aussi en affaiblir d'autres comme le droit à la vie privée ou à la sécurité.

Aussi, toutes les organisations qui traitent des données à caractère personnel doivent se mettre en conformité avec le RGPD. Entré en application le 25 mai 2018 dans toute l'Union Européenne, le RGPD adapte le cadre juridique aux évolutions technologiques de notre société. S'il introduit certaines grandes nouveautés, les principes fondamentaux[1] établis par la loi française « Informatique et Libertés » (loi I&L) de 1978 modifié constituent toujours le socle de la protection des données personnelles.

Tous les **services sociaux et médico-sociaux** traitent de nombreuses informations, souvent sensibles, concernant les familles et les personnes accompagnées**. Outre l'application stricte du règlement, il convient qu'ils s'engagent dans une démarche éthique,** afin de trouver un juste équilibre entre le respect de la vie privée d'une part, et la nécessité d'utiliser des données pour garantir un accompagnement de qualité d'autre part. Tel est par exemple le cas des **services mandataires à la protection des majeurs** ou des **services délégués aux prestations familiales,** qui viennent illustrer le présent guide.

Enfin, les Udaf, comme d'autres organisations, sont des organismes de droit privé, chargés d'une mission de service public. A ce titre, en plus des règles relatives au RGPD, elles sont soumises au régime des archives publiques.

[1] Finalité, loyauté et licéité de la collecte, proportionnalité du traitement, protection renforcée des données sensibles, droits de personnes (cf. Loi n°78-17 du 6 janvier 78)

Deux corpus de textes sont donc à respecter, leur articulation n'étant pas toujours aisée :

- **le Code du patrimoine** axé sur la conservation des archives publiques, tant pour des besoins administratifs qu'à des fins de recherches scientifiques ou historiques[2], et sur l'accès par toute personne intéressée aux documents publics ;

- **le RGPD** qui défend les droits des personnes concernant leurs données à caractère personnel, qui limite l'accès et la durée de conservation de ces données. Toutefois, l'article 89 du RGPD prévoit une exception pour les services publics, à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques.

LES TRAVAUX DE L'UNAF SUR L'ARCHIVAGE ET LA PROTECTION DES DONNÉES DES PERSONNES ACCOMPAGNÉES

Quel que soit leur degré d'avancement dans l'élaboration et la mise en œuvre de procédures formelles, toutes les Udaf, comme d'autres organisations, sont confrontées au quotidien à des questions d'archivage et de protection des données.

Les évolutions légales ont provoqué de nombreuses interrogations dans l'ensemble du secteur associatif.

C'est pourquoi, l'Etat et l'Unaf ont choisi d'inscrire, dans leur convention d'objectifs pluriannuelle, une action dédiée à l'archivage et la dématérialisation des documents dans les services.

Cette action a permis d'actualiser le **protocole national d'accord du traitement des archives** des Udaf, signé avec le ministère de la Culture en 1998, et d'élaborer le présent guide.

Afin d'apporter un soutien et des bases communes dans cette démarche, de favoriser son essaimage auprès des équipes, l'Unaf a proposé aux Udaf intéressées de participer à une production collective. Plus d'une trentaine d'Udaf ont participé à la rédaction de ce guide[3].

[2] Art. L 211-2 du Code du patrimoine
[3] Cf. liste des participants à la page de remerciements

LA REFONTE DU PROTOCOLE POUR LA GESTION DES ARCHIVES DES UDAF

Le **protocole d'accord pour le traitement des archives des Udaf** de 1998 nécessitait une mise à jour, pour **être plus conforme aux évolutions législatives et à l'élargissement des activités des Udaf.**

Dans ce cadre, l'Unaf a signé le 3 février 2021, avec le Ministère de la Culture (service interministériel des Archives de France – SIAF), un **protocole d'accord** et en annexe une **nouvelle stratégie nationale d'archivage des Udaf**. Validés par le Ministère de la Culture, ils ont également été approuvés par le Ministère de la Justice et le Ministère des Solidarités et de la Santé.

Ces documents sont accessibles sur le portail *France Archives* :
https://francearchives.fr/fr/circulaire/DGPA_SIAF_2021_002?j

Ils peuvent être utilisés par d'autres opérateurs impliqués dans les mêmes activités que les Udaf.

- Le nouveau « **protocole** » constitue une note de cadrage signée entre le SIAF et l'Unaf, qui vise à formaliser et préciser les modalités de gestion des archives par les Udaf et l'exercice du contrôle scientifique et technique (CST) de l'administration des archives sur les Udaf.

- Est annexée à ce protocole, la « **stratégie nationale** » qui énonce les règles applicables aux dossiers clos (textes de références, durée de conservation, sort final). Elle donne aussi des préconisations de tri interne des documents constituant le dossier actif de protection juridique des majeurs.

LA RÉALISATION D'UN VADE-MECUM

Ce guide pratique a vocation à **rappeler le cadre juridique et à donner des repères en termes d'organisation, de pratiques professionnelles et de réflexions éthiques.**

Ce document, principalement axé sur les droits des publics accompagnés, concerne tous les professionnels intervenants dans les associations :

→ Fonctions supports (RH, comptabilité,…)

→ Vie institutionnelle (gestion des adhérents et des représentants, votes,…)

→ Actions de politique familiale (observatoires,…)

→ Services auprès des personnes et familles (MJPM, MJAGBF, PCB, Famille-Gouvernante, ASLL,…)

Ce guide est organisé ainsi :

Quatre chapitres...

- **Chapitre I :** Les notions du RGPD
- **Chapitre II :** Les principes de la protection des données
- **Chapitre III :** L'information et les droits des personnes
- **Chapitre VI :** Les étapes de mise en conformité au RGPD

... comprenant des encarts spécifiques :

- **Des exemples** pour éclairer, illsutrer et préciser les propos grâce aux expériences développées par les Udaf.
- **Des recommandations** qui donnent des conseils concrets aux Udaf concernant la réalisation de certaines pratiques.
- **Des références juridiques**, tout au long du document, viennent préciser le cadre légal des pratiques. Ces références sont recensées à la fin du document.

Des annexes

- Un exemple de procédure d'accès aux données personnelles
- Des recommandations pour la numérisation
- Les obligations des sous-traitants
- Une note pratique pour les professionnels de l'accompagnement
- Présentation du référentiel social et médico-social de la CNIL

Une foire aux questions

- Présentée sous forme de questions/réponses, elle répond aux interrogations les plus fréquemment posées par les Udaf.

Une liste des sigles et un glossaire

- Face à un vocabulaire technique ponctué d'anglicismes, d'abréviations, d'acronymes et de sigles en tout genre, il n'est pas toujours évident de s'y retrouver. Afin de mieux comprendre les jargons du RGPD et de l'archivage, un kit de survie lexical, décliné en une liste des sigles et un glossaire, sont à votre disposition à la fin de ce document.

CHAPITRE I

LES NOTIONS DU RGPD

1. LES DONNÉES PERSONNELLES

« Toute information se rapportant à une personne physique identifiée ou identifiable ».[4]

Dans le secteur social et médico-social, les familles et personnes accompagnées peuvent par exemple être identifiées par leur :

- *Nom, prénom ;*
- *Numéro de téléphone, adresse postale ou adresse mail, photo ;*
- *Numéro de sécurité sociale, numéro de rattachement à un organisme (CAF, CNAV, etc.) ;*
- *Situation financière concernant les ressources et les dettes ou encore les prestations et avantages sociaux perçus dès lors qu'ils sont rattachables à une personne.*

FOCUS : ANONYMISATION DES DONNÉES PERSONNELLES

L'anonymisation est un traitement qui consiste à utiliser un ensemble de techniques **de manière à rendre impossible, en pratique, toute identification de la personne par quelque moyen que ce soit et de manière irréversible.**

Les autorités de protection des données européennes définissent trois critères qui permettent de s'assurer qu'un jeu de données est véritablement anonyme :

1. **l'individualisation** : il ne doit pas être possible d'isoler un individu dans le jeu de données.

Par exemple : une base de données de CV où seuls les noms et prénoms d'une personne auront été remplacés par un numéro (qui ne correspond qu'à elle) permet d'individualiser cette personne. Dans ce cas, cette base de données est considérée comme pseudonymisée et non comme anonymisée ;

2. **la corrélation** : il ne doit pas être possible de relier entre eux des ensembles de données distincts concernant un même individu.

Par exemple : une base de données cartographique renseignant les adresses de domiciles de particuliers ne peut être considérée comme anonyme si d'autres bases de données, existantes par ailleurs, contiennent ces mêmes adresses avec d'autres données permettant d'identifier les individus ;

[4] Article 4 du RGPD

3. **l'inférence** : il ne doit pas être possible de déduire, de façon quasi certaine, de nouvelles informations sur un individu.

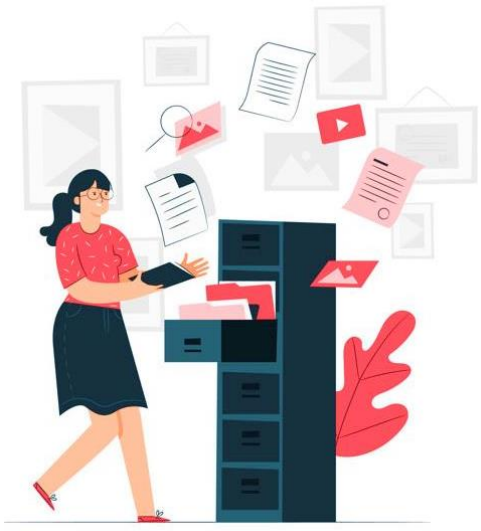
Par exemple : si un jeu de données supposément anonyme contient des informations sur le montant des impôts de personnes ayant répondu à un questionnaire, que tous les hommes ayant entre 20 et 25 ans qui ont répondu sont non imposables, il sera possible de déduire, si on sait que M. X, homme âgé de 24 ans, a répondu au questionnaire, que ce dernier est non imposable.

Pour en savoir plus : une fiche relative à l'anonymisation des données personnelles est disponible sur le site de la CNIL.

S'il est possible par regroupement d'informations (âge, sexe, ville, diplôme, etc.) d'identifier une personne, les données sont alors toujours considérées comme personnelles.

2. LE TRAITEMENT DES DONNÉES PERSONNELLES

Il s'agit de l'ensemble des opérations, portant sur des données personnelles, quel que soit le procédé utilisé : collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission, diffusion ou toute autre forme de mise à disposition, rapprochement.



Les données traitées peuvent être **numériques** mais aussi intégrées dans des **documents papiers**.

Par exemple, le RGPD et la loi Informatique et Libertés s'appliquent aux carnets de note des travailleurs sociaux ainsi qu'aux fiches de liaisons sociales remplies à la main par les usagers.

Le simple fait de procéder à la collecte de ces données est un traitement et doit être, à cet égard, recensé dans le registre des activités de traitements. [5]

[5] Le registre de traitement est un document de recensement et d'analyse, qui doit refléter la réalité des traitements de données personnelles. Pour plus de détail, voir chapitre 4.

3. LE RESPONSABLE DE TRAITEMENT

Il s'agit de la personne morale ou physique, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement et qui décide de sa création.

Il s'agit généralement de la personne morale d'une association, d'une collectivité incarnée par son représentant légal (le maire, le président ou le directeur d'une association, etc.) ;

Par exemple, une Udaf est susceptible d'être considérée comme responsable de traitement dès lors qu'elle a pris l'initiative de la création du traitement de données à caractère personnel et piloté les moyens techniques et/ou humains liés à sa mise en œuvre.

Le responsable de traitement doit être en mesure de démontrer à tout moment le respect du RGPD par la mise en place de mesures techniques et organisationnelles appropriées.

L'objet de ce guide est justement de vous aider à mettre en place ces mesures.

4. LES SOUS-TRAITANTS

Le **sous-traitant** est la personne physique ou morale (entreprise privée ou organisme public) qui traite des données pour le compte d'un autre organisme (le responsable de traitement), dans le cadre d'un service ou d'une prestation.

Par exemple, les éditeurs de logiciels, les hébergeurs de données, les prestataires de stockage d'archives intermédiaires,…

Les sous-traitants ont des obligations concernant les données personnelles, qui doivent être présentes dans le contrat :

- une **obligation de transparence** et de **traçabilité** ;
- la **prise en compte des principes de protection des données ;**
- une **obligation de garantir la sécurité des données traitées** ;
- une **obligation d'assistance, d'alerte et de conseil** (par exemple, existence d'une procédure de notification des violations de données personnelles).[6]

Recommandations

Vous pouvez vous appuyer sur un exemple de contrat avec les sous-traitants sur le site de la Cnil : https://www.cnil.fr/fr/sous-traitance-exemple-de-clauses et vous référer à l'annexe 3 du présent guide.

[6] https://www.cnil.fr/fr/definition/sous-traitant

CHAPITRE II

LES PRINCIPES DE LA PROTECTION DES DONNÉES

Ce chapitre définit les principes à respecter lors de la collecte, du traitement et de la conservation de données personnelles. Ils doivent guider la réflexion et les pratiques des professionnels au quotidien.[7]

1. LE PRINCIPE DE LICÉITÉ : DÉFINIR LA BASE LÉGALE D'UN TRAITEMENT DE DONNÉES

Le traitement des données personnelles n'est autorisé que s'il repose sur une base légale. Déterminer cette base constitue donc une étape-clé.

Tout traitement doit se fonder sur au moins l'une des 6 « bases légales » définies par l'article 6 du RGPD :

- **Consentement** de la personne concernée,

Dans le secteur social et médico-social, **le consentement n'est pas une base légale recommandée** (*cf.* focus sur le consentement ci-après).

- **Exécution d'un contrat** conclu avec la personne concernée,

Fournir des prestations définies dans le cadre du contrat conclu entre l'organisme et la personne concernée ou son représentant légal, et le cas échéant, assurer la gestion du dossier administratif de la personne concernée. Dans le cadre d'un contrat de mandat de protection future par exemple.

- Respect d'une **obligation légale**[8] à laquelle le responsable de traitement est soumis,

Gestion administrative, financière et comptable de l'établissement, du service ou de l'organisme

- Sauvegarde des **intérêts vitaux de la personne concernée** (ou d'une autre personne physique),

Lorsque le traitement est nécessaire pour suivre la propagation d'épidémies ou dans les cas d'urgence humanitaire.

- Exécution d'une **mission d'intérêt public** ou relevant de l'exercice de l'autorité publique dont est investi le responsable de traitement[9],

Accompagnement social et médico-social adapté aux difficultés rencontrées ayant notamment pour objet d'élaborer un projet personnalisé d'accompagnement, d'assurer le

[7] Le principe de transparence et de respect des droits ne sera pas abordé dans ce chapitre. Le chapitre 3 est notamment consacré à l'information et droits des personnes.
[8] https://www.cnil.fr/fr/lobligation-legale-dans-quels-cas-fonder-un-traitement-sur-cette-base-legale
[9] https://www.cnil.fr/fr/la-mission-dinteret-public-dans-quels-cas-fonder-un-traitement-sur-cette-base-legale

suivi des personnes dans l'accès aux droits et, le cas échéant, d'orienter les personnes vers les structures compétentes susceptibles de les prendre en charge ;

Échange et partage des informations strictement nécessaires permettant de garantir la coordination et la continuité de l'accompagnement et du suivi des personnes entre les intervenants sociaux, médicaux et paramédicaux ;

Instruction, gestion et, le cas échéant, ouverture des droits et/ou versement des demandes de prestations sociales légales ou facultatives ;

- **Intérêts légitimes poursuivis par le responsable de traitement** (ou par un tiers), sauf si des intérêts, libertés, ou droits fondamentaux de la personne concernée prévalent.[10]

Accompagnement social et médico-social adapté aux difficultés rencontrées ayant notamment pour objet d'élaborer un projet personnalisé d'accompagnement, d'assurer le suivi des personnes dans l'accès aux droits et, le cas échéant, d'orienter les personnes vers les structures compétentes susceptibles de les prendre en charge ;

Échange et partage des informations strictement nécessaires permettant de garantir la coordination et la continuité de l'accompagnement et du suivi des personnes entre les intervenants sociaux, médicaux et paramédicaux ;

Instruction, gestion et, le cas échéant, ouverture des droits et/ou versement des demandes de prestations sociales facultatives

Attention, « ***lorsqu'un même traitement de données poursuit plusieurs finalités, c'est-à-dire plusieurs objectifs, une base légale doit être définie pour chacune de ces finalités.*** *En revanche, il n'est pas possible de « cumuler » des bases légales pour une même finalité : il faut en choisir une seule. »* [11]

La ou les bases légales du traitement doivent être mentionnées dans les éléments d'information fournis aux personnes dont les données sont traitées.

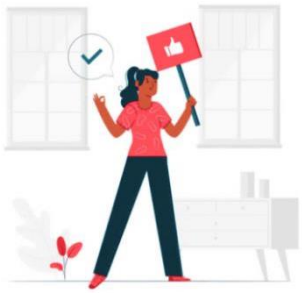
Recommandations

Pour vous aider à définir votre base légale, vous pouvez consulter les fiches pratiques réalisées par la CNIL sur https://www.cnil.fr/fr/les-bases-legales

[10] Cette base légale ne s'applique pas au traitement effectué par les autorités publiques dans l'exécution de leurs missions.

[11] https://www.cnil.fr/fr/la-liceite-du-traitement-lessentiel-sur-les-bases-legales-prevues-par-le-rgpd

FOCUS : LE CONSENTEMENT DE LA PERSONNE CONCERNÉE



Dans le secteur social et médico-social, **le consentement n'est pas une base légale recommandée** dans la mesure où les personnes accompagnées, souvent en situation de vulnérabilité, ne sont pas toujours en mesure de donner, de refuser ou de révoquer librement leur consentement. Les usagers se retrouvent en effet souvent dans une situation de dépendance vis-à-vis des organismes sociaux et médico-sociaux.

Dans le cas où le traitement repose sur le consentement, le responsable de traitement devra démontrer qu'il a bien obtenu, auprès de la personne concernée, le droit de traiter ses données à caractère personnel. La demande de consentement auprès de la personne doit être présentée sous une **forme compréhensible et aisément accessible**, et formulée en des **termes clairs et simples. La personne doit être informée qu'elle a le droit de retirer son consentement à tout moment**.[12]

Le consentement est valide seulement s'il est conforme à quatre critères[13] :

- **libre** : le consentement ne doit pas être contraint ni influencé. La personne doit se voir offrir un choix réel, sans avoir à subir de conséquences négatives en cas de refus ;
- **spécifique** : un consentement doit correspondre à un seul traitement, pour une finalité déterminée ;
- **éclairé** : pour qu'il soit valide, le consentement doit être accompagné d'un certain nombre d'informations communiquées à la personne avant qu'elle ne consente ;
- **univoque** : le consentement doit être donné par une déclaration ou tout autre acte positif clairs. Aucune ambiguïté quant à l'expression du consentement ne peut demeurer.

Il convient de distinguer le consentement en tant qu'exception prévue par le RGPD autorisant la collecte de données sensibles, du consentement en tant que base légale ou base juridique qui autorise légalement la mise en œuvre du traitement.

Pour aller plus loin : l'ensemble des conditions applicables au consentement est précisé dans la fiche relative aux conditions de recueil du consentement disponible sur le site de la CNIL.

[12] Néanmoins, les traitements réalisés avant le retrait de consentement restent licites.
[13] https://www.cnil.fr/fr/conformite-rgpd-comment-recueillir-le-consentement-des-personnes

2. LE PRINCIPE DE FINALITÉ

Le responsable de traitement ne peut enregistrer et utiliser des informations sur des personnes physiques que dans un **but bien précis, légal et légitime**. La finalité d'un traitement correspond à la raison pour laquelle il est créé.

Les données à caractère personnel, les durées de conservation et la liste des personnes pouvant y accéder vont ensuite être déterminées en fonction de l'objectif poursuivi par le traitement.

Quelques exemples de finalités de traitement dans le secteur social et médico-social :

- l'**exercice des mesures de protection ou autres missions confiées** ;

Par exemple, l'exercice d'une mesure de tutelle pour protéger une personne majeure et/ou tout ou partie de son patrimoine si elle n'est plus en état de veiller sur ses propres intérêts.

- la **fourniture des prestations** définies dans le cadre d'un contrat conclu entre l'organisme et la personne concernée ou son représentant légal et, le cas échéant, la gestion du dossier administratif de la personne concernée ;

Le contrat de séjour ou le document individuel de prise en charge entre l'organisme (EHPAD, CHRS,…) et la personne concernée.

- **l'accompagnement social et médico-social adapté** aux difficultés rencontrées ayant notamment pour objet **d'élaborer un projet personnalisé d'accompagnement** au regard des habitudes de vie, des demandes particulières, des besoins particuliers, de l'autonomie physique et psychique de la personne et d'en assurer le suivi conformément aux dispositions des articles L. 311-3 du CASF, **le suivi des personnes dans l'accès aux droits** notamment l'assistance dans les relations et les démarches à effectuer et, le cas échéant, **l'orientation des personnes vers les structures compétentes susceptibles de les prendre en charge** ;

Par exemple, l'accompagnement éducatif et budgétaire des personnes, dans le cadre d'un service PCB,

La gestion des demandes d'hébergement et d'accès au logement, la gestion des impayés et la prévention des expulsions, dans le cadre d'une mesure ASLL,

Le suivi des personnes et des familles dans le cadre de la médiation familiale

- **l'échange et le partage des informations** strictement nécessaires dans le respect des dispositions de l'article L. 1110-4 du CSP et des dispositions du CASF, permettant de garantir la coordination et la continuité de l'accompagnement et du suivi des personnes entre les intervenants sociaux, médicaux et paramédicaux ;

- la **gestion administrative, financière et comptable** de l'établissement, du service ou de l'organisme ;

→ **la remontée des informations préalablement anonymisées aux autorités compétentes** concernant des dysfonctionnements graves ou évènements ayant pour effet de menacer ou de compromettre la santé, la sécurité ou le bien-être des personnes prises en charge conformément aux dispositions des articles R. 331-8 et suivants du CASF**, l'établissement des statistiques, des études internes et des enquêtes de satisfaction** aux fins d'évaluation de la qualité des activités et des prestations et des besoins à couvrir**.**

Ces exemples de finalités sont issus du référentiel social et médico-social de la CNIL.

3. LE PRINCIPE DE PROPORTIONNALITÉ ET DE PERTINENCE

La CNIL rappelle que les données ne peuvent être systématiquement collectées. Le responsable de la collecte doit pouvoir justifier de son **caractère nécessaire et proportionné**, notamment en fonction des particularités des situations sociales rencontrées et du type de prestation ou d'aide demandée. Il doit notamment veiller à ce que seules les données nécessaires à la poursuite des finalités du traitement soient effectivement collectées et traitées.

Dans le cadre d'un service de microcrédit, on ne pourra pas recueillir des données non pertinentes pour instruire le dossier, telles que le numéro de sécurité sociale des personnes, le numéro MDPH, etc. mais des données en lien avec des critères de remboursement et de ressources par exemple.

On ne peut pas collecter et/ou conserver des données personnelles « au cas où parce que cela pourrait servir un jour ».

Cette réutilisation peut se faire seulement si elle est conforme aux dispositions de l'article 6.4 du RGPD (existence d'un lien entre les finalités pour lesquelles les données personnelles ont été collectés et les finalités du traitement ultérieur envisagé, existence de garanties appropriées,...) De même, les personnes concernées doivent être informées de cette réutilisation des données personnelles.

Il est important de distinguer les informations à connaître, de celles à enregistrer et donc de faire un tri entre les informations dont le responsable de traitement dispose et celles dont il a réellement besoin pour sa mission, c'est-à-dire les données à enregistrer.

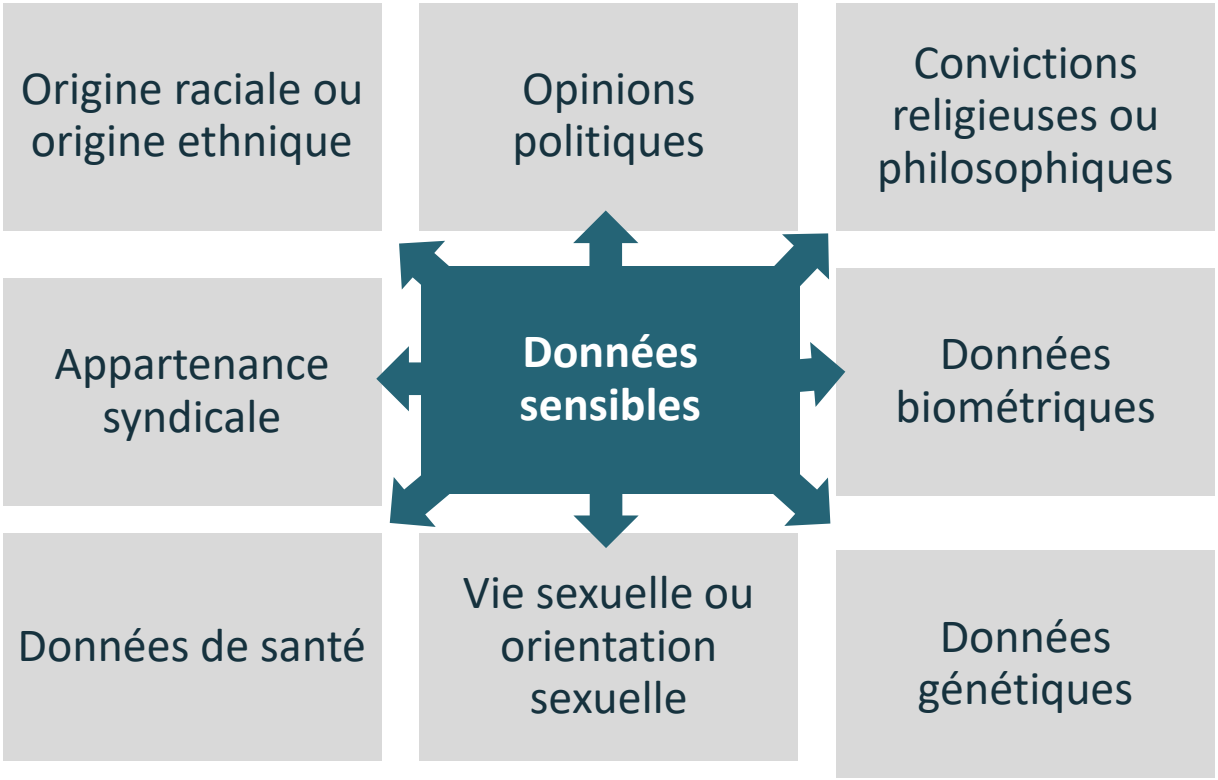
Les informations communiquées par l'usager afin de l'aider à accomplir un formulaire qui sera par la suite adressé à un organisme tiers n'ont pas vocation à être enregistrées par l'intervenant si elles ne lui servent pas dans le cadre de l'accompagnement et du suivi social et médico-social qu'il réalise.

Dans le secteur social et médico-social, de nombreux organismes utilisent des logiciels métiers pour assurer le suivi des familles et personnes accompagnées. Dans ce cadre, les professionnels doivent être vigilants à ce qu'ils écrivent dans les « **zones de commentaires libres** » Les commentaires ne doivent à cet égard pas être inappropriés ou subjectifs.[14] Ces recommandations sont aussi valables pour les documents en format papier. Elles renvoient plus généralement vers des principes juridiques et éthiques des écrits professionnels.

3.1 LE TRAITEMENT DES DONNÉES SENSIBLES

Certaines données personnelles sont particulièrement protégées, ce sont les **données sensibles** (art.9 du RGPD), auxquelles s'applique un régime de droit plus contraignant.

Il s'agit des informations qui sont susceptibles de révéler :



[14] Pour aller plus loin : https://www.cnil.fr/fr/zones-bloc-note-et-commentaires-les-bons-reflexes-pour-ne-pas-deraper

Par principe, les **données sensibles** font l'objet d'une **interdiction de traitement.** Néanmoins par **exception**, elles peuvent être traitées dans des circonstances bien précises :

- Lorsque la personne concernée a donné son **consentement explicite**[15] pour une ou plusieurs finalités spécifiques,

Dans le cadre de la gestion d'une crèche, ou de logements accompagnés et partagés, on pourra exceptionnellement collecter des informations relatives à la santé (allergie) ou des informations sur les pratiques religieuses, afin d'organiser les repas.

- Lorsque le traitement est nécessaire aux fins de la prise en charge sanitaire ou sociale, ou la gestion des systèmes et des services sanitaires ou sociaux sur la base du droit français (le Code de l'action sociale et des familles ou Code de la santé publique en l'occurrence),

Une notification MDPH pour un enfant en situation de handicap dans le cadre de la MJAGBF

- Lorsque le traitement est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice.

Dans le cadre de la mission légale des Udaf d'ester en justice pour défendre les intérêts des familles.

[15] Voir le focus sur le consentement de la personne concernée ci-après.

3.2 FOCUS SUR LE TRAITEMENT DES DONNÉES DE SANTÉ DANS LES SERVICES MJPM

D'une façon générale, les données de santé englobent toutes les **informations relatives à la santé physique ou mentale d'une personne.** (art. 4-15 du RGPD)

Le traitement de ces données nécessite une protection accrue. L'article 9 du RGPD pose un **principe d'interdiction de traitement de cette catégorie de données**, et une **série d'exceptions**.[16]

En application de **l'article L 1111-7 du Code de la santé publique,** modifié par l'ordonnance du 11 mars 2020[17] :

> Toute personne a accès à l'ensemble des informations concernant sa santé, notamment les résultats d'examen, comptes rendus de consultation, d'intervention, d'exploration ou d'hospitalisation, des protocoles et prescriptions thérapeutiques, des correspondances entre professionnels de santé.

Dans le cadre de leurs missions, les mandataires judiciaires ont parfois besoin de collecter et conserver les données de santé des personnes protégées :

- *Pour réaliser une démarche administrative auprès de la mutuelle de la personne protégée par exemple*
- *Pour répondre à son devoir d'information auprès de la personne protégée, afin que celle-ci puisse prendre la meilleure décision possible pour elle concernant la réalisation d'un acte de santé, c'est-à-dire de la manière la plus éclairée. Le MJPM doit conserver certaines données afin d'adapter les informations transmises à la personne protégée en fonction de sa situation personnelle. (art. 457-1 du code civil). La conservation des données permet également au MJPM de rendre compte de l'accomplissement de ses missions au juge.*
- *Pour autoriser un acte de santé. En effet, selon l'article L 1111-4 du CSP : lorsque la personne protégée bénéficiaire d'une mesure de protection juridique avec représentation relative à la personne, n'est pas en mesure de donner son consentement, « il appartient à la personne chargée de la mesure de protection juridique avec représentation relative à la personne de donner son autorisation en tenant compte de l'avis exprimé par la personne protégée »*

Aussi pour répondre à leurs missions et conformément aux dispositions de l'article L1111-2 du CSP, les mandataires judiciaires peuvent être informés par les professionnels de santé

[16] L'article 9.2 points a à j du RGPD prévoit 10 cas où le traitement de données de santé est autorisé.
[17] Entrée en vigueur le 1er octobre 2020

dans certaines conditions et selon le mandat confié par le juge, des données de santé des personnes qu'ils accompagnent :

- lorsque la personne bénéficie d'une mesure de protection avec représentation relative à la personne, le protecteur doit également avoir accès à ces informations ;
- lorsque la personne bénéficie d'une mesure de protection avec assistance relative à la personne, le protecteur peut avoir accès aux informations, si la personne protégée y consent expressément ;
- la personne chargée d'une mesure portant uniquement sur la protection relative aux biens ne peut pas accéder au dossier médical de la personne protégée.

Ainsi, la collecte des données de santé ne peut intervenir que dans deux cas :

- si le mandat confié par le juge prévoit une représentation à la personne ;
- si le mandat prévoit une assistance à la personne, mais, dans ce cas, uniquement s'il y a accord de la personne protégée.

Une fois ces données récoltées, il convient de bien respecter les conditions de partage de ces informations avec les autres professionnels.

En effet, conformément à l'**article L. 1110-4 du CSP**[18], le MJPM « *peut échanger avec un ou plusieurs professionnels identifiés des informations relatives à une même personne prise en charge à condition* ***qu'ils participent tous à sa prise en charge*** *et que ces informations soient* ***strictement nécessaires à la coordination ou la continuité des soins, à la prévention ou à son suivi médico-social ou social*** ».

Il convient de distinguer deux situations :

- **lorsque le MJPM transmet ces informations au sein du service PJM :** les informations transmises par la personne protégée sont réputées confiées à l'ensemble de l'équipe (*article L. 1110-4 II. du CSP*). Le MJPM peut donc consigner et transmettre à son équipe les informations strictement nécessaires à la prise en charge de la personne protégée ;
- **lorsque le MJPM transmet des informations à des professionnels du secteur sanitaire, social et médico-social extérieurs au service.** Il doit préalablement informer la personne protégée (*article L. 1110-4 III. et R. 1110-3 du CSP*).

[18] Cet article rappelle le droit au respect de la vie privée des personnes et encadre la question du partage des informations personnelles entre professionnels du secteur sanitaire, social et médico-social (dont font partie les services de protection juridique des majeurs)

Il ne peut communiquer que des informations répondant aux deux conditions suivantes (article R. 1110-1 du CSP) :

- informations « ***strictement nécessaires*** *à la coordination ou à la continuité des soins, à la prévention, ou au suivi médico-social ou social*» de la personne protégée ;
- **et** relevant du périmètre de ses missions auprès de la personne protégée (c'est-à-dire uniquement s'il y a une mesure de protection à la personne).

RECOMMANDATIONS

1. **Examiner le jugement pour déterminer l'étendue exacte de la mission confiée** par le juge : est-ce que la mission comporte la protection à la personne ? Si oui, quelle est l'étendue de la mission (assistance, représentation) ?

2. Cette analyse permet **d'identifier la base légale justifiant la collecte et le traitement de données de santé** :
   - En effet, pour que la collecte d'informations par le mandataire en matière de santé soit possible, il faut que le mandat confié prévoit expressément une mission de protection à la personne. De ce fait, le traitement des données se justifie pour permettre l'accompagnement ainsi que l'assistance et/ou la représentation de la personne protégée dans le cadre de sa protection à la personne.

3. **Apprécier, dans le cas où le mandat le prévoit, pour chaque personne protégée, la pertinence de collecter ou non des données de santé**. Toute collecte systématique des données de santé, ne tenant pas en compte de la singularité de chaque personne et de sa situation, serait disproportionnée et donc non conforme au RGPD.

4. **Attention**, même si les missions confiées dans le jugement autorisant la collecte des données relatives à la santé, **il convient d'informer les personnes protégées de leurs droits** conformément aux articles 13 et 14 du RGPD.

5. Comme indiqué plus haut, il est important de distinguer les informations à connaître, de celles à enregistrer. Lors d'échanges informels, les personnes protégées peuvent communiquer certaines informations à leur mandataire (ex : reprise d'alcool ou de drogue dans des situations d'addictologie, grossesse, cancer…). Ces informations **doivent être retranscrites avec pertinence, exactitude et uniquement dans le cas où la conservation est nécessaire et autorisé**, c'est-à-dire que si le jugement prévoit une mission de protection à la personne.

3.3 LE TRAITEMENT DES DONNÉES RELATIVES AUX INFRACTIONS, CONDAMNATIONS ET MESURES DE SÛRETÉ

Les infractions, les condamnations et les mesures de sûreté sont des données sensibles, dont le traitement doit être encadré et réservé à certains organismes.

Notons que la collecte et le traitement de ces données sont, par principe, **interdits.**

Conformément aux dispositions de l'article 46 de la loi Informatique et Libertés, les traitements de ces données ne peuvent être effectués que par :

- Les juridictions, autorités publiques, et personnes morales gérant un service public dans le cadre de leurs attributions légales **ainsi que les personnes morales de droit privé collaborant au service public de la justice et appartenant à des catégories dont la liste est fixée par les dispositions de l'article 76 du décret n° 2019-536 du 29 mai 2019.** A cet égard, sont notamment mentionnés les mandataires judiciaires à la protection des majeurs mentionnés à l'article L. 471-1 du code de l'action sociale et des familles ;

Les services MJPM, en fonction du mandat qui leur est confié, sont autorisés à prendre connaissance, par exemple, d'une convocation de garde à vue, une comparution immédiate de la personne protégée dans le cadre d'une tutelle ou curatelle.

- Les auxiliaires de justice pour exercer les missions que la loi leur confie ;
- Les personnes physiques ou morales victimes pour exercer une action en justice ;
- Les sociétés de perception et de répartition des droits d'auteur et organismes de défense du droit d'auteur.

4. LE PRINCIPE D'UNE DURÉE DE CONSERVATION LIMITÉE

Il est interdit de conserver des informations sur des personnes dans un fichier pour une durée indéfinie. Une durée de conservation précise doit être fixée, en fonction du type d'information enregistrée et de la finalité du fichier.[19]

La durée de conservation d'un document nécessaire à la gestion des affaires en cours ou utile à des fins juridiques est définie par la **durée d'utilité administrative (DUA).**[20]

« Dès leur création, les documents et les données doivent donc être intégrés dans une réflexion sur la gestion de l'information dont le cadre général est le passage des documents et données à travers trois âges successifs : les archives courantes, intermédiaires et définitives.

***Les archives courantes :** cet âge commence dès la création du document et dure tant que ce dernier est utilisé quasi-quotidiennement par le service qui l'a produit. De ce fait, le document doit être conservé dans son service d'origine et les données doivent être à disposition des agents chargés de leur traitement ; »*[21]

Recommandations

Pour les besoins de l'accompagnement social et médico-social des personnes**, la CNIL recommande que les données collectées ne soient pas conservées dans la base active au-delà de deux ans à compter du dernier contact émanant de la personne ayant fait l'objet de cet accompagnement** (ex. : dernier courriel ou courrier envoyé par la personne concernée, etc.), sauf dispositions législatives ou réglementaires contraires ou cas particulier.

*« **Les archives intermédiaires :** cet âge débute quand le document n'a plus d'usage fréquent (par exemple lorsque l'affaire qu'il concernait est terminée), mais que le service qui l'a produit peut encore en avoir besoin pour faire face à des recours, à d'éventuels délais de prescription (…). Dans le contexte numérique, cela implique une restriction de l'accès aux données afin de garantir leur sécurité et leur confidentialité »* [22]

[19] Pour aller plus loin : https://www.cnil.fr/fr/les-durees-de-conservation-des-donnees
[20] La durée de conservation de chaque document, ainsi que son sort final sont rappelés dans le protocole d'archivage des Udaf.
[21] Comité interministériel aux Archives de France, Référentiel général de gestion des archives, octobre 2013
[22] Idem

Recommandations

Dans le cadre de l'archivage intermédiaire, les données doivent être conservées sur un support distinct que celui de la base active. Un tri doit aussi être préalablement opéré entre les données qui doivent être archivées et celles qu'il faut supprimer dans la mesure où elles n'ont plus d'utilité.

*« **Ces deux âges (archives courantes et archives intermédiaires) forment la DUA** durant laquelle les archives sont sous la responsabilité du service qui les a produites.*

***Les archives définitives** : certaines archives peuvent être conservées au-delà de leur DUA. Il s'agit des documents qui présentent un intérêt historique, scientifique, statistique ou public permanent, et qui doivent être conservés indéfiniment pour la connaissance de notre société par nos descendants…»*[23] D'autres documents sont dépourvus d'un tel intérêt et sont alors voués à la destruction.

Il est à noter que les règles relatives aux durées de conservations et aux sorts finaux sont les mêmes pour le traitement papier comme numérique. Le support n'impacte pas la nature des archives.

Par exemple, les documents comptables des bénéficiaires (factures, justificatifs de ressources...) ne doivent pas être conservés au-delà de 10 ans.

Pour les dossiers PJM : L'article 515 du code civil porte la prescription à 5 ans à compter de la fin de la mesure. Dans tous les cas, il convient de conserver une copie du dossier 5 ans à compter de la fin de la mesure et 10 ans si le dossier administratif est mélangé avec le dossier comptable.

En cas de mainlevée, les pièces rendues à la personne doivent faire l'objet d'une copie qui est placée dans le dossier.

En cas de décès, ces pièces pourront être confiées au notaire ou à la famille et feront également l'objet d'une copie placée dans le dossier.

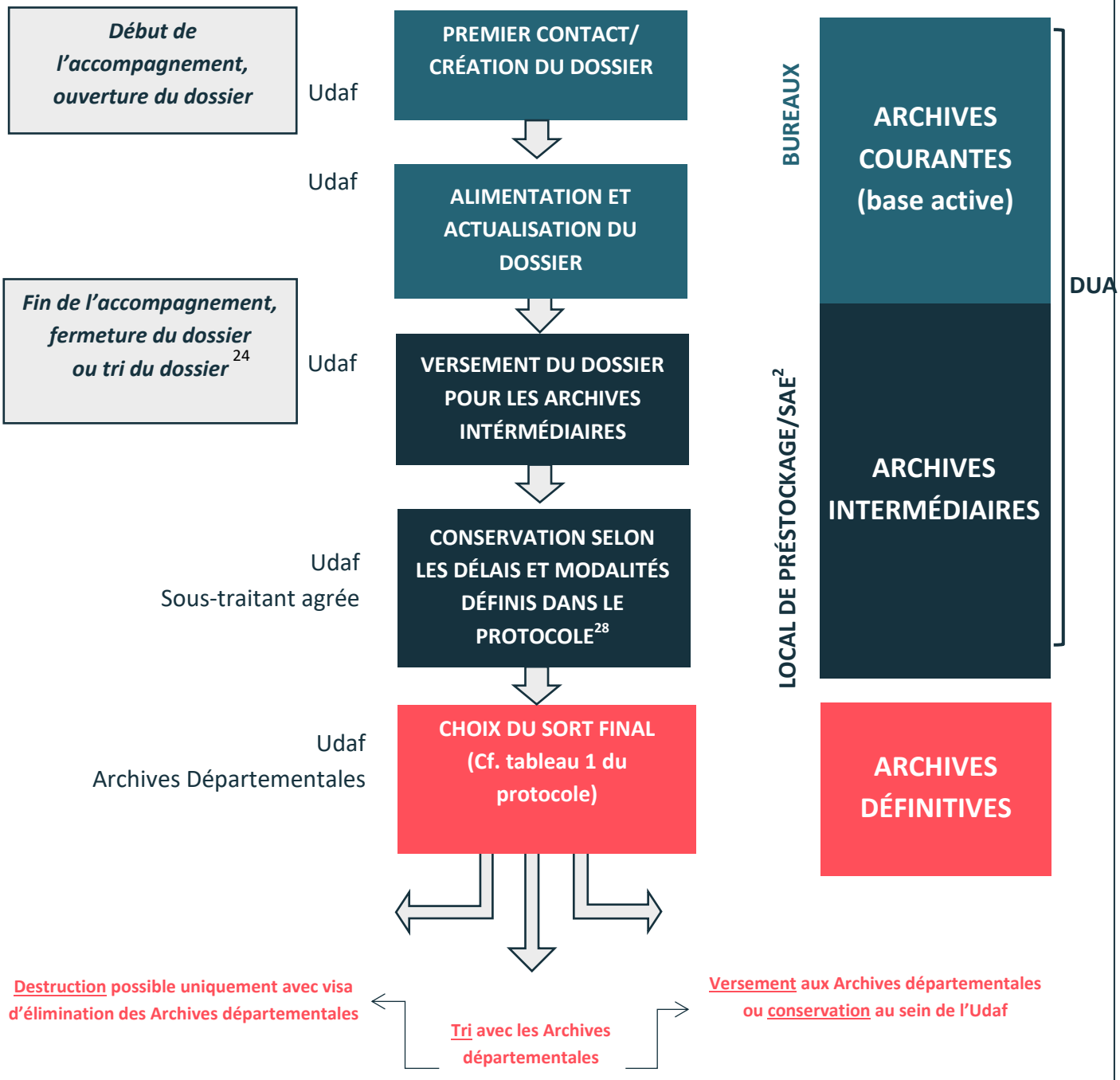
En cas de transfert de mesure, un tri du dossier doit être effectué afin de transmettre les documents jugés essentiels au nouveau mandataire. Par sécurité, il est préconisé de conserver des copies au moins durant 5 ans après clôture du mandat. Si le dossier comptable est mélangé avec le dossier administratif, il faut conserver l'ensemble 10 ans après clôture du mandat.

Recommandations

Il est fortement conseillé aux associations de se rapprocher de leurs Archives Départementales pour définir les modalités de tri, de versement et de destruction des archives.

[23] Comité interministériel aux Archives de France, Référentiel général de gestion des archives, octobre 2013

Cycle de vie d'un dossier d'une personne ou d'une famille accompagnée dans une Udaf



Source : Unaf, 2021

[24] Dans les cas où une personne ou une famille est accompagnée depuis plusieurs années par l'Udaf, il est possible de verser aux archives intermédiaires des éléments de son dossier jugés anciens et non nécessaires à l'accompagnement quotidien.
[25] Système d'archivage électronique
[26] Cf. protocole sur le portail France Archives : https://francearchives.fr/fr/circulaire/DGPA_SIAF_2021_002?j

FOCUS : FAIRE APPEL À UN PRESTATAIRE DE TIERS-ARCHIVAGE AGRÉE

Voir les références juridiques à la fin du document

Concernant les archives publiques, si un responsable de traitement souhaite faire appel à un prestataire de tiers-archivage pour stocker ses archives intermédiaires, celui-ci doit être obligatoirement agréé. Certaines sociétés ou dépôts ne sont en effet pas recommandés pour le stockage des archives publiques ; c'est le sens des recommandations du Service interministériel des archives de France (SIAF).

Il convient de :

- déclarer le dépôt à l'administration des archives ;
- rédiger un cahier des charges en s'appuyant sur les exigences requises pour le contrat de dépôt ;
- s'informer sur les prestataires agréés ;
- vérifier si le prestataire dispose bien d'une certification pour l'hébergement de données de santé, le cas échéant ;
- rédiger un contrat de dépôt[27] qui doit obligatoirement être transmis aux Archives départementales avant sa signature.

Attention toutefois à ne pas stocker chez des prestataires même agréés, des archives ayant passé leur DUA car les prestataires de tiers-archivage privés n'ont pas le droit de conserver des archives publiques considérées comme historiques.

En pratique, dès lors qu'un dossier PJM dont le mandat à l'Udaf est clos depuis plus de cinq ans, il faudra, suivant l'accord de tri défini avec le directeur/trice des Archives départementales, soit :

- *rapatrier le dossier à l'Udaf et le préparer pour le verser aux Archives départementales,*
- *soit le détruire après l'obtention de l'autorisation de ces dernières.*

Recommandations

Voir la liste des sous-traitants agréés dans la rubrique « Pour aller plus loin » à la fin du présent document.

[27] Article R 212-21 et 22 du Code du patrimoine : Ce contrat doit contenir la nature et le support des archives déposées, la description des prestations réalisées et des moyens mis en œuvre, ainsi que les dispositifs de communication matérielle, d'accès et de restitution des archives, les conditions de recours à des sous-traitants, les polices d'assurance, la durée du contrat et les conditions de renouvellement.

5. LE PRINCIPE DE CONFIDENTIALITÉ

5.1 DESTINATAIRES DES DONNÉES ET ACCÈS AUX INFORMATIONS

LES PERSONNES ACCÉDANT AUX DONNÉES POUR LE COMPTE DU RESPONSABLE DE TRAITEMENT

La confidentialité est intrinsèquement liée à l'accès aux données, c'est une garantie nécessaire et conjointe de la sécurité que doit apporter le responsable de traitement[28].

Seules les personnes habilitées au titre de leurs missions ou de leurs fonctions peuvent accéder aux données à caractère personnel traitées, et ce dans la stricte limite de leurs attributions respectives et de l'accomplissement de ces missions et fonctions. Il peut s'agir, par exemple, des professionnels et de tout membre du personnel de l'établissement, du service concourant à une ou plusieurs des finalités susvisées, dans la limite de leurs attributions respectives et des règles encadrant le partage et l'échange d'informations.

Aussi, les données personnelles ne peuvent être rendues accessibles qu'aux seules personnes habilitées à en connaitre par le responsable de traitement, au regard de leurs attributions.

Le personnel des services ressources humaines, de communication, d'action familiale etc. ne doit pas avoir accès aux dossiers des personnes accompagnées.

Les personnes habilitées à accéder aux dossiers et les critères de choix doivent être clairement énoncés, par le responsable de traitement.

Dans le cadre de l'informatisation, il faut définir les profils et les droits souhaités, afin que chaque professionnel puisse lire et/ou modifier l'information qui le concerne, en fonction des pratiques et besoins.

[28] Article 35 de la Loi I&L

LES DESTINATAIRES DES DONNÉES PERSONNELLES

Le RGPD définit les destinataires comme « *tout organisme qui reçoit la communication des données* ». Peuvent **notamment** être destinataires des données :

- s'agissant de données traitées par une personne soumise au secret médical/professionnel, les professionnels et tout membre du personnel membre de la même équipe de soins ou non, sous réserve dans ce dernier cas du recueil du consentement de la personne concernée conformément aux dispositions de l'article L. 1110-4 du CSP, qui participent à une ou plusieurs des finalités susvisées ;
- les personnes appelées à intervenir dans la gestion financière et successorale du patrimoine de la personne ayant fait l'objet d'un accompagnement et d'un suivi ;
- les organismes instructeurs et payeurs de prestations sociales ;
- les organismes financeurs et gestionnaires, s'agissant exclusivement de données préalablement anonymisées, à l'exception de ceux autorisés par une disposition légale ou réglementaire à obtenir la communication de données à caractère personnel des personnes accompagnées.

LES TIERS AUTORISES

Des organismes qualifiés de « tiers autorisés » [29] peuvent aussi accéder à certaines données contenues dans les dossiers des personnes accompagnées, comme par exemple les organismes de sécurité sociale dans le cadre de la lutte contre la fraude sociale ou l'administration fiscale.

Il est donc nécessaire d'informer les personnes que leurs données peuvent être accessibles à des **tiers autorisés.** Lorsqu'un tiers autorisé demande l'accès aux informations d'une personne contenues dans un fichier, l'organisme concerné est tout à fait en droit de demander sur quel texte légal il se fonde pour justifier sa demande. De plus, le tiers autorisé n'a pas à avoir accès à tout le fichier.

LES SOUS-TRAITANTS

Le responsable de traitement qui souhaite avoir recours à un sous-traitant doit veiller à ne faire appel qu'à des organismes présentant des garanties suffisantes. Un contrat définissant les caractéristiques du traitement ainsi que les différentes obligations des parties en matière de protection des données doit être établi entre elles (article 28 du RGPD).

Recommandations

- → Vous pouvez vous appuyer sur un exemple de contrat avec les sous-traitants sur le site de la Cnil : https://www.cnil.fr/fr/sous-traitance-exemple-de-clauses et vous référer à l'annexe 3.
- → Vous pouvez aussi consulter le guide du sous-traitant édité par la CNIL : https://www.cnil.fr/sites/default/files/atoms/files/rgpd-guide_sous-traitant-cnil.pdf

[31] Pour aller plus loin : https://www.cnil.fr/cnil-direct/question/quest-ce-quun-tiers-autorise?visiteur=pro

5.2 LE SECRET PROFESSIONNEL

Le droit à la confidentialité des personnes se traduit en miroir pour les professionnels par l'obligation de discrétion, doublée du secret professionnel. *« Les informations détenues par les professionnels sont ainsi confidentielles et ne doivent pas être dévoilées sans l'autorisation de la personne concernée, à l'exception des informations qui sont tenues d'être révélées. (…) Tous les intervenants (professionnels, bénévoles, stagiaires, etc.) sont soumis à un devoir de discrétion et certains sont de plus, selon leur mission, fonction ou profession, tenus par la loi au secret professionnel, dont la transgression est pénalement sanctionnée.»*[30]

> *Article L.1110-4 du Code de santé publique :*
> *Toute personne prise en charge par […] un professionnel du secteur médico-social ou social ou un établissement ou service social et médico-social […] a droit au respect de sa vie privée et du secret des informations la concernant.*
> *Excepté dans les cas de dérogation expressément prévus par la loi, ce secret couvre l'ensemble des informations concernant la personne venues à la connaissance du professionnel, de tout membre du personnel de ces établissements, services ou organismes et de toute autre personne en relation, de par ses activités, avec ces établissements ou organismes.*

Par conséquent, lorsque les professionnels sont tenus à une obligation du secret professionnel de par leur état, leur statut, leur profession (exemple : professionnels de santé, assistants de service social), **leur mission ou leur fonction** (intervention dans la prise en charge médico-sociale ou sociale en application de l'article L.1110-4 du Code de la santé publique), **toute violation les expose à des sanctions pénales**[31]. Il en va ainsi notamment lorsque les modalités de partage d'informations à caractère secret définies par la loi ne sont pas respectées. Cela concerne tout le secteur sanitaire mais aussi le secteur social et médico-social.[32]

[30] Haut Conseil du Travail Social - Commission éthique et déontologie du travail. *Les informations à caractère personnel concernant les personnes accompagnées : des données à protéger et parfois à partager.* 2017.
[31] L'article 226-13 du Code pénal stipule : « *La révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire, est punie d'un an d'emprisonnement et de 15 000 euros d'amende.* »
[32] Décret n°2016-994 du 20 juillet 2016 relatif aux conditions d'échange et de partage d'informations entre professionnels de santé et autres professionnels des champs social et médico-social et à l'accès aux informations de santé à caractère personnel.

5.3 LE PARTAGE DE DONNÉES À CARACTÈRE SECRET

Le « secret partagé » n'existe pas dans la loi. C'est là un abus de langage commun, risqué dans la mesure où il pourrait laisser supposer que sous son couvert, on peut tout se dire, favorisant ainsi la mise en œuvre de pratiques que ni la loi ni la déontologie ne sauraient autoriser. En réalité, ce qu'autorise la loi, c'est le partage de certaines informations à caractère secret dans des conditions et pour des finalités bien définies.

Article L.1110-4 du Code de Santé Publique :

II. Un professionnel peut échanger avec un ou plusieurs professionnels identifiés des informations relatives à une même personne prise en charge, à condition qu'ils participent tous à sa prise en charge et que ces informations soient strictement nécessaires à la coordination ou à la continuité des soins, à la prévention ou à son suivi médico-social et social.

III.- Lorsque ces professionnels appartiennent à la même équipe de soins[33] […], ils peuvent partager les informations concernant une même personne qui sont strictement nécessaires à la coordination ou à la continuité des soins ou à son suivi médico-social et social. Ces informations sont réputées confiées par la personne à l'ensemble de l'équipe de soins.

Le partage d'information à caractère secret, au sein des services sociaux et médico-sociaux, est indispensable à leur bon fonctionnement et facilite la qualité de l'accompagnement des personnes**. Ce partage d'information est encadré afin de garantir le respect de la vie privée et préserver la confiance entre les professionnels et les personnes accompagnées.**

C'est la loi du 26 janvier 2016 de modernisation de notre système de santé[34] qui prévoit notamment les règles applicables.

[33] L'équipe de soin ne concerne pas seulement le secteur sanitaire. Elle est définie à l'article L. 1110-12 du CSP *: « l'équipe de soins est un ensemble de professionnels qui participent directement au profit d'un même patient à la réalisation d'un acte diagnostique, thérapeutique, de compensation du handicap, de soulagement de la douleur ou de prévention de perte d'autonomie, ou aux actions nécessaires à la coordination de plusieurs de ces actes. »*

[34] Et son décret d'application 2016-994 relatif aux conditions d'échange et de partage d'informations entre professionnels de santé et autres professionnels des champs social et médico-social et à l'accès aux informations de santé à caractère personnel ainsi que l'article L 1110-4.II du Code de la santé publique (CSP).

Les professionnels concernés par le partage des informations à caractère secret sont notamment :

- → les professionnels de santé qui sont mentionnés dans le Code de la santé publique ;
- → les autres professionnels pour lesquels une liste précise a été établie[35]. On y trouve pour exemple, les psychologues, les assistantes sociales, les éducateurs, les personnels pédagogiques des accueils collectifs de mineurs, les mandataires judiciaires à la protection des majeurs et délégués aux prestations familiales, etc.

Le partage d'information à caractère secret doit donc rester limité à ce qui est **pertinent**, **nécessaire** et **suffisant** à la réalisation des objectifs déterminés et des missions des professionnels de santé ou du secteur médico-social ou social. Ainsi, sauf cas particuliers, le partage des informations collectées devrait notamment respecter les principes suivants :

- les informations échangées ne doivent servir qu'à évaluer la situation de la personne ou de la famille concernée afin de déterminer les actions à mettre en œuvre ;
- ces échanges d'informations doivent en outre être strictement limités à l'accomplissement des missions de l'organisme ou du service mettant en œuvre le traitement ;
- ils ne peuvent pas porter sur l'ensemble des informations dont les intervenants sont dépositaires mais doivent être limités à celles nécessaires à l'accompagnement et au suivi des personnes, dans le respect de leur vie privée ;
- les échanges doivent être réalisés dans les conditions fixées par les textes législatifs et réglementaires.

Dans tous les cas, ces professionnels doivent **informer les personnes** que certaines de leurs informations personnelles seront éventuellement transmises à des organismes ou des professionnels extérieurs.

Recommandations

- → Avant de communiquer des informations, il convient donc de se poser plusieurs questions :
  - Pour quelles raisons je dois transmettre ces informations ?
  - La demande de communication est-elle légitime ? Est-elle nécessaire à la continuité du suivi social ou médico-social ?
  - Quelles sont les informations à communiquer ?
  - Est-ce que j'ai informé la personne de mon intention de partager des informations avec d'autres professionnels ou organismes ?

[35] Article R 1110-2 du CSP

Le respect des droits de la personne, de sa dignité et de son intérêt doit être au centre des préoccupations de tout intervenant amené à partager des informations qui, même recueillies dans le cadre de son exercice professionnel, n'appartiennent qu'à la personne concernée.

Attention, les proches demandent souvent des informations au sujet de la personne accompagnée. Le professionnel doit leur rappeler son obligation de confidentialité et les informer de leurs droits (notamment la possibilité de déposer une requête au juge des contentieux de la protection, dans le cadre d'une mesure de protection par exemple).

6. LE PRINCIPE DE SÉCURITÉ

Voir les références juridiques à la fin du document

Le responsable du traitement doit garantir la sécurité des informations qu'il détient. Il doit en particulier veiller à ce que seules les personnes autorisées aient accès à ces informations (art. 32 du RGPD).

De même, l'article 34 de la loi I&L impose au responsable de traitement

« de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès. […] » ***sous peine de sanctions administratives (sanctions CNIL) et/ou pénales (peines de 5 ans d'emprisonnement et de 300.000 euros*** *prévues par l'article 226-17 du Code pénal).*

Recommandations

La gestion des documents, quel que soit leur support (papier ou numérique), s'appuie sur la mise en œuvre d'une sécurité physique des locaux de stockage des documents papier, du traitement de numérisation et du stockage des documents numériques.
Cela peut se résumer aux pratiques recommandées, notamment par la norme NF ISO/IEC 27001, valables pour la sécurité physique et informatique :

- contrôle d'accès ;
- détection d'intrusion ;
- détection et extinction incendie ;
- détection et prévention de dégâts des eaux ;
- détection et prévention des risques liés aux rongeurs ;
- détection et prévention des risques liés aux crues ;
- double sauvegarde des fichiers sur sites distants ;
- avoir défini un Plan de Continuité d'Activité (PCA) ;
- avoir défini une Politique de sécurité informatique.

6.1 MISE EN PRATIQUE DES RÈGLES DE SECURITÉ INFORMATIQUE

Voici une check-list de 12 règles, rédigée par l'ANSSI[36] et la CPME[37] pour la sécurité des systèmes d'information, extraite de leur *Guide des bonnes pratiques de l'informatique*[38] :

RECOMMANDATIONS	ILLUSTRATIONS
Choisir avec soin ses mots de passe	• Définissez un identifiant (login) unique à chaque utilisateur • Adoptez une politique de mot de passe utilisateur conforme aux recommandations CNIL • Obligez l'utilisateur à changer son mot de passe après réinitialisation • Limitez le nombre de tentatives d'accès à un compte • Les mécanismes d'attribution des mots de passe doivent être automatiques et s'auto-effacer après 24 heures. • Proscrivez les pratiques dangereuses de copier-coller des mots de passe. • Proscrivez l'envoi des mots de passe par messagerie
Mettre à jour régulièrement vos logiciels et prévoir la sauvegarde et la continuité d'activité (PCA)	• Effectuez des sauvegardes régulières • Stockez les supports de sauvegarde dans un endroit sûr • Prévoyez des moyens de sécurité pour le convoyage des sauvegardes • Prévoyez et testez régulièrement la continuité d'activité
Bien connaître ses utilisateurs	• Définissez des profils d'habilitation : un mécanisme de gestion des habilitations est mis en œuvre et régulièrement mis à jour pour garantir que les personnes habilitées n'ont accès qu'aux seules données nécessaires à la réalisation de leurs missions • Supprimez les permissions d'accès obsolètes • Réalisez une revue annuelle des habilitations
Effectuer des sauvegardes régulières des serveurs	• Installez sans délai les mises à jour critiques • Assurez une disponibilité des données

[36] ANSSI : Agence nationale de la sécurité des systèmes d'information
[37] CPME : confédération des petites et moyennes entreprises
[38] Cf. https://www.ssi.gouv.fr/guide/guide-des-bonnes-pratiques-de-linformatique/

RECOMMANDATIONS	ILLUSTRATIONS
Sécuriser l'accès Wi-Fi de votre entreprise	• Mettez en œuvre le protocole WPA2 ou WPA2-PSK pour les réseaux Wi-Fi
Être aussi prudent avec son ordiphone (smartphone) ou sa tablette qu'avec son ordinateur	• Prévoyez une procédure de verrouillage automatique de session • Utilisez des antivirus régulièrement mis à jour • Installez un « pare-feu » (firewall) logiciel • Recueillez l'accord de l'utilisateur avant toute intervention sur son poste pour le sécuriser • Prévoyez des moyens de chiffrement des équipements mobiles et privilégiez des téléphones à usage professionnel • Faites des sauvegardes ou synchronisations régulières des données • Exigez un secret pour le déverrouillage des smartphones
Protéger ses données lors de ses déplacements	• Limitez les flux réseau au strict nécessaire • Sécurisez les accès distants des appareils informatiques nomades par VPN
Être prudent lors de l'utilisation de sa messagerie et sécuriser les échanges	• Chiffrez les données très confidentielles avant leur envoi (utilisation de la signature électronique) • Assurez-vous qu'il s'agit du bon destinataire • Transmettez les données confidentielles via un canal différent (extranet avec une utilisation temporaire et sécurisée) • Ne pas transmettre des fichiers contenant des données personnelles en clair *via* des messageries grand public[39]
Être vigilant avec Internet	• Vérifiez qu'aucun mot de passe ou identifiant ne passe dans les url • Contrôlez que les entrées des utilisateurs correspondent à ce qui est attendu • Mettez un bandeau de consentement pour les cookies non nécessaires au service • Proscrivez ou restreignez le paiement en ligne
Séparer les usages personnels des usages professionnels et sensibiliser les utilisateurs	• Informez et sensibilisez les personnes manipulant les données • Rédigez une charte informatique et lui donner une force contraignante • Les accès aux lieux de stockage et aux lieux de numérisation doivent être protégés et n'être accessibles qu'aux personnes habilitées disposant d'un droit d'accès. Leurs personnels doivent avoir suivi les formations élémentaires sur la sécurité et avoir signé un engagement de confidentialité.

[39] *Cf*. p25 du guide de la CNIL relatif à la sécurité des données personnelles : https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle.pdf

RECOMMANDATIONS	ILLUSTRATIONS
Prendre soin de ses informations personnelles, professionnelles et de son identité numérique	• Limitez l'accès aux outils et interfaces d'administration aux seules personnes habilitées • Les accès aux outils et interfaces d'administration font l'objet d'une traçabilité afin de permettre la détection d'éventuelles tentatives d'accès frauduleux ou illégitimes
Gérer la sous-traitance	• Gérez vos sous-traitants en leur demandant de prévoir une clause spécifique dans leur contrat en conformité avec le RGPD • Prévoyez les conditions de restitution et de destruction des données • Assurez-vous de l'effectivité des garanties prévues (audits de sécurité, visites, etc.)
Encadrer les développements informatiques	• Proposez des paramètres respectueux de la vie privée aux utilisateurs finaux • Évitez les zones de commentaires ou encadrez-les strictement • Testez sur des données fictives ou anonymisées • Évitez de mettre en place un moteur de recherche sur l'ensemble des outils internes accessibles à tous
Archiver de manière sécurisée	• Mettez en œuvre des modalités d'accès spécifiques aux données archivées avec un unique profil habilité • Détruisez les archives obsolètes de manière sécurisée après autorisation de l'autorité des archives publiques (Archives départementales) • Conservez les traces des destructions
Encadrer la maintenance et la destruction des données	• Enregistrez les interventions de maintenance dans une main courante • Encadrez par un responsable de l'organisme les interventions par des tiers • Effacez les données de tout matériel avant sa mise au rebut
Renforcer la sécurité des locaux hébergeant les serveurs informatiques et les matériels réseaux.	• Installez des alarmes anti-intrusion et les vérifier périodiquement. • Mettez en place des détecteurs de fumée ainsi que des moyens de lutte contre les incendies, et les inspecter annuellement. • Protégez les clés permettant l'accès aux locaux et les codes d'alarme. • Protégez physiquement les matériels informatiques par des moyens spécifiques (système anti-incendie dédié, surélévation contre d'éventuelles inondations, redondance d'alimentation électrique et/ou de climatisation, etc.).[40]

[40] Cf. p26 du guide de la CNIL relatif à la sécurité des données personnelles : https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle.pdf

6.2 FOCUS SUR LA TRACABILITÉ DES ACCÈS

Selon la CNIL[41], il faut tracer les accès et prévoir des procédures pour gérer les incidents afin de pouvoir réagir en cas de violation de données (atteinte à la confidentialité, l'intégrité ou la disponibilité).

Pour ce faire, un dispositif de gestion des traces et des incidents doit être mis en place. Celui-ci doit enregistrer les évènements pertinents et garantir que ces enregistrements ne peuvent être altérés.

Le dispositif est généralement mis en place avec l'éditeur de logiciel.

- **Prévoir un système de journalisation** (c'est-à-dire un enregistrement dans des « fichiers journaux » ou « logs ») des activités des utilisateurs, des anomalies et des événements liés à la sécurité :
  - → ces enregistrements doivent conserver les évènements sur une période glissante ne pouvant excéder six mois (sauf obligation légale, ou risque particulièrement important) ;

La durée d'effacement des logs doit être travaillée avec le prestataire.

  - → la journalisation doit concerner, au minimum, les accès des utilisateurs en incluant leur identifiant, la date et l'heure de leur connexion, et la date et l'heure de leur déconnexion ;
  - → dans certains cas, il peut être nécessaire de conserver également le détail des actions effectuées par l'utilisateur, les types de données consultées et la référence de l'enregistrement concerné.

- **Informer les salariés et bénévoles** de la mise en place d'un tel système et des finalités, après information et consultation des représentants du personnel.

Inscrire cette information dans une charte informatique[42]

- **Protéger les équipements de journalisation et les informations journalisées** contre les accès non autorisés, notamment en les rendant inaccessibles aux personnes dont l'activité est journalisée.

[41] https://www.cnil.fr/fr/securite-tracer-les-acces-et-gerer-les-incidents
[42] Voir les conseils de la CNIL à ce propos : https://www.cnil.fr/fr/securite-informatique-sensibiliser-les-utilisateurs

- **Etablir des procédures détaillant la surveillance de l'utilisation du traitement et examiner périodiquement les journaux d'événements** pour y détecter d'éventuelles anomalies.

Recommandations

Demander au responsable informatique de vérifier régulièrement l'absence d'intrusion d'une personne non autorisée.

Recommandations

Cette protection renvoie à la gestion des habilitations et au droit d'utilisation. Il convient de s'assurer de manière régulière que les habilitations sont conformes à la réglementation.

- **S'assurer que les sous-traitants notifient, dans les plus brefs délais, toute anomalie ou tout incident de sécurité** au responsable de traitement.

- **Notifier toute violation de données à caractère personnel au DPO et à la CNIL** et, sauf exception prévue par le RGPD, aux personnes concernées pour qu'elles puissent en limiter les conséquences.

Recommandations

Si l'association a subi une violation de données (des données personnelles ont été, de manière accidentelle ou illicite, détruites, perdues, altérées, divulguées ou si vous avez constaté un accès non autorisé à des données), alors il convient de le **signaler à la CNIL dans les 72 heures,** si cette violation est susceptible de représenter un risque pour les droits et libertés des personnes concernées.

Cette notification s'effectue en ligne sur le site de la CNIL : https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles

Si ces risques sont élevés pour ces personnes, vous devez les en informer.

Pour plus d'informations, voir l'article 33 du RGPD sur la notification à l'autorité de contrôle d'une violation de données à caractère personnel et l' article 34 du RGPD sur la communication à la personne concernée d'une violation de données à caractère personnel.

CHAPITRE III

L'INFORMATION ET LES DROITS DES PERSONNES

« *Toute personne dispose du droit de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant, dans les conditions fixées par la présente loi* ». Article 1er alinéa 3 de la loi I&L

Le recueil et le traitement de données personnelles sont nécessaires dans le cadre de l'exercice des missions des associations. Toutefois, ils engendrent une importante responsabilité du fait des risques qu'ils font encourir sur la vie privée des personnes concernées. Si ces données peuvent être utiles pour la qualité de l'accompagnement et contribuer à la continuité des parcours, une atteinte à la sécurité de ces données est aussi susceptible de causer des préjudices aux personnes concernées.

Les données gérées par les services sociaux et médico-sociaux ne leur appartiennent pas. Elles sont confiées par les personnes aux professionnels et ce le temps de l'accompagnement.

La loi 2002-2 du 2 janvier 2002 a consacré et renforcé des droits aux personnes accompagnées et accueillies lesquels sont énoncés à l'article L 311-3 du CASF. Huit outils[43] ont été créés pour les garantir. En 2018, ils ont été déclinés de façon spécifique pour les MJPM.[44] D'autres textes juridiques promeuvent aussi des droits des personnes concernées (CASF, RGPD, loi relative à l'informatique, aux fichiers et aux libertés, etc.) Parmi tous ces droits, sept seront abordés dans cette partie :

Le droit à l'information	**Le droit d'accès**	**Le droit de rectification**
Le droit d'opposition	**Le droit à l'oubli**	**Le droit à la limitation de traitement**
	Le droit à la portabilité des données	

[43] Le livret d'accueil, le règlement de fonctionnement, la charte des droits et libertés de la personne accueillie, le projet de service, le contrat de séjour ou le DIPEC, le conseil de vie sociale ou autre forme de participation des usagers, la personne qualifiée et la personne de confiance (loi ASV du 28 décembre 2015).

[44] Le document individuel de protection, la notice d'information, la charte des droits et libertés de la personne majeur protégée, modèle de récépissé (Décret n° 2008-1556 du 31 décembre 2008 relatif aux droits des usagers des mandataires judiciaires à la protection des majeurs et des délégués aux prestations familiales)

FOCUS : DES DISPOSITIONS QUI S'APPLIQUENT À TOUS LES DROITS, À LA CROISÉE DU RGPD ET DU RÉGIME DES ARCHIVES PUBLIQUES

LE DÉLAI DE RÉPONSE À UNE DEMANDE RELATIVE À L'EXERCICE D'UN OU DE PLUSIEURS DROITS

Lorsqu'une personne accompagnée formule une demande relative à l'exercice d'un ou de plusieurs droits (droit à l'oubli, d'opposition, de rectification, d'accès,…), le responsable de traitement doit fournir à la personne concernée « *des informations sur les mesures prises […] dans les meilleurs délais et en tout état de* ***cause dans un délai d'un mois à compter de la réception de la demande****. Au besoin, ce délai peut être prolongé de deux mois, compte tenu de la complexité et du nombre de demandes.* ».(art 12 du RGPD) Le cas échéant, le responsable de traitement devra justifier la raison d'un délai supplémentaire. En l'absence de réponse, la personne pourra porter plainte auprès de la CNIL (cf. les voies de recours possibles ci-après).

DES DÉROGATIONS AUX DROITS DES PERSONNES SUR LES ARCHIVES PUBLIQUES

Conformément au protocole d'archivage, les Udaf sont **tenues de verser certains documents – considérés comme des archives publiques – aux Archives Départementales,** et ce **à des fins archivistiques**, de recherches scientifiques, historiques ou statistiques. **Les services publics d'archives peuvent alors déroger aux droits des personnes[45], lorsque cela est nécessaire,** pour conserver et mettre à disposition des chercheurs des archives publiques.[1]

Il s'agit là des dérogations au droit à l'oubli, au droit d'opposition, au droit de rectification, au droit à la limitation du traitement, au droit à la portabilité des données et au droit d'accès de la personne concernée. Cette dérogation vaut aussi pour l'obligation de notification en ce qui concerne la rectification ou l'effacement des données ou la limitation du traitement.

Ces dérogations aux droits des personnes ont été obtenues en contrepartie de conditions et garanties appropriées, que l'on retrouve dans un riche corpus normatif.[1] (cf. les conditions d'accès aux archives publiques ci-après)

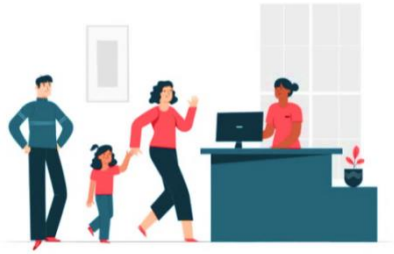
Recommandations

Pour aller plus loin, vous pouvez aussi consulter le guide de la CNIL : https://www.cnil.fr/sites/default/files/atoms/files/guide_durees_de_conservation.pdf

[45] Ces dérogations s'appliquent également aux archives définitives, encore conservées par les producteurs, dans l'attente de leur versement aux Archives départementales.

1. LE DROIT A L'INFORMATION

Voir les références juridiques à la fin du document



Le droit à l'information est un droit fondamental qui s'applique pour tous les traitements de données à caractère personnel.

Les personnes doivent être informées de manière **claire, simple et complète**, de l'ensemble des mentions d'information visées par les dispositions de l'article 13 du RGPD :

- l'identité et les coordonnées de l'organisme collecteur, du responsable de traitement ;
- le contact du délégué à la protection des données ;
- les finalités du traitement ainsi que la base juridique du traitement ;
- les intérêts légitimes poursuivis par le responsable de traitement si le traitement s'appuie sur cette base juridique ;
- les destinataires des données personnelles ;
- la durée de conservation ;
- leurs droits (accès, modification, rectification, etc.).

Les personnes doivent savoir pourquoi le responsable de traitement collecte des données et comment il peut les utiliser.

Lorsque les données personnelles n'ont pas été collectées directement auprès de la personne concernée, alors il convient de fournir les mêmes informations listées ci-dessus ainsi que celles énoncées au sein de l'article 14 du RGPD.

Recommandations

→ Vous pouvez consulter des exemples de mentions d'informations disponibles sur le site de la Cnil : https://www.cnil.fr/fr/rgpd-exemples-de-mentions-dinformation

Pour les services MJPM, l'article 457-1 du Code civil énonce que la personne protégée a droit à une information complète et adaptée, afin de lui permettre de prendre seule les décisions la concernant lorsque son état le lui permet.
Pour le mineur, si le traitement des données n'est possible qu'avec l'autorisation des titulaires de l'autorité parentale[46], l'obligation d'information adaptée demeure.

[46] Sauf exception, dans le cadre de la protection de l'enfance par exemple

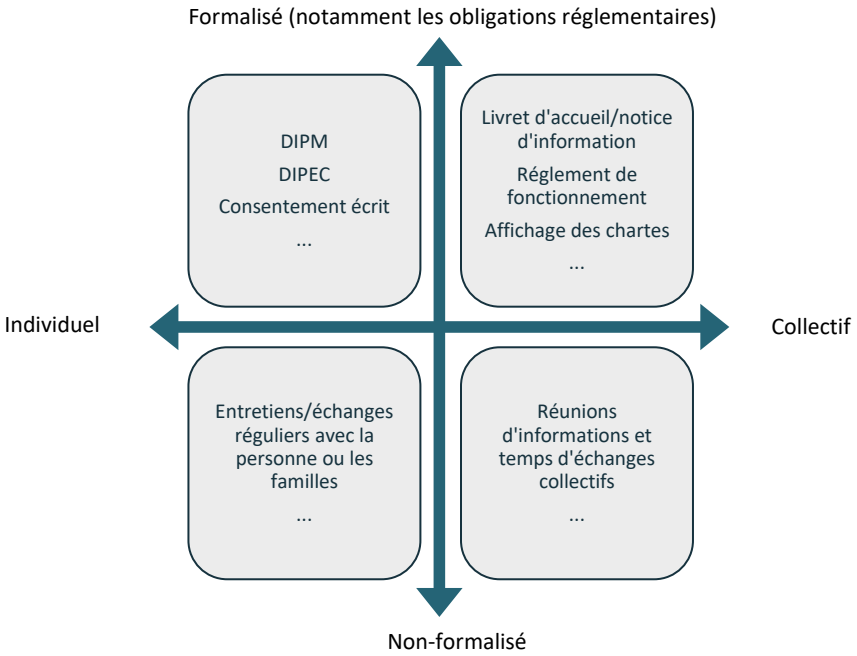
1.1 MODALITÉS DE TRANSMISSION DE L'INFORMATION

Si légalement l'information doit matériellement être transmise au plus tard au moment de l'accueil, par la remise du livret d'accueil/notice d'informations, tout événement ou évolution est l'occasion de réitérer une information ou de la mettre à jour :

- début de l'accompagnement, ouverture du dossier
- actualisation du projet personnalisé ;
- évolution des modalités d'accompagnement en lien avec celle de la situation de la personne ;
- identification des difficultés dans la relation personne/professionnel ;
- questionnement de la personne ou de son entourage sur les modalités de l'accompagnement.

Pour faciliter la compréhension et l'effectivité des droits, il importe d'utiliser différents supports d'informations. Les temps d'échanges tant individuels que collectifs, sont des occasions de transmettre de l'information. La communication verbale apparait primordiale, en plus de l'information écrite.[47]

Par exemple, dans le cadre de la PJM, lors de l'établissement du DIPM, une note d'information peut également être fournie et lue à la personne protégée concernant la protection de ses données. Le consentement de la personne protégée est obtenu par la signature du Récépissé d'ouverture de mesure. Il en va de même avec les parents pour le DIPEC en MJAGBF.



[47] Le responsable de traitement devra démontrer que l'information a bien été délivrée.

L'information doit être adaptée à la compréhension de la personne.

Des images ludiques pour les enfants ou encore le recours à la méthode FALC (Facile À Lire et à Comprendre) pour les personnes en situation de handicap.

Les associations doivent indiquer aux personnes si les données collectées sont obligatoires ou facultatives. Elles doivent leur signaler quelles sont les conséquences éventuelles si elles ne communiquent pas les informations.

Dans le cadre d'une mesure de protection, si le conjoint d'une personne protégée refuse de transmettre ses revenus à la CAF, les allocations ne pourront pas être versées à la personne protégée. Le mandataire devra alors saisir le Juge des contentieux de la protection.

Recommandations

→ **Dans les documents tels que le livret d'accueil/notice d'information, créer ou intégrer un focus dédié à la protection des données personnelles** soumises à la règlementation des archives publiques. Ces documents doivent être remis aux salariés, aux bénévoles et aux personnes accompagnées.

→ **Informations à transmettre quand vous collectez des données personnelles** :

- Identité et coordonnées du responsable de traitement
- Les coordonnées du délégué à la protection des données
- Les finalités du traitement auquel sont destinées les données personnelles ainsi que la base juridique du traitement
- Intérêts légitimes si traitement fondés sur de tels intérêts
- Destinataire ou catégorie de destinataires des données personnelles
- Durée de conservation des données personnelles
- Présentation des droits de la personne (accès, rectification, effacement, limitation, opposition, portabilité)
- Droit de retirer le consentement à tout moment si on est dans le cadre d'un consentement
- Droit d'introduire une réclamation auprès d'une autorité de contrôle
  - Envisager une information régulière orale, écrite, individuelle ou collective tout au long de l'accompagnement à un moment opportun pour la personne.
  - Informer les personnes sur l'obligation de discrétion qui incombe aux professionnels (cf. Charte des droits et libertés de la personne protégée)

1.2 VOIES DE RECOURS POUR LES PERSONNES ACCOMPAGNÉES

L'information doit notamment porter sur les différentes voies de recours possibles :

1. DPO

- Les coordonnées du DPO doivent être accessibles aux personnes concernées car il est le premier niveau de recours. Les modalités de communication sont déterminées par l'association (par courriel, téléphone,...)

2. Le responsable de traitement

- En cas d'absence du DPO ou à défaut de réponse, les personnes peuvent contacter directement le responsable de traitement.

3. CNIL

- L'article 77 du RGPD reconnaît le droit des personnes d'introduire une réclamation auprès d'une autorité nationale de contrôle. Après une première demande restée sans suite auprès de l'Udaf ou si la réponse ne convient pas, la personne peut adresser une réclamation ou une plainte à la CNIL.

- Pour cela, elle peut adresser une plainte en ligne via le formulaire présent à cette adresse : https://www.cnil.fr/fr/plaintes. ou adresser un courrier postal à cette adresse : CNIL – 3 Place de Fontenoy – TSA 80715 – 75334 PARIS CEDEX 07. Elle devra communiquer toutes les pièces pouvant attester d'un manquement de l'Udaf.

4. Personne qualifiée

- Les "personnes qualifiées" interviennent sur demande de l'usager en cas de conflit, ou impossibilité de défendre ses droits et intérêts auprès d'un service ou d'un établissement. Elles sont désignées par décision conjointe du Préfet, du directeur général de l'Agence régionale de santé (ARS) et du président du Conseil départemental.

- La saisine de la personne qualifiée se fait auprès du Conseil départemental, de l'ARS, et plus exactement à la délégation territoriale dont la personne dépend dans la région. Exemple de lettre type de sollicitation, modèle de l'ARS Ile-de-France :
- https://framework.agevillage.com/documents/pdfs/lettre_type_sollicitation_personne_qualifiee.pdf.PDF)

5. Autorités de contrôle et de tarification (ARS, CD, DRJSCS, DDCSPP)

- Sans préjudice de tout autre recours administratif ou juridictionnel, toute personne concernée a le droit d'introduire une plainte auprès d'une autorité de contrôle si elle considère que le traitement de données à caractère personnel la concernant constitue une violation du RGPD. (Article 77 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016)

2. LE DROIT D'ACCÈS

2.1. DROIT D'ACCÈS DE LA PERSONNE ACCOMPAGNÉE

Voir les références juridiques à la fin du document

Le droit d'accès est un droit fondamental de la personne.
Il permet d'obtenir la communication dans un format compréhensible des données traitées et d'en contrôler l'exactitude le cas échéant.

La personne a accès à l'intégralité de ses informations contenues dans son dossier.

Il est possible de lui proposer un accompagnement adapté pour la consultation de son dossier.[48] Cet accompagnement reste facultatif.

Chaque responsable de traitement devra déterminer les modalités qu'il souhaite appliquer et en informer les personnes accompagnées notamment dans le livret d'accueil.

Recommandations

- La demande d'accès doit être faite auprès du responsable de traitement par voie électronique, ou courrier.
- Dans le cas où la demande est effectuée sur place et qu'il n'est pas possible d'y répondre immédiatement, il faut remettre au demandeur un avis de réception daté et signé.
- Une réponse doit être apportée dans un délai maximum d'un mois ou trois mois en fonction de la complexité de la demande (article 12.3 du RGPD).
- Il doit être proposé à la personne, qui souhaite consulter son dossier, un accompagnement adapté, en lui permettant par exemple d'être accompagnée par un tiers.

Se référer à l'exemple de procédure d'accès aux données personnelles en annexe.

[48] Article 3 de la charte des droits et libertés de la personne accueillie

2.2. LE COÛT DE L'ACCÈS AU DOSSIER POUR LE DEMANDEUR

Le RGPD prévoit un **principe de gratuité** pour les copies fournies dans le cadre d'une demande d'accès[49].

Il est toutefois possible de demander à la personne de payer toute copie qu'elle demanderait en plus, ou si sa demande est manifestement infondée ou excessive. En ce cas, le prix demandé doit correspondre au coût des « frais raisonnables basés sur les coûts administratifs », fixés dans l'arrêté du 1er octobre 2001[50]. De même, ils ne doivent pas être une entrave à l'exercice du droit d'accès.

2.3. LES RÈGLES D'ACCÈS POUR LES TIERS/AYANTS DROITS

LES TIERS

La personne concernée par les données peut mandater la personne de son choix pour exercer son droit d'accès.

Dans ce cas, cette tierce personne doit présenter un écrit précisant l'objet du mandat, l'identité du mandant (la personne concernée par les données qui donne mandat pour exercer son droit d'accès), identité du mandataire (son identité).

Pour les mineurs, ce sont, selon les cas, les parents ou les titulaires de l'autorité parentale qui effectuent la démarche.

LES AYANTS DROITS

La communication de données à caractère personnel n'est possible qu'à la personne concernée[51]. **La seule qualité d'ayant droit de cette dernière, ne confère pas la qualité de personne concernée par leur traitement.**

Toutefois, si la personne concernée – victime – engage une action en réparation avant son décès, ses héritiers peuvent exercer ce droit comme elle. En effet, lorsque la victime d'un dommage décède, son droit à réparation entre dans son patrimoine et est transmis à ses héritiers.

Il existe également des cas spécifiques dans lesquels les ayants droits peuvent avoir accès aux données de la personne défunte. A titre d'illustration, depuis le 1er janvier 2016, les héritiers peuvent obtenir directement communication des données, issues du Fichier

[49] Article 12 du RGPD

[50] Cf. Arrêté du 1er octobre 2001 relatif aux conditions de fixation et de détermination du montant des frais de copie d'un document administratif

[51] Articles 2 et 39 de la loi I &L

National des Comptes Bancaires et Assimilés (Ficoba), relatives aux comptes ouverts par la personne décédée[52].

De plus, les héritiers de la personne concernée décédée peuvent exiger une actualisation de ses données à caractère personnel, afin notamment de préserver la mémoire de celle-ci et de protéger sa vie privée[53].

Enfin, il est à noter que toute personne peut définir des directives relatives à la conservation, à l'effacement et à la communication de ses données à caractère personnel après son décès. Ces directives peuvent notamment être enregistrées auprès d'un tiers de confiance numérique certifié par la CNIL[54].

FOCUS SUR LES SERVICES MJPM

Ce principe d'accès par exception pour les héritiers doit être croisé avec les dispositions de la loi n° 2007-308 du 5 mars 2007 portant réforme de la protection juridique des majeurs.

L'article 514 du Code civil modifié par cette loi prévoit qu'à la fin de la mission, il doit être remis une copie des cinq derniers comptes de gestion et du compte de gestion des opérations intervenues depuis l'établissement du dernier compte :

- à la personne devenue capable si elle n'en a pas déjà été destinataire,
- à la personne nouvellement chargée de la mesure de gestion
- ou aux héritiers de la personne protégée.

Dans tous les cas, la personne en charge d'une mesure de protection remet à ces personnes les pièces nécessaires à la continuité de gestion ou pour assurer la liquidation de la succession, ainsi que l'inventaire initial et les actualisations auxquelles il a donné lieu.

[52] Art L 151 B du Livre des procédures fiscales

[53] Délibération n° 2010-460 du 9 décembre 2010 de la Commission nationale de l'informatique et des libertés portant recommandation relative aux conditions de réutilisation des données à caractère personnel contenues dans des documents d'archives publiques.

[54] Cf. Article 63 de la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique

2.4. LES RÈGLES D'ACCÈS AUPRÈS DE TIERS DÉTENANT DES INFORMATIONS RELATIVES À LA PERSONNE PROTÉGÉE

Lorsqu'il existe une mesure de protection, les règles d'accès pour le protecteur sont régies de la manière suivante :

- Pour les majeurs en tutelle :
  Le tuteur pourra demander directement par écrit les informations aux tiers en joignant à sa demande un extrait du jugement de tutelle.

- Pour les majeurs en curatelle :

  - Curatelle simple : la démarche devra être effectuée par le majeur protégé ; le curateur ne pouvant pas intervenir directement dans le suivi administratif de la personne. Toutefois, du fait de sa mission d'information, il devra, le cas échéant, aider la personne protégée à la rédaction d'une demande auprès d'un organisme.

  - Curatelle renforcée : La démarche ne pourra être effectuée par le curateur que pour les actes qui relèvent de sa gestion en représentation. Il pourra donc solliciter l'accès aux dossiers des personnes protégées auprès:
    - Des organismes bancaires pour le fonctionnement des comptes et la gestion de l'épargne
    - Des organismes prestataires octroyant des ressources à la personne protégée (CAF, CPAM,…)
    - Des organismes pour lesquels la personne protégée est rattachée par le paiement de dépenses (bailleur, assurance, mutuelle…).

Pour les autres démarches, seule la personne protégée sera amenée à réaliser cette demande auprès des organismes. Le curateur conserve toutefois une mission d'information auprès de la personne protégée pour l'aider dans la réalisation de cette démarche comme en curatelle simple.

FOCUS : L'ACCÈS AU DOSSIER MÉDICAL DES PERSONNES PROTÉGÉES PAR LE MANDATAIRE JUDICIAIRE

Aux termes de **l'article L 1111-7 du Code de la santé publique,** modifié par l'ordonnance du 11 mars 2020[55] :

> Toute personne a accès à l'ensemble des informations concernant sa santé, notamment les résultats d'examen, comptes rendus de consultation, d'intervention, d'exploration ou d'hospitalisation, des protocoles et prescriptions thérapeutiques, des correspondances entre professionnels de santé.
> Lorsque la personne bénéficie d'une tutelle avec représentation relative à la personne, le protecteur a également accès à ces informations.
> De ce fait, la personne chargée d'une mesure de tutelle avec représentation relative aux biens ne peut pas accéder au dossier médical de la personne protégée.

Dans le cas d'une curatelle, le curateur ne peut exercer le droit d'accès au nom de la personne protégée. Cette dernière doit donc exercer elle-même son droit d'accès ou donner son consentement exprès à son curateur.

L'article R 1111-1 du CSP fixe la **liste des personnes qui peuvent également accéder aux informations relatives à la santé de la personne**. Y figure notamment **la personne en charge de l'exercice de la mesure de protection, habilitée à la représenter ou à l'assister.**

Pour ce qui concerne l'accès au DMP « **dossier médical partagé** »[56], seule la personne titulaire du DMP et les médecins de son choix peuvent y avoir accès.

Les certificats médicaux peuvent être collectés et traités dès lors qu'une des bases légales existe[57], c'est-à-dire le consentement exprès ou la nécessité pour la prise en charge sanitaire et sociale.

En ce qui concerne les délais d'accès, **la communication doit être faite au plus tôt** dans les 48 heures, suivant la demande (compte tenu du délai de réflexion prévu par la loi dans l'intérêt de la personne) et **au plus tard dans les 8 jours.** Si les informations remontent à plus de cinq ans, le délai est porté à 2 mois (article L 1111-7 du CSP)[58].

[55] Entrée en vigueur le 1er octobre 2020
[56] Il s'agit d'un carnet de santé dématérialisé qui peut contenir : des comptes rendus hospitaliers et radiologiques, résultats d'analyses de biologie, antécédents et allergies, actes importants réalisés, médicaments qui vous ont été prescrits et délivrés.
[57] Cf. chapitre 2 sur le principe de licéité
[58] https://www.cnil.fr/fr/professionnels-comment-repondre-une-demande-de-droit-dacces

2.5. LES RÈGLES D'ACCÈS PAR LA PERSONNE, UNE FOIS SON DOSSIER ARCHIVÉ AUX ARCHIVES DEPARTEMENTALES

Conformément au protocole d'archivage, les Udaf sont **tenues de verser certains documents aux Archives Départementales,** et ce **à des fins archivistiques**, de recherches scientifiques, historiques ou statistiques. **Les services publics d'archives peuvent alors déroger aux droits des personnes[59], lorsque cela est nécessaire,** pour conserver et mettre à disposition des chercheurs des archives publiques.

Ainsi, il est fortement **recommandé d'informer la personne** concernée de ce versement, ainsi que des possibilités d'accès aux documents d'archives publiques.[60]

Ces archives peuvent être consultées par les personnes elles-mêmes ou leurs ayant-droits[61]. Elles sont aussi par principe librement communicables à toute personne qui en fait la demande[62], selon les modalités suivantes :

- par la consultation gratuite sur place ;
- par la délivrance d'une copie réalisée aux frais du demandeur ;
- par courrier électronique et sans frais lorsque le document est disponible sous forme électronique.

Cependant, les documents contiennent parfois des informations qu'il est nécessaire de protéger pendant un certain temps, avant de permettre leur communication. La vie privée, le secret médical,… font partie des informations protégées. **Ainsi, certains documents administratifs ne sont communicables qu'à l'intéressé[63].** Ceux :

- dont la communication porterait atteinte à la protection de la vie privée, au secret médical et au secret des affaires ;
- portant une appréciation ou un jugement de valeur sur une personne physique, nommément désignée ou facilement identifiable ;
- faisant apparaître le comportement d'une personne, dès lors que la divulgation de ce comportement pourrait lui porter préjudice.

---

[59] Ces dérogations s'appliquent également aux archives définitives, encore conservées par les producteurs, dans l'attente de leur versement aux Archives départementales.

[60] La communicabilité de ces documents tombe dans le droit commun :
- la loi n° 78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal, dite « loi CADA »,
- la loi n° 2008-696 du 15 juillet 2008 relative aux archives

[61] En vertu du droit d'accès aux archives publiques dans le Code du patrimoine, et le Code des relations entre le public et l'administration

[62] Art. L 213-1 du Code du patrimoine

[63] Art. L 311-6 du Code des relations entre le public et l'administration

3. Le droit de rectification

Voir les références juridiques à la fin du document

La personne a le **droit d'obtenir la rectification de ses données si elles sont inexactes ou incomplètes,** lorsque des erreurs ou inexactitudes ont été décelées, ou en présence de données dont la collecte, l'utilisation, la communication ou la conservation est interdite.

Un salarié se marie et formule son droit de rectification auprès du responsable de traitement pour changer son nom de famille.

4. Le droit d'opposition

Voir les références juridiques à la fin du document

Toute personne peut s'opposer, pour des motifs légitimes[64], à ce que ses données soient utilisées, en justifiant sa demande. De la même manière, le responsable de traitement peut également justifier de la nécessité de traiter des données à défaut desquelles, elle serait dans l'impossibilité d'exercer sa mission. **Il est noté que le droit d'opposition ne peut être exercé que si le traitement est fondé sur l'intérêt légitime ou la mission d'intérêt public.**

Si le traitement des données personnelles est fondé sur l'obligation légale alors la personne ne pourra pas s'opposer au traitement de ses informations.

En cas d'opposition des personnes, l'organisme doit entreprendre plusieurs actions :

- → Informer sans délai de cette opposition tout autre responsable de traitement avec qui il a partagé ces données.

- → Donner une réponse à cette demande d'opposition sous un mois, et dans un délai maximal de trois mois en fonction de la complexité et du nombre de demandes.

Une personne dans un groupe d'entraide mutuelle (GEM) s'oppose à la collecte d'une information concernant sa situation professionnelle. Cette donnée n'étant pas indispensable, il convient de faire droit à sa demande et d'en informer dans les meilleurs délais les autres organismes auxquels cette information aurait été transmise.

[64] Arrêt du 18 mars 2019, le Conseil d'Etat précise le motif légitime :
-Une demande d'opposition doit être justifiée par des motifs légitimes tenant de manière prépondérante à la situation particulière de la personne concernée ;
-L'invocation de craintes d'ordre général, sans lien avec la situation personnelle du demandeur, ne constitue pas un motif légitime valable.

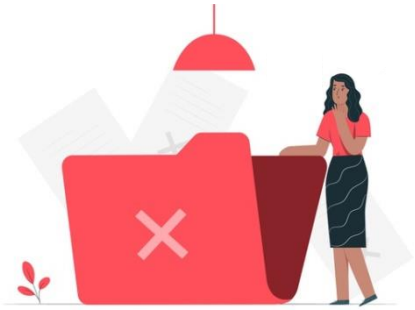
Si la personne s'oppose au traitement de ses données, et que son accompagnement est maintenu, il convient que les équipes :

- examinent les raisons et éventuellement en posant les nouvelles bases de l'intervention,
- étudient les conséquences du refus,
- informent la personne des conséquences de son refus ou des modifications apportées sur la qualité de son accompagnement.

5. Le droit à l'oubli

Voir les références juridiques à la fin du document

Le responsable de traitement a l'obligation d'effacer des données à caractère personnel dans les cas suivants :



→ Si les données ne sont plus nécessaires

Le service de gestion de patrimoine/juridique de l'Udaf a collecté des données relatives à l'état de santé de la personne dans le cadre d'un projet de placement d'épargne handicap. Si ce projet est abandonné, ces informations n'ont plus de finalité et doivent être effacées.

→ Si la personne retire son consentement ou s'oppose au traitement et il n'existe pas d'autre base légale au traitement.

→ Si les données ont fait l'objet d'un traitement illicite

Une information relative à la confession religieuse de la personne est collectée dans le cadre d'une mesure d'accompagnement social personnalisé (MASP). Cette donnée est illicite, et aucune exception ne s'impose en ce cas car elle n'est justifiée par aucune finalité. En effet, le travailleur social n'a pas vocation à organiser des obsèques, comme c'est le cas dans le cadre d'une mesure de protection.

→ Les données doivent être effacées pour respecter une obligation légale prévue par le droit de l'UE ou du pays

Le Code du travail français impose la suppression, dans le dossier du salarié, de toute trace relative à une sanction disciplinaire, au bout de 3 ans.

Ce droit ne s'applique pas si cela est nécessaire :

→ à des fins archivistiques dans l'intérêt public
→ à l'exercice du droit à la liberté d'expression et d'information de la personne
→ au respect d'une obligation légale, ou pour exécuter une mission d'intérêt public
→ à la constatation, à l'exercice ou à la défense de droits en justice

6. Le droit à la limitation du traitement

Voir les références juridiques à la fin du document

La personne concernée peut demander de geler temporairement l'utilisation de certaines de ses données, notamment si elle conteste leur exactitude ou si elle s'oppose à ce qu'elles soient traitées. Ce droit vient donc faciliter l'exercice des droits précédents.

Concrètement, l'association ne devra plus utiliser les données de la personne, mais devra les conserver le temps de la vérification ou examen de la demande.

Inversement, il est possible que la personne puisse demander de conserver provisoirement ses données, alors que l'association souhaite elle-même les effacer.

Une personne a formulé un droit d'opposition au traitement d'une ou de plusieurs données personnelles. Elle peut en outre demander de geler l'utilisation de ces données, le temps de l'instruction de sa requête.

7. Le droit à la portabilité des données

Voir les références juridiques à la fin du document

Introduit par le RGPD, le droit à la portabilité offre aux personnes la possibilité d'obtenir et de réutiliser leurs données personnelles pour répondre à leurs propres besoins.

Ce droit permet à une personne :

- **de récupérer les données la concernant** traitées par un organisme, **pour son usage personnel**, et de les stocker sur un appareil ou un cloud privé par exemple. Ce droit permet de gérer plus facilement et par soi-même ses données personnelles.
- **de transférer ses données personnelles d'un organisme à un autre**. Les données personnelles peuvent ainsi être transmises à un nouvel organisme :
  - soit par la personne elle-même ;
  - soit directement par l'organisme qui détient les données, si ce transfert direct est « techniquement possible ».

Ce nouveau droit s'applique si ces trois conditions sont toutes réunies :

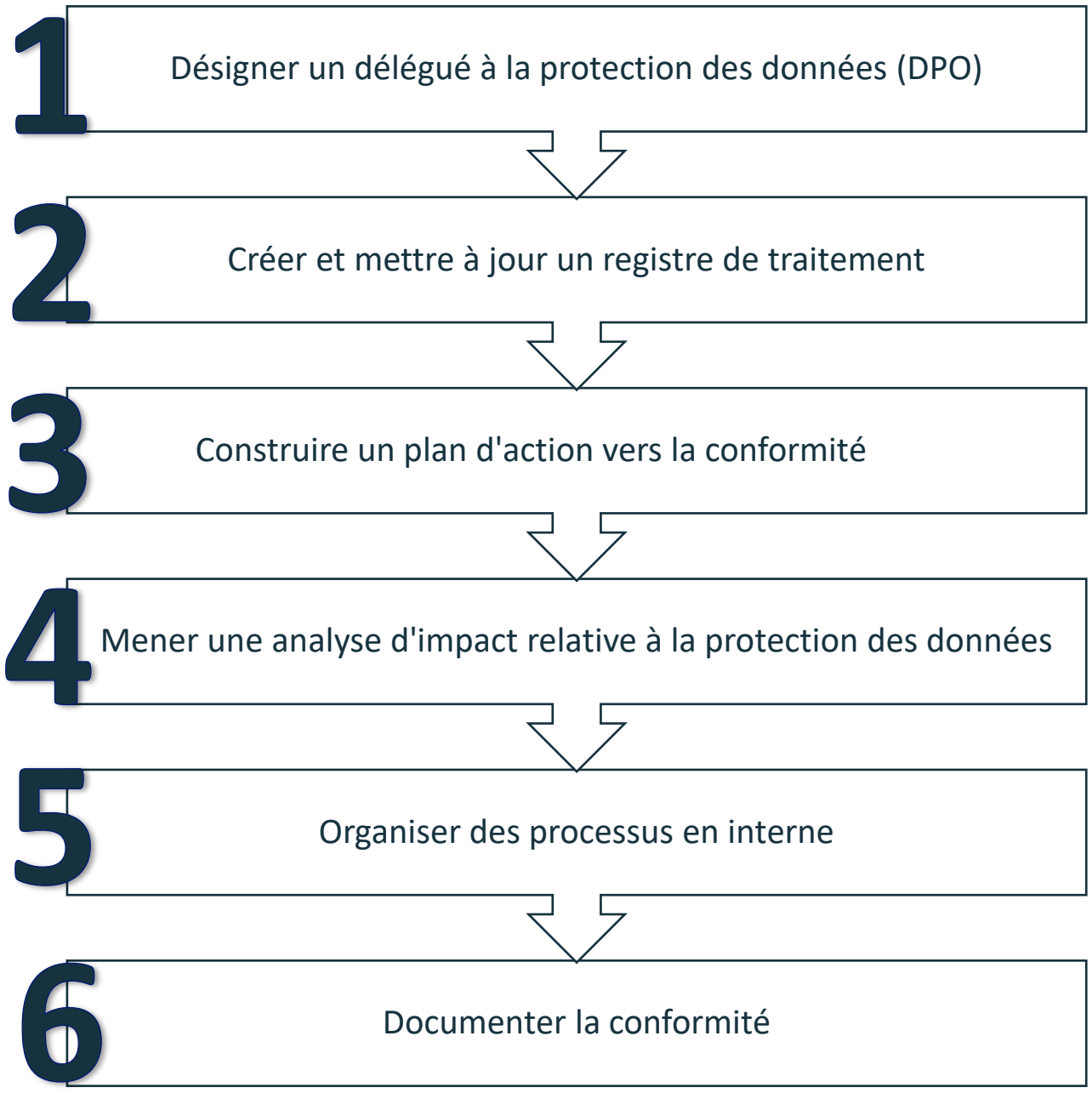
1. **le droit à la portabilité est limité aux données personnelles fournies par la personne concernée ;**
2. Il ne s'applique **que si les données sont traitées de manière automatisée** (les fichiers papiers ne sont donc pas concernés) et sur la base du **consentement préalable** de la personne concernée ou de **l'exécution d'un contrat conclu avec la personne concernée** ;
3. L**'exercice du droit à la portabilité ne doit pas porter atteinte aux droits et libertés de tiers,** dont les données se trouveraient dans les données transmises suite à une demande de portabilité.

Pour en savoir plus, voir le site de la CNIL : https://www.cnil.fr/fr/le-droit-la-portabilite-en-questions

CHAPITRE IV

LES ETAPES DE MISE EN CONFORMITÉ AU RGPD

Les étapes de la mise en conformité au RGPD



1. DÉSIGNER UN DÉLEGUÉ À LA PROTECTION DES DONNÉES (DPO)[65]

1.1. LES MISSIONS DU DPO

Le délégué à la protection des données est chargé de piloter la gouvernance des données du responsable de traitement. **Il est le chef d'orchestre qui exerce une mission d'information, de conseil et de contrôle en interne.**[66]

Son rôle est notamment d'informer sur le contenu et l'impact des nouvelles obligations, de réaliser l'inventaire des traitements, de sensibiliser et de piloter la conformité en continu.
Il facilite le dialogue avec les autorités de protection des données et gère les risques de contentieux.

En dehors de toute faute intentionnelle qui pourra être poursuivie devant les juridictions pénales, le DPO ne saurait supporter la responsabilité des éventuels manquements aux obligations du RGPD. En effet, en qualité de responsable de traitement, l'association, restera la seule et unique responsable de la protection des données.

1.2. LA DESIGNATION D'UN DPO : OBLIGATOIRE OU FALCUTATIVE ?

La désignation d'un délégué est obligatoire si :

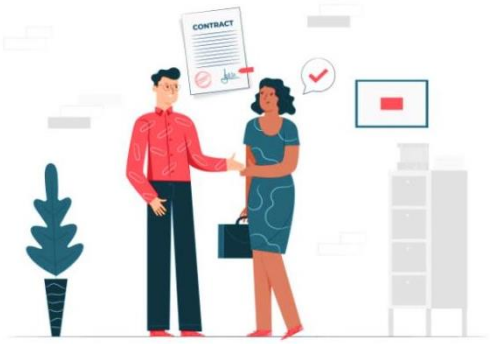
- → Vous êtes un organisme public ;
- → Vous êtes un organisme dont l'activité de base vous amène à réaliser un suivi régulier et systématique des personnes à grande échelle, ou à traiter à grande échelle des données dites « sensibles » ou relatives à des condamnations pénales et infractions.

Dans les autres cas, la désignation d'un délégué à la protection des données est fortement encouragée par la CNIL.

La volumétrie et la nature des données à caractère personnel traitées obligent **les Udaf à procéder à la désignation d'un DPO.**[67]

[65] Le sigle français pour « Délégué à la Protection des Données » est « DPD ». Toutefois, dans l'intégralité de ce document, nous avons fait le choix d'utiliser l'anglicisme « DPO » pour « Date Protection Officer » car c'est le terme usuel.
[66] Pour aller plus loin : https://www.cnil.fr/fr/le-delegue-la-protection-des-donnees-dpo
[67] La désignation d'un DPO n'est pas obligatoire pour les associations qui ne gèrent pas de services dans le domaine de l'action sociale et qui ne traitent pas des données sensibles.

1.3. LA PROCEDURE À SUIVRE POUR DESIGNER UN DPO



Le DPO conseille et accompagne de manière indépendante les organismes qui le désignent. Il doit être exempt de conflit d'intérêt, ce qui signifie notamment que cette fonction ne peut être assurée par un membre de la Direction des Systèmes d'Information (DSI) ou un collaborateur impliqué dans la gestion des données des personnes accompagnées[68].

Un intervenant social, un directeur, un responsable de ressources humaines, ne peuvent pas être désignés en qualité de DPO. En revanche, un responsable qualité peut l'être.

Le DPO doit notamment détenir des compétences en matière de protection des données personnelles. Il peut être interne à l'organisation (salarié ou bénévole). S'il est externe (cabinet d'avocat ou de conseil, etc.), il est désigné sur la base d'un contrat de prestation de service. Le RGPD ne donne aucune indication sur le niveau de rémunération du DPO. **Il est tout à fait possible de mutualiser un DPO. Certaines Udaf le font déjà par exemple.**

Recommandations

1. Rédiger une fiche de poste et/ou une lettre de mission du DPO (voir modèles sur https://afcdp.net/dpo-fiche-de-poste-et-lettre-de-mission/)
2. Si un DPO est désigné en interne, s'assurer qu'il bénéficie d'une formation pour exercer ses missions.
3. Désigner un DPO en ligne sur le site de la CNIL via un téléservice dédié : https://www.cnil.fr/fr/designez-en-ligne-votre-delegue-la-protection-des-donnees-aupres-de-la-cnil
4. Lors de la désignation en ligne, la CNIL demande, outre les coordonnées nominatives du DPO, des coordonnées professionnelles. Il est recommandé de choisir une adresse électronique générique (ex : « dpo ou donnéespersonnelles@exemple.fr)
5. Le DPO étant le « point de contact » concernant la protection des données, il est important d'informer de son existence et de communiquer ses coordonnées :
   - *aux personnes concernées* ;
   - *au personnel de l'association ;*
   - *aux administrateurs de l'association, aux représentants familiaux et aux bénévoles impliqués auprès des personnes accompagnées ;*
   - *à la CNIL avec laquelle il coopère.*

[68] Le DPO ne peut pas exercer au sein de l'organisme une fonction qui l'amènerait à déterminer les finalités et les moyens du traitement des données.

2. CRÉER ET METTRE À JOUR UN REGISTRE DE TRAITEMENT

L'article 30 du RGPD impose à chaque responsable de traitement la tenue d'un tel registre. Chaque association doit ainsi en tenir un.

Il s'agit d'un document de recensement et d'analyse, qui doit refléter la réalité de vos traitements de données personnelles.

Au-delà d'une simple obligation juridique, le registre est surtout un outil de pilotage de votre conformité au RGPD. Il vous permet de documenter et disposer d'une vue d'ensemble de la manière dont vous traitez vos données.

Recommandations

1. La première étape est d'identifier, avec les professionnels concernés par le traitement de données, les activités principales de votre association qui nécessitent la collecte et le traitement de données.

2. Chaque activité recensée fera ensuite l'objet d'une fiche spécifique dans laquelle il faudra notamment préciser :
   - les parties prenantes ;
   - les catégories de données traitées ;
   - à quoi elles servent, qui accède aux données, et à qui elles sont communiquées ;
   - leur durée de conservation ;
   - comment elles sont sécurisées.

3. A partir de ce travail de recensement, créer et mettre à jour un registre de traitement

→ La CNIL propose un modèle de registre des activités de traitement : https://www.cnil.fr/fr/RGDP-le-registre-des-activites-de-traitement

3. CONSTRUIRE UN PLAN D'ACTION VERS LA CONFORMITÉ

La création et la mise à jour d'un registre de traitement sont aussi l'occasion d'identifier et de hiérarchiser les risques au regard du RGPD. Cette étape essentielle permet d'en déduire un plan d'action avec des priorités identifiées, pour améliorer les pratiques.

Recommandations

→ **Dans le cadre de l'élaboration du plan d'action, il convient de** :

- S'assurer que seules les données strictement nécessaires à la poursuite de vos objectifs sont collectées et traitées
- Identifier la base juridique sur laquelle se fonde votre traitement (par exemple : consentement de la personne, intérêt légitime, contrat, obligation légale)
- Réviser vos mentions d'information afin qu'elles soient conformes aux exigences du règlement
- Vérifier que vos sous-traitants connaissent leurs nouvelles obligations et leurs responsabilités
- S'assurer de l'existence de clauses contractuelles, rappelant les obligations du sous-traitant en matière de sécurité, de confidentialité et de protection des données personnelles traitées
- Prévoir les modalités d'exercice des droits des personnes concernées (droit d'accès, de rectification, droit à la portabilité, retrait du consentement...)
- Vérifier les mesures de sécurité mises en place

→ **<u>Exemple d'actions à mettre en œuvre :</u>**

↳ RH, sensibilisation et formation des salariés et autres collaborateurs (bénévoles, stagiaires,…)

- Mettre à jour le kit documentaire remis au salarié (règlement intérieur, livret d'accueil, charte informatique, etc.)
- Mettre à jour les contrats de travail
- Mettre en place des formations des salariés et autres collaborateurs sur les bonnes pratiques

4. MENER UNE ANALYSE D'IMPACT RELATIVE À LA PROTECTION DES DONNEES

Selon l'article 35 du RGPD, une analyse d'impact (AIPD) **est obligatoire pour tout traitement susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées.**

L'AIPD est un outil important qui aide les associations non seulement à construire des traitements de données respectueux de la vie privée, mais aussi à démontrer leur conformité au RGPD.

La CNIL a établi une liste des types d'opérations pour lesquelles elle a estimé l'AIPD obligatoire. **Y figurent notamment les « traitements ayant pour finalité l'accompagnement social ou médico-social des personnes »[69]. Les associations, telles que les Udaf, sont donc concernées par la réalisation de cette analyse.**

Pour les opérations suivantes, la CNIL estime qu'une AIPD n'est pas requise :

- Traitements mis en œuvre uniquement à des fins de ressources humaines pour la seule gestion du personnel des organismes qui emploient moins de 250 personnes, à l'exception du recours au profilage[70].
- Traitements de gestion de la relation fournisseurs.
- Traitements destinés à la gestion des activités des comités d'entreprise et d'établissement.
- Traitements mis en œuvre par une association, une fondation ou toute autre institution sans but lucratif, pour la gestion de ses membres et de ses donateurs dans le cadre de ses activités habituelles, dès lors que les données ne sont pas sensibles.
- Traitements mis en œuvre par les collectivités territoriales et les personnes morales de droit public et de droit privé, aux fins de gérer les services en matière d'affaires scolaires, périscolaires et de la petite enfance.
- Traitements mis en œuvre aux seules fins de gestion des contrôles d'accès physiques et des horaires pour le calcul du temps de travail, en dehors de tout dispositif biométrique.

[69] https://www.cnil.fr/sites/default/files/atoms/files/liste-traitements-avec-aipd-requise-v2.pdf

[70] Le profilage est le traitement automatisé de données à caractère personnel qui consiste à utiliser ces données pour évaluer certains aspects de la personne concernée, et analyser ou prédire ses intérêts, son comportement et d'autres attributs. Vous trouverez la définition officielle de « profilage » selon le RGPD dans l'article 4.4 du RGPD.

Recommandations

Les associations sont tenues de réaliser et tenir à jour une AIPD sur les activités de traitement mises en œuvre dans le cadre de leurs missions.

L'AIPD contient *a minima* :

- une description détaillée du traitement mis en œuvre, comprenant tant les aspects techniques qu'opérationnels ;
- l'évaluation, de nature plus juridique, de la nécessité et de la proportionnalité concernant les principes et droits fondamentaux (finalité, données et durées de conservation, information et droits des personnes, etc.) non négociables, qui sont fixés par la loi et doivent être respectés, quels que soient les risques ;
- l'étude, de nature plus technique, des risques sur la sécurité des données (confidentialité, intégrité et disponibilité) ainsi que leurs impacts potentiels sur la vie privée, qui permet de déterminer les mesures techniques et organisationnelles nécessaires pour protéger les données.

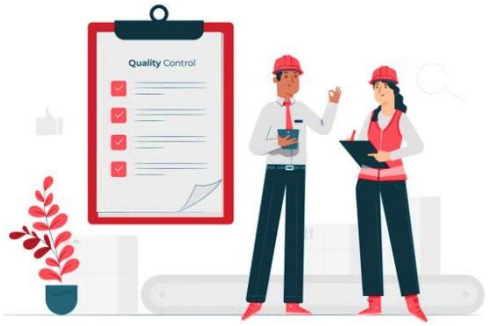
Si un DPO a été désigné, il coordonne la réalisation de l'AIPD en lien avec la DSI (Directions du Système d'Information) et les professionnels.

→ La CNIL a publié une solution informatique dédiée aux AIPD, accessible à tous : https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil

→ Elle propose également des guides et modèles d'AIPD : https://www.cnil.fr/fr/guides-aipd

5. ORGANISER DES PROCESSUS EN INTERNE

Afin de garantir un haut niveau de protection des données personnelles, il est important de mettre en place des procédures internes face, par exemple, à une faille de sécurité ou pour gérer des demandes de rectification ou d'accès.



Ces processus font suite aux précédentes étapes et doivent respecter les priorités définies dans le plan d'action.

Organiser les processus implique notamment de :

- **Prendre en compte** la protection des données personnelles dès la conception d'un traitement (minimisation de la collecte au regard de la finalité, durées de conservation, mentions d'information, recueil du consentement, sécurité et confidentialité des données, s'assurer du rôle et de la responsabilité des acteurs impliqués dans la mise en œuvre de traitements de données)

- **Sensibiliser et organiser** la remontée d'informations en construisant notamment un plan de formation et de communication auprès des salariés et des bénévoles

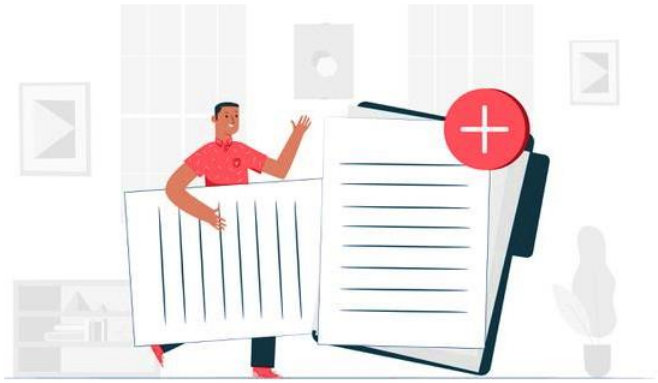
- **Traiter** les réclamations et les demandes des personnes concernées quant à l'exercice de leurs droits (droits d'accès, de rectification, d'opposition, droit à la portabilité, retrait du consentement) en définissant les acteurs et les modalités (par courrier, par mail ou en face à face) (*Cf. chapitre 3, l'information et les droits des personnes)*

- **Définir une procédure d'accès aux données personnelles** (*Cf. annexe 1, un exemple de procédure)*

- **Anticiper** les violations de données en prévoyant, dans certains cas, la notification à la CNIL dans les 72 heures, et aux personnes concernées dans les meilleurs délais (*Cf. chapitre 2 les recommandations sur la traçabilité des accès.)*

- **S'assurer du respect des obligations des sous-traitants** (*Cf. annexe 3, les obligations des sous-traitants)*

6. DOCUMENTER LA CONFORMITÉ



Les associations doivent être en mesure de démontrer le respect du RGPD par un ensemble de mesures techniques et organisationnelles appropriées.

Pour cela, il est nécessaire de constituer et regrouper dans un dossier toute la documentation relative aux actions réalisées pour assurer la protection continue des données personnelles.

Ce dossier devra notamment comporter les éléments suivants :

La documentation sur vos traitements de données personnelles

- le registre des traitements (pour les responsables de traitements) ou des catégories d'activités de traitements (pour les sous-traitants)
- les analyses d'impact sur la protection des données (le logiciel PIA est à télécharger ici) pour les traitements susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes
- Les contrats qui définissent les rôles et les responsabilités des acteurs, les contrats avec les sous-traitants
- les procédures internes en cas de violation de données

L'information des personnes

- les mentions d'information
- les modèles de recueil du consentement des personnes concernées
- les procédures mises en place pour l'exercice des droits des personnes
- les preuves que les personnes concernées ont donné leur consentement lorsque le traitement de leurs données repose sur cette base ou dans le cadre de la collecte de données sensibles.

ANNEXES

1. EXEMPLE DE PROCÉDURE D'ACCÈS AUX DONNÉES PERSONNELLES DANS UNE UDAF

1. OBJET

Cette procédure définit les modalités de communication des données personnelles détenues par l'Udaf en cas de demande d'accès par la personne et/ou, le cas échéant, de son entourage.

2. DÉFINITION

Une **donnée personnelle** est toute information se rapportant à une personne physique identifiée ou identifiable, directement ou indirectement. (Nom, numéro de téléphone, numéro de sécurité sociale…)

Les **données sensibles** sont relatives à l'origine raciale ou ethnique, aux opinions politiques, aux convictions religieuses ou philosophiques, à l'appartenance syndicale, à la vie sexuelle ou à l'orientation sexuelle et à la santé, ainsi que des données génétiques et biométriques.

L'exercice du **droit d'accès** permet de savoir si vos données sont traitées et d'en obtenir la communication dans un format compréhensible. Il permet également d'en contrôler leur exactitude et, au besoin, de les faire rectifier ou effacer.

3. DOMAINE D'APPLICATION

La présente procédure s'applique à l'ensemble des professionnels des Udaf.

4. DOCUMENTS DE RÉFÉRENCE

- RGPD
- Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée
- Loi n°2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé
- Arrêté du 5 mars 2004, portant homologation des recommandations de bonnes pratiques relatives à l'accès aux informations concernant la santé d'une personne
- Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé
- Articles L 1111-2 du Code de la Santé Publique
- Article R 1111-7 et -8 du Code de la Santé Publique
- Article 371-1 Code Civil
- Article 311-3 du Code de l'Action Sociale et des Familles
- Arrêté du 8 septembre 2003 relatif à la Charte des droits et libertés de la personne accueillie, mentionnée à l'article L 311-4 du Code de l'Action Sociale et des Familles

5. LE PROCESSUS

5.1 La demande de consultation du dossier

➢ **Qui demande ?**

- La personne concernée
- Le(s) titulaire(s) de l'autorité parentale pour les mineurs
- Les ayants droit pour les personnes décédées. La demande doit alors être motivée par le souci de connaitre les causes du décès, défendre la mémoire du défunt ou de faire valoir leurs droits
- Une tierce personne désignée par la personne. Dans ce cas, elle doit disposer d'un écrit précisant l'objet du mandat, l'identité du mandant et celle du mandataire

➢ **Comment demander ?**

La demande doit être faite par mail ou courrier recommandé avec accusé de réception ou remis en main propre auprès du responsable de traitement identifié au sein de l'Udaf.

➢ **Quand ?**

- Jusqu'à 5 ou 10 ans, en fonction des données, après la clôture du dossier ou la fin d'accompagnement : les Udaf conservent les dossiers des personnes accompagnées
- Au-delà des 10 ans : consulter les Archives départementales

5.2 Réception de la demande

Dans tous les cas, il faut :

- Accuser réception de la demande par tout moyen, même si elle est imprécise et y donner suite
- Il convient à ce moment de noter dans un registre (papier ou informatique) la demande, la date, l'objet et la signature du demandeur
- Vérifier la qualité de la personne pour le droit de transmission

5.3 Les délais de réponse

La réponse doit être fournie par écrit dans un délai d'un mois maximum, ou trois mois en fonction de la complexité de la demande.

En ce qui concerne l'accès aux données de santé :
Les délais accordés pour obtenir la communication du dossier sont :

- au plus tôt, après qu'un délai de réflexion de 48 heures (2 mois lorsque les informations médicales demandées datent de plus de 5 ans) ;
- au plus tard dans les 8 jours suivant la demande.

Si les informations remontent à plus de 5 ans, le délai est porté à 2 mois (article L 1111-7 du Code de la santé publique).

En cas de refus de l'Udaf à la demande d'accès, il convient de le motiver et d'informer le demandeur des voies de recours et des délais dont il dispose pour contester ce refus.

5.4 Organisation de la consultation du dossier

➢ Consultation sur place

Un espace d'accueil adapté doit être proposé au sein du service.
Le droit d'accès est un droit fondamental de la personne. Néanmoins, il faut être vigilant à son état psychologique et affectif, afin que ces informations ne nuisent pas à sa santé mentale.
Il est donc nécessaire de proposer à la personne qui souhaite consulter son dossier, un accompagnement adapté, en lui permettant par exemple d'être accompagnée par un tiers. (Article 3 de la Charte des droits et libertés de la personne accueillie).

Dans le cas particulier de la présence d'une tierce personne lors de la consultation du dossier, à la demande de la personne ou du médecin, **il est indispensable d'informer** :

- Le demandeur du fait que la tierce personne aura connaissance d'informations strictement personnelles sur sa santé.
- La tierce personne, qu'elle est tenue pénalement de respecter la confidentialité des informations de santé de la personne qu'elle accompagne.

Dans tous les cas les informations transmises au demandeur doivent être lisibles et compréhensibles.

➢ Copie

Le **principe est celui de la gratuité**.
Il est toutefois possible de demander le paiement de frais raisonnables basés sur les coûts administratifs : pour toute copie supplémentaire demandée par la personne concernée ; ou si la demande est manifestement infondée ou excessive.

➢ Demande d'envoi

Les personnes peuvent demander l'envoi du dossier. Il est alors conseillé d'envoyer le dossier photocopié par lettre recommandée avec un avis de réception. L'intérêt étant de garantir la confidentialité des données envoyées.

S'il est impossible de photocopier un document, il faut prévenir que la consultation ne pourra se faire que sur place.

Conformément au protocole d'archivage des Udaf, celles-ci sont tenues de verser certains documents aux Archives départementales. Dans ces cas, il est **recommandé d'informer la personne concernée ou ses représentants légaux de ce versement.** Ainsi, la communicabilité de ces documents tombe dans le droit commun.

2. RECOMMANDATIONS POUR LA NUMÉRISATION

Voir les références juridiques à la fin du document

La numérisation est le procédé technique consistant à passer d'une information ou donnée sur support papier vers un support numérique.

Les évolutions législatives suite à la loi 13 mars 2000[71], ont peu à peu conduit à donner au **document numérique** ou issu de la numérisation, la **même valeur ou force probante que le document natif papier.**

Depuis des décennies, de nombreuses normes, textes réglementaires sont apparus pour mieux encadrer le droit de la preuve. Aujourd'hui, l'article 1379 du Code civil rappelle que :

> *« La copie fiable a la même force probante que l'original. **La fiabilité est laissée à l'appréciation du juge**. Néanmoins est présumée fiable jusqu'à preuve du contraire toute copie résultant d'une reproduction **à l'identique de la forme et du contenu** de l'acte, et dont **l'intégrité est garantie dans le temps** par un procédé conforme à des conditions fixées par décret[72] en Conseil d'Etat. Si l'original subsiste, sa présentation peut toujours être exigée. »*

Concernant les associations, telles que les Udaf, l'enjeu de fiabilité est d'autant plus nécessaire et important, qu'une majeure partie des dossiers et documents produits dans le cadre des activités, sont considérés comme des documents d'archives publiques.

Le procédé technique et organisationnel doit être scrupuleusement encadré et contrôlé, notamment en cas de numérisation de dossiers et documents d'archives publiques par les Archives départementales.

Dans ce cadre, le SIAF (Service interministériel des Archives de France) a émis des recommandations dans un ***Vade-mecum*[73]*,*** afin de fournir des critères d'exigences pour autoriser ou non la destruction des archives publiques après leur numérisation.

Par ailleurs, pour les dossiers d'archives privées, suivre les recommandations de ce Vade-mecum peut être judicieux, car ces dossiers peuvent entrainer un certain nombre de risques, notamment en cas de litiges ou de réclamations ; d'où l'intérêt de bien maîtriser sa gestion documentaire et sa numérisation.

Un processus de numérisation conforme au Vade-mecum du SIAF, ou à la norme Z 42-026 est la condition sine qua non pour autoriser la destruction des dossiers papier après leur numérisation.

[71] Loi 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique

[72] Décret n° 2016-1673 du 5 décembre 2016 relatif à la fiabilité des copies

[73] *Autoriser la destruction de documents sur support papier après leur numérisation. Quels critères de décision* : Vade-mecum du Service interministériel des Archives de France, mars 2014, p. 7.

Le Vade-mecum du SIAF fait office de bonnes pratiques en matière de processus de numérisation. Il est la référence des archivistes professionnels du secteur public ou privé. Il se présente sous la forme du tableau ci-après.

RECOMMANDATIONS	ILLUSTRATIONS
1. Évaluer la valeur des documents originaux papier	Le Registre des traitements et le Protocole permettent d'évaluer la valeur des documents candidats potentiels à la numérisation : délais de prescription, données à caractère personnel
2. Encadrer le processus de numérisation par des règles	Quels dossiers papier ? Quels documents ? Quel volume ? Quel temps de préparation ? Quel périmètre pour le stock de reprise d'archives ? Par exemple : les dossiers actifs. Quel périmètre pour le flux ? Par exemple : le courrier entrant à partir d'une date donnée et sur un secteur donné. Prévoir d'exclure les documents contenant des données de santé ; par exemple : • Le certificat médical dans le cadre des dossiers MDPH • Le rapport social de signalement • L'autorisation aux actes de soins • L'ordonnance médicale ou la feuille de soins • L'arrêt maladie, le dossier médical pour admission en structure spécialisée • Le certificat médical circonstancié pour un renouvellement de mesure • Le certificat médical de non-retour au domicile • Le rapport annuel de situation s'il comporte des données de santé confidentielles
3. Encadrer les opérations de numérisation	Préciser les modalités concrètes des opérations de numérisation dans le processus : • Qui fait quoi : le donneur d'ordre (DO), l'opérateur de numérisation (OP), le fournisseur de l'outil de GED et de la chaîne de dématérialisation du stock et du flux, l'utilisateur, le contrôleur qualité, le Contrôleur scientifique (C. Patrimoine R 212-2) • Points de contrôle • Résultats des contrôles Il est également recommandé d'avoir établi le plan de classement des documents, ainsi que la liste des métadonnées caractérisant les documents numérisés. Le Vade-mecum préconise de collecter certains types de métadonnées : • Identifiant du dossier/document numérique • Index générés par l'outil métier ou par une autre application

RECOMMANDATIONS	ILLUSTRATIONS
	• Attributs relatifs aux délais de conservation et au sort final • Attributs relatifs aux droits d'accès et aux habilitations • Index de plan de classement (éventuellement) • Métadonnées techniques : lot de numérisation, Date de création, Date de Modification, Opérateur de numérisation, Identifiant du 1er document numérisé, Identifiant du dernier document numérisé.
4. Définir les modalités techniques de l'opération de numérisation	Les formats d'images choisis doivent reposer sur une norme ou un standard comme PDF/A-1, dans le but de garantir l'interopérabilité des systèmes et la pérennisation des données. Il faut également prévoir de définir en amont des règles de nommage des fichiers et répertoires. Pour l'étalonnage de la chaîne de numérisation, le Vade-mecum recommande une résolution a minima de 200 dpi avec une colorimétrie en couleurs RVB de 12 bits par pixel, voire 8 bits par pixel en couleurs indexées. Il est recommandé d'opter au maximum pour une compression sans perte ou avec un taux de compression limité. Le Vade-mecum recommande de générer pour chaque fichier une empreinte numérique afin de permettre les vérifications d'intégrité ultérieures. Seuls les documents dont la valeur probante est à démontrer feront l'objet de l'application de cette technologie. Le Vade-mecum préconise l'enregistrement des traces qui sont : • L'identifiant du 1er document ou du 1er lot numérisé et stocké de la journée • L'identifiant du dernier document ou du dernier lot numérisé et stocké de la journée • Le nombre total de pages traitées (au sens d'un traitement de post-numérisation pour améliorer la qualité des images par exemple) • Le nombre total de pages non traitées • Le nombre total de pages blanches
5. Assurer le contrôle de la numérisation	Contrôle sur : • La quantité de pages numérisées • La qualité et la fidélité des images par rapport aux originaux • La justesse des informations d'indexation Le Vade-mecum recommande de respecter des points de contrôle sur la qualité des images et la justesse des

RECOMMANDATIONS	ILLUSTRATIONS
	informations d'indexation, en précisant que le contrôle pourra être effectué par échantillonnage. Ce type de contrôle, eu égard à la quantité, ne peut être effectué que sur un échantillon représentatif. Pour cela, l'échantillon sera constitué suivant les recommandations de la norme NF ISO 2859-1. Pour la mise en place des mesures correctives, si le contrôle est défavorable, le Vade-mecum recommande de répéter l'opération (plan de contrôle double). En fonction des résultats du contrôle de plusieurs lots successifs, il peut également être décidé de réduire ou de renforcer les contrôles.
6. Garantir la sécurité des données	Voir Chapitre II. 5 « Le principe de sécurité et de confidentialité »
7. Garantir l'archivage sécurisé des données	Il s'agit ici de disposer d'une plateforme d'archivage numérique. Pour les fonctionnalités de cette plateforme, se reporter à la grille d'évaluation du SIAF.[74] On peut noter ici qu'il s'agit de documents dont la durée d'utilité administrative (DUA) est environ de 20 ans, pour les dossiers de PJM, notamment. Cela implique, au regard du Vade-mecum, de disposer d'une plateforme d'archivage numérique pour les associations ; étant donné la durée d'archivage légale. L'acquisition de ce type d'outil paraît indispensable en effet pour pouvoir conserver sur le long terme les dossiers numériques et ainsi pourvoir supprimer à partir de cette condition, les documents sur support papier. Les dossiers numériques clos pourront être archivés dans une GED, dans un espace dédié "Archives". Dans cet espace, les dossiers seront ainsi classés par année de clôture, l'association pourra indiquer aux Archives départementales, le nombre de dossiers clos par année civile, les Archives départementales se chargeront ensuite de calculer le taux d'échantillonnage et le nombre de dossiers à leur verser, en cas de procédure de tri. Ces versements pourront être effectués via un formulaire SEDA dans un Système d'archivage électronique à valeur probante des Archives départementales, dès lors que ces dernières en seront dotées et que la mise en œuvre des collectes numériques sera opérationnelle.

[74] https://francearchives.fr/fr/article/91524885

A retenir :

Tout processus de numérisation doit impérativement être scrupuleusement documenté et contrôlé en quantité et qualité, de façon à disposer de copies fiables et à pouvoir obtenir l'autorisation de détruire les documents papier après avoir contrôlé et validé leur numérisation. Se conformer au Vade-mecum du SIAF ou à la norme Z 42-026.

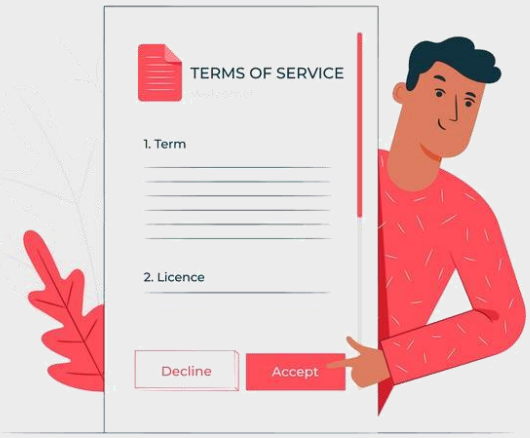
Une copie fiable est la juste reproduction à l'identique de l'original, dans la forme et le contenu, sans aucun traitement, comme la suppression des pages blanches ou des fonds de page.

Dans tous les cas, afin de déterminer quelle numérisation choisir, il faut adapter le procédé de numérisation à la valeur probante du document et non l'inverse.

Aucun logiciel n'est certifié Z42-026. Ce sont les processus de numérisation qui peuvent l'être. Actuellement, seul *Locarchives* a certifié des sites de numérisation. Il vaut mieux élaborer une Convention de Numérisation avec l'opérateur de numérisation (même en interne) et revoir le contrat du sous-traitant sur le stockage des données.

- → Un processus de numérisation est conforme si un contrôle sur la qualité et la quantité est garanti et mis en œuvre.
- → Le 7ème point des Bonnes Pratiques recommande de disposer d'une plateforme d'archivage numérique pour les dossiers dont la DUA est supérieure à 20 ans.
- → Actuellement, une minorité d'Archives départementales est dotée d'une plateforme d'archivage numérique. L'archivage continue donc à se faire sur le support papier, tant que les Archives départementales ne sont pas dotées d'une plateforme capable de collecter les données et fichiers automatiquement en numérique.

3. LES OBLIGATIONS DES SOUS-TRAITANTS



L'usage d'outils ou de logiciels développés[75] par des tiers dans le cadre de la mise en œuvre d'un traitement de données à caractère personnel reste sous la responsabilité de l'association, qui doit notamment vérifier que ces outils ou logiciels respectent les obligations que la loi met à sa charge.

L'association conserve la responsabilité des données à caractère personnel communiquées ou gérées par ses sous-traitants. Le contrat établi entre les parties doit mentionner les obligations incombant au sous-traitant en matière de préservation de la sécurité et de la confidentialité des données et prévoit que le sous-traitant ne peut agir que sur instructions du responsable de traitement.

Les contrats signés avec les sous-traitants doivent être clairs au niveau des principes de :

1. Minimisation des données dans la collecte
2. Chiffrement des données en cas de transfert (en Europe / hors d'Europe)
3. Anonymisation ou pseudonymisation après durée de conservation échue
4. Transparence, traçabilité et sécurité / assistance, alerte et conseil
5. Protection des données dès la conception et par défaut
6. Assistance, alerte et conseil

[75] Exemple de logiciels : *Kelio* pour le suivi des temps de travail et les absences, *PCPass Evolution* pour les contrôles d'accès.

1. Minimisation des données dans la collecte

→ En théorie

Article 5 du RGPD : «1. Les données à caractère personnel doivent être :
a) traitées de manière licite, loyale et transparente au regard de la personne concernée (licéité, loyauté, transparence) ;
b) collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités ; 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, conformément à l'article 89, paragraphe 1, comme incompatible avec les finalités initiales (limitation des finalités) ;
c) adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données) ;
d) exactes et, si nécessaire, tenues à jour ; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder (exactitude) (…) ».

→ En pratique

Il faut bien veiller à ce que les contrats des sous-traitant, responsables de la mise à disposition des outils informatiques, soient clairs et précis sur :

- Les données collectées : les contrats doivent clairement citer les types de données récoltées ; par exemple : les noms, prénom, date de naissance, numéro de compte bancaire… avec pour chaque type de donnée collectée, les raisons pour lesquelles celles-ci sont collectées ;
- La façon dont ils collectent les données sources : API, dépôt sur des boîtes mail, sur serveur FTP (File Transfert Protocol (Protocole de transfert de fichier)) ;
- La périodicité de réactualisation de la collecte des données sources ;
- Ce qui est prévu en termes de conservation limitée : les mécanismes prévus pour calculer une durée de stockage des données après un événement déclencheur comme la clôture d'un mandat judiciaire ;
- Faire supprimer au maximum les champs de textes libres présents dans les logiciels : il est fréquent de voir consigner dans les zones de « commentaires » ou zones de champs libres des informations très sensibles, il faut donc les éviter au maximum !

Si les contrats sont clairs sur ces éléments et que les mécanismes mis en place ont pu être testés et prouvés, les principes peuvent être considérés comme suivis. Il faudra veiller à consigner scrupuleusement ces éléments dans le registre de traitement que le DPO doit mettre à jour.

2. Chiffrement des données en Europe et hors d'Europe

Le chiffrement des données[76], notamment des données sensibles, en cas de transfert de ces données est un principe de sécurisation très important à mettre en œuvre pour tout mouvement ou migration des données en Europe.

Le stockage des données hors d'Europe doit être proscrit. Ce qui exclut *de facto* les éditeurs ou sous-traitants qui effectuent le stockage hors d'Europe. Dans le même ordre d'idée, on évitera tout logiciel dit « gratuit » qui ne garantit aucune sécurisation des données.

[76] Le chiffrement des données permet de protéger la confidentialité des données en les encodant sous une forme qu'il est impossible de déchiffrer sans la clé adéquate.

3. Anonymisation ou pseudonymisation[77] après durée de conservation échue

→ En théorie

Extrait de l'*Article 5 du RGPD* : *« Les données à caractère personnel doivent être :*

e) 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; les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises par le présent règlement afin de garantir les droits et libertés de la personne concernée (limitation de la conservation) ».

→ En pratique

Les contrats des sous-traitants doivent préciser ce qui est prévu après l'échéance de la durée limitée de conservation : anonymisation /pseudonymisation, effacement des données dans l'outil de gestion ou versement des données dans un outil d'archivage sécurisé et conforme.

Les données d'archives publiques sont protégées dans leur intégrité de tout effacement, anonymisation ou pseudonymisation. Seules les Archives départementales peuvent y procéder.

Dans ce cas, un **mécanisme automatique de purge** à l'expiration de la durée de conservation est **à proscrire.** Il convient de se rapprocher des Archives départementales. Le responsable de traitement peut dans ce cas demander au sous-traitant de prévoir un mécanisme « d'isolement » dans un répertoire sécurisé accessible uniquement de l'administrateur de l'outil pour les données ayant dépassé la durée de conservation requise.

4. Transparence, traçabilité et sécurité

→ En théorie

Les sous-traitants doivent tenir un registre des activités de traitement effectuées pour le compte de leurs clients. Dans certains cas, ils devront désigner un DPO dans les mêmes conditions qu'un responsable de traitement.

Extrait de l'*Article 5 du RGPD* : *« Les données à caractère personnel doivent être :*

f) traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité) ;

Article 32 du RGPD : Sécurité du traitement

« Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins :

a) la pseudonymisation et le chiffrement des données à caractère personnel ;

[77] L'anonymisation est un processus compliqué qui ne doit pas être confondu avec la pseudonymisation. Pour aller plus loin, cf. https://www.cnil.fr/fr/lanonymisation-de-donnees-personnelles

b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
c) des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;
d) une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement ».

→ En pratique

Le sous-traitant doit s'engager à prendre toutes les mesures concernant les incidents et les failles de sécurité. Le registre des traitements peut être une annexe à ce contrat. L'association doit veiller à ce que le contrat détaille bien ce qui est prévu en matière :

- d'incidents
- de restitution des données
- d'hébergement
- de sous-traitance
- de sécurité
- de personnel
- de réversibilité des données
- de confidentialité
- d'assurance responsabilité

L'article 32 du RGPD recommande au responsable du traitement, avec l'aide de son ou ses prestataires sous-traitants de procéder à une analyse des risques pour l'ensemble des traitements. Il doit ensuite adapter les moyens à mettre en place en fonction des résultats de cette analyse.
L'étape préalable de registre des traitements est donc le prérequis nécessaire à cette étape d'évaluation des risques et de mise en sécurité par les moyens adéquats.

5. Protection des données, dès la conception et par défaut

→ En théorie

Article 25 du RGPD : Protection des données dès la conception et protection des données par défaut
« Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, que présente le traitement pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, qui sont destinées à mettre en œuvre les principes relatifs à la protection des données, par exemple la minimisation des données, de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du présent règlement et de protéger les droits de la personne concernée.
Le responsable du traitement met en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées. Cela s'applique à la quantité de données à caractère personnel collectées, à l'étendue de leur traitement, à leur durée de conservation et à leur accessibilité. En particulier, ces mesures garantissent que, par défaut, les données à caractère personnel ne sont pas rendues accessibles à un nombre indéterminé de personnes physiques sans

l'intervention de la personne physique concernée.
Un mécanisme de certification approuvé en vertu de l'article 42 peut servir d'élément pour démontrer le respect des exigences énoncées aux paragraphes 1 et 2 du présent article ».

→ En pratique

Le sous-traitant doit garantir à l'association qu'il respecte le RGPD et protège les droits des personnes concernées. Cela signifie notamment que :

1. **dès leur conception**, les applications ou services offerts, intègrent de façon effective les principes relatifs à la protection des données.
2. **par défaut,** les outils, produits, applications ou services garantissent que seules sont traitées les données nécessaires à la finalité du traitement au regard de la quantité de données collectées, de l'étendue de leur traitement, de la durée de conservation et du nombre de personnes qui y a accès.

6. Assistance, alerte et conseil

→ En théorie

Article 33 du RGPD : Notification à l'autorité de contrôle d'une violation de données à caractère personnel
« En cas de violation de données à caractère personnel, le responsable du traitement en notifie la violation en question à l'autorité de contrôle compétente conformément à l'article 55, dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques. Lorsque la notification à l'autorité de contrôle n'a pas lieu dans les 72 heures, elle est accompagnée des motifs du retard.
Le sous-traitant notifie au responsable du traitement toute violation de données à caractère personnel dans les meilleurs délais après en avoir pris connaissance ».

→ En pratique

Comme énoncé précédemment, le sous-traitant doit clairement s'engager, dans son contrat, à prendre toutes les mesures de sécurité concernant les incidents et les failles de sécurité.

Le sous-traitant doit par exemple notifier au responsable du traitement toute violation de données à caractère personnel dans les meilleurs délais après en avoir pris connaissance.

Le sous-traitant aide le responsable de traitement pour la réalisation d'analyses d'impact relatives à la protection des données et pour la réalisation de la consultation préalable de l'autorité de contrôle (CNIL).

4. NOTE PRATIQUE POUR LES PROFESSIONNELS DANS LE CADRE DE L'ACCOMPAGNEMENT

- **J'informe en toute transparence**

Pourquoi je collecte, qu'est-ce que je collecte, que vais-je en faire, pour combien de temps, j'indique à la personne qu'elle peut y avoir accès, s'y opposer, rectifier, effacer.

- **Je demande le moins d'informations possible**

Ne collectez que les données nécessaires, uniquement celles qui sont nécessaires pour accomplir une tâche prévue dans le cadre de l'accompagnement. Il faut toujours se poser les questions suivantes : quelle est l'utilité des informations recueillies pour le projet de la personne ? Est-ce que les données que je collecte sont nécessaires au regard de la finalité poursuivie par le traitement ?

Un bénévole « Lire et Faire lire », n'a pas besoin de récupérer le numéro de sécurité sociale d'une personne.

- **Je reste discret**

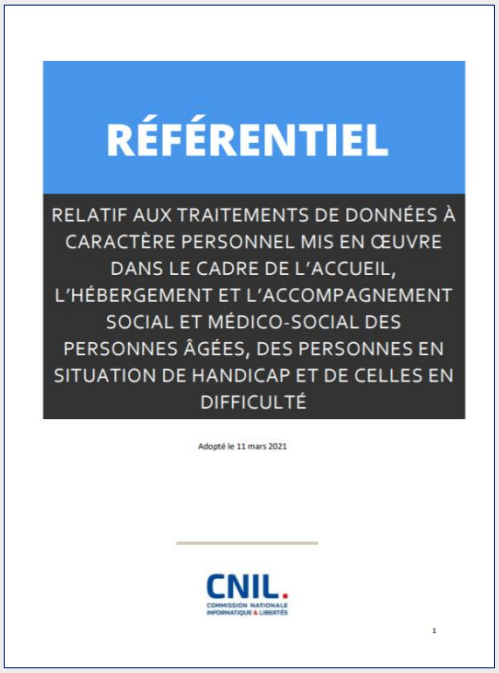
En tant que professionnel vous êtes soumis à une obligation de confidentialité, notamment concernant les informations fournies par la personne.

La discrétion va jusqu'à ne pas laisser des documents au photocopieur, fermer ses armoires le soir, faire attention aux fichiers joints dans les mails,…

- **Je fais attention à la rédaction des documents**

L'ensemble des écrits contenus dans le dossier de la personne doit être précis, neutre, clair et lisible. Ces écrits doivent éviter tout jugement ou interprétation.
La formalisation des données doit suivre une écriture exigeante et consciente des conséquences sur la personne susceptible d'en prendre connaissance et de son ressenti.

5. PRÉSENTATION DU RÉFÉRENTIEL SOCIAL ET MEDICO-SOCIAL DE LA CNIL



Ce référentiel s'adresse aux professionnels du secteur social et médico-social mettant en œuvre des **traitements relatifs à l'accompagnement et au suivi social et médico-social des personnes âgées, en situation de handicap et en difficultés.**

Instrument de régulation « souple » essentiel, il a vocation à donner davantage de sécurité juridique aux organismes et répond à deux objectifs principaux :

→ guider les professionnels dans leurs démarches de mise en conformité ;

→ constituer une aide à la réalisation d'une analyse d'impact relative à la protection des données (AIPD) dans le cas où celle-ci est nécessaire.

Ce nouveau référentiel reprend la plupart du contenu des autorisations et actes réglementaires uniques relatifs à l'accompagnement et au suivi social et médico-social des personnes âgées, en situation de handicap et en difficultés et notamment les traitements mis en œuvre dans le cadre de :

- → l'accompagnement et au suivi social et médico-social des personnes handicapées et des personnes âgées (AU-47) ;
- → l'accompagnement et au suivi social et médico-social des personnes en difficultés (AU-48) ;
- → l'enregistrement et l'instruction des prestations, le suivi des décisions prises et leur mise en œuvre au sein des Maisons Départementales des Personnes Handicapées (MDPH) (RU-05) ;
- → la gestion de l'Allocation personnalisée d'autonomie (APA) et de l'Aide sociale à l'hébergement (ASH) (RU-63).

Ces anciennes autorisations et actes réglementaires étant dépourvus de valeur juridique depuis le 25 mai 2018, ce référentiel a vocation à couvrir l'ensemble des traitements susvisés**.**

Vous trouverez ce document sur le site de la CNIL : https://www.cnil.fr/fr/publication-du-referentiel-pour-la-prise-en-charge-medico-sociale-personnes-agees-handicap-difficulte

RÉFERÉNCES JURIDIQUES

RGPD, loi informatique et libertés et délibérations de la CNIL

- Règlement (UE) 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel
- Loi n°78-17 « Informatique et Libertés » du 6 janvier 1978 modifiée
- Loi n°2016-1321 du 7 octobre 2016, pour une République numérique
- Décret n°2019-536 du 29 mai 2019, pris pour l'application de la loi de 1978 relative à l'informatique, aux fichiers et aux libertés
- Délibération n° 2018-326 du 11 octobre 2018, sur les lignes directrices des analyses d'impact sur la protection des données (AIPD)
- Délibération n°2018-327 du 11 octobre 2018, sur les types d'opérations de traitement avec analyse d'impact sur la protection des données
- Délibération n° 2021-028 du 11 mars 2021 portant adoption d'un référentiel relatif aux traitements de données à caractère personnel mis en œuvre dans le cadre de l'accueil, l'hébergement et l'accompagnement social et médico-social des personnes âgées, des personnes en situation de handicap et de celles en difficulté

Le traitement des données sensibles

- Article 9 du RGPD
- Article 6 de la loi « Informatique et Libertés »

Le traitement des données relatives aux infractions, condamnations et mesures de sûreté

- Article 10 du RGPD
- Article 46 de la loi « Informatique et Libertés »
- Article 76 du décret n° 2019-536 du 29 mai 2019

Le dépôt d'archives publiques auprès de tiers-archiveurs

- Articles L 212-4 et R 212-19 à R 212-31 du Code du patrimoine
- Arrêté ministériel du 4 décembre 2009, précisant les normes relatives aux prestations en archivage et gestion externalisée
- Articles L 1111-8, R 1111-9 à R 1111-15-1 et R 1111-16 du Code de la santé publique, (relatifs à l'hébergement des données de santé à caractère personnel par des personnes physiques ou morales agréés à cet effet)
- Ordonnance n°2017-27 du 12 janvier 2017, relative à l'hébergement des données de santé à caractère personnel

Le principe de sécurité et de confidentialité

- Article 32 du RGPD
- Loi n°2000-230 du 13 mars 2000, portant adaptation du droit de la preuve aux technologies de l'information et relatif à la signature électronique, modifiant le Code civil
- Ordonnance n°2005-1516 du 8 décembre 2005, relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives

- Ordonnance n° 2017-29 du 12 janvier 2017, relative aux conditions de reconnaissance de la force probante des documents comportant des données de santé à caractère personnel créés ou reproduits sous forme numérique et de destruction des documents conservés sous une autre forme que numérique
- Décret n°2010-112 du 2 février 2010, pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005, relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives
- NF Z 42-013 (ISO 14641-1) Spécifications relatives à la conception et à l'exploitation de systèmes d'informatiques en vue d'assurer la conservation et l'intégrité des documents stockés dans ces systèmes
- NF Z 42-020, Spécifications fonctionnelles d'un composant Coffre-Fort Numérique destiné à la conservation d'informations numériques dans des conditions de nature à en garantir leur intégrité dans le temps
- NF ISO/IEC 27001, Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences
- ISO 15489-1 : 2016, Information et documentation « Records management » - Partie 1 : Principes directeurs – Partie 2 : Guide pratique

Le droit à l'information

- Article 3 de la charte des droits et libertés de la personne accueillie
- Article 48 de la loi « Informatique et Libertés »
- Articles 12, 13 et 14 du RGPD
- Article L 311-3 du CASF

Le droit d'accès

- Article 15 du RGPD
- Article 49 de la loi « Informatique et Libertés »
- Article L 1111-7 du Code de la santé publique
- Article 514 du Code civil

Le droit de rectification

- Article 16 du RGPD
- Article 50 de la loi « Informatique et Libertés »

Le droit d'opposition

- Article 21 du RGPD
- Article 56 de la loi « Informatique et Libertés »

Le droit à l'oubli

- Article 17 du RGPD
- Article 51 de la loi « Informatique et Libertés »

Le droit à la limitation de traitement

- Article 18 du RGPD
- Article 53 de la loi « Informatique et Libertés »

Le droit à la portabilité des données

- Article 20 du RGPD
- Article 55 de la loi « Informatique et Libertés »

La numérisation

Références juridiques

- Article 1379 du Code civil
- Loi n°2000-230 du 13 mars 2000, portant adaptation du droit de la preuve aux technologies de l'information et relatif à la signature électronique, modifiant le Code civil
- Ordonnance n°2005-1516 du 8 décembre 2005, relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives
- Ordonnance n° 2017-29 du 12 janvier 2017, relative aux conditions de reconnaissance de la force probante des documents comportant des données de santé à caractère personnel créés ou reproduits sous forme numérique et de destruction des documents conservés sous une autre forme que numérique
- Décret n° 2016-1673 du 5 décembre 2016, relatif à la fiabilité des copies et pris pour l'application de l'article 1379 du Code civil
- Décret n°2010-112 du 2 février 2010, pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005, relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives

Références normatives

- NF Z42-026 : 2017-05, Définition et spécifications des prestations de numérisation fidèle de documents sur support papier et contrôle de ces prestations
- NF Z 42-013 (ISO 14641-1), Spécifications relatives à la conception et à l'exploitation de systèmes d'informatiques en vue d'assurer la conservation et l'intégrité des documents stockés dans ces systèmes
- NF ISO 2859-1, Règles d'échantillonnage pour le contrôle par attributs – Partie 1 : Procédures d'échantillonnage pour les contrôles lot par lot
- Autoriser la destruction de documents sur support papier après leur numérisation. Quels critères de décision : Vade-mecum du Service interministériel des Archives de France, mars 2014
- ISO 23081-1 :2017, Information et documentation – Processus de gestion des documents d'activité – Métadonnées pour les documents d'activité
- NF ISO 30300, Information et documentation – Systèmes de gestion des documents d'activité – Principes essentiels et vocabulaire

FOIRE AUX QUESTIONS

ARCHIVAGE[78]

Pourquoi archiver des documents ?

Les enjeux juridiques

La loi française oblige les organismes à conserver leurs archives pendant une durée minimale. Ce délai de conservation, qui varie selon la nature des documents, peut aller jusqu'à cent-vingt ans. L'archivage permet de protéger ses droits en cas de contentieux et de justifier son activité lors d'un contrôle. L'archivage permet également de se plier aux exigences légales en matière de tri, de conservation et de communication des documents. Enfin, pour avoir une valeur probante, il est indispensable de pouvoir justifier de l'authenticité et de l'intégrité des archives.

Les enjeux de sécurité

L'archivage ne doit pas compromettre la sécurité des archives, en particulier celles qui contiennent des informations à caractère sensible. C'est pourquoi sécuriser les lieux de stockage des archives, physiques ou numériques, est une priorité. Les sites de conservation doivent par exemple être protégés des sinistres et des intrusions. Les solutions d'archivage numérique doivent quant à elles disposer de plusieurs outils de sécurité (mot de passe, pare-feu, traçabilité, etc.).

Les enjeux financiers

Le temps consacré à la recherche d'archives, le non-respect de la législation en vigueur et les logiciels obsolètes peuvent engendrer des coûts élevés. L'archivage induit un gain de temps par une meilleure efficacité dans la recherche des documents ainsi qu'un gain d'espace et une optimisation des coûts.

Les enjeux technologiques

La pérennité des données, la capacité des systèmes à opérer entre eux ou encore la réversibilité des formats sont des problématiques auxquelles sont confrontées la plupart des organismes. Elles sont prises en compte par les systèmes d'archivage qui en font une priorité.

Les enjeux historiques

Certaines archives ont une grande valeur d'un point de vue patrimonial. D'ailleurs, certaines archives ne sont pas détruites en raison de leur intérêt historique et sont conservées dans le but d'être valorisées pour être consultées par exemple par des chercheurs, historiens, biographes, etc.

[78] Cette foire aux questions a été constituée à partir de l'expertise d'une archiviste et de sites internet multiples :
- https://archives.ille-et-vilaine.fr/fr/article/foire-aux-questions-sur-l-archivage#
- https://www.novarchive.fr/faq/

Qu'est-ce qu'un bon archivage ?

Un **bon archivage c'est** :

1. Le **respect de la réglementation** et des **procédures** (cf. protocole d'archivage des Udaf)
2. La **mise en boîte des dossiers** au fur et à mesure de la fin des projets, des dispositifs, des années
3. Des **boîtes** dont le **contenu est clairement renseigné** : sujet et dates extrêmes au minimum
4. Des **opérations de tri régulières** pour éviter l'encombrement

Quelles sanctions encourues en cas de destruction abusive d'archives ?

Tout producteur d'archives publiques est **responsable des documents qu'il produit ou reçoit**, mais il n'en est **pas propriétaire** : il est **tenu de les remettre au service d'archives chargé de les conserver.**
En effet, **les archives publiques sont imprescriptibles et inaliénables** : elles font partie du **domaine public mobilier** et ne peuvent être **ni aliénées ni détruites sans autorisation de l'État** (ministère de la Culture, représenté par le directeur des Archives de France). **Toute infraction à ce principe** ainsi que **tout détournement d'archives publiques** sont passibles **d'amendes et de peines d'emprisonnement** (loi n°2008-696, art. 19).

Comment savoir à quel(s) prestataire(s) extérieur(s) faire appel pour externaliser des archives publiques intermédiaires ?

Attention ! L'**externalisation d'archives publiques** n'est possible **qu'auprès de prestataires agréés par le ministère de la Culture**. La liste des entreprises agréées est disponible **sur le site internet du Service interministériel des Archives de France.**

Quand faut-il archiver ?

En premier lieu, l'**archivage** est un **moyen pour les associations concernées** de remplir leurs **obligations en matière d'archives**, depuis les mesures prises **pour assurer leur bonne conservation et organisation**, jusqu'à **leur élimination réglementaire** ou **leur versement**. De plus, un **archivage régulier évite l'encombrement** des espaces de préarchivage, de même que les risques de détérioration ou de pertes d'archives. Il permet également de **maîtriser les coûts engendrés** par le stockage. Il est recommandé de procéder à des **opérations de tri entre une à deux fois par an** jusqu'à tous les deux ans, en fonction des volumes.
Il est essentiel de vérifier régulièrement la DUA des documents (cf. protocole d'archivage des Udaf). Certains logiciels d'archivage prévoient un rappel automatique de ces délais.

Que doit-on faire des documents lorsque leur DUA arrive à leur terme ?

Les archives dont la DUA est expirée doivent être versées aux Archives départementales ou détruites après la délivrance d'un visa d'élimination par les Archives départementales.
Il est recommandé aux associations concernées de ne pas laisser au prestataire de stockage d'archives intermédiaires le dossier mais de le rapatrier dans leurs locaux dans l'attente de la décision des Archives départementales.

Après la destruction d'un dossier, quelle est la trace minimale qu'il est possible de conserver ?

Les données sont anonymisées ou détruites dans les systèmes informatiques dès lors que la demande de destruction aura été signée**. Il faut juste conserver les preuves de destruction.**

Que faire en cas de situation hybride : mi papier mi numérique ?

Dans ce cas**, il est préconisé de rédiger des règles et des processus dans des documents écrits en indiquant notamment les documents candidats à la numérisation.**

Les documents originaux papier auront toujours la force probante et **on ne doit supprimer aucun document papier numérisé sans l'accord de l'autorité des archives publiques** ; a fortiori, quand la numérisation n'est pas fidèle. (cf. en annexe les recommandations pour la numérisation)

En cas de dossiers d'archives à verser aux Archives départementales, il faudra voir au cas par cas. Quoiqu'il en soit, les versements d'archives se font plutôt encore aujourd'hui sur support papier et la plupart des Archives départementales préconisera des modalités de tri (d'échantillonnage) très précises. Mais là encore, **il est recommandé, en particulier pour les Udaf, de se rapprocher de leur directeur-trice des Archives départementales afin de valider les préconisations décidées**, comme précisé dans le protocole d'archivage.

Comment vérifier la fiabilité d'une numérisation ?

Sur cette thématique la norme Z42-013 est en refonte. Pour la copie formelle, **se focaliser sur la norme Z42-026.**

Attention, très peu de prestataires donnent actuellement les garanties sur la numérisation fidèle !

Cette question est traitée par les bonnes pratiques (cf. en annexe les recommandations pour la numérisation) : **si vous avez un 7/7, vous avez un processus conforme.**

Quelles différences entre GED, SAE et coffre-fort électronique ?

La GED (gestion électronique de documents) : l'organisation des contenus numériques vivants et modifiables

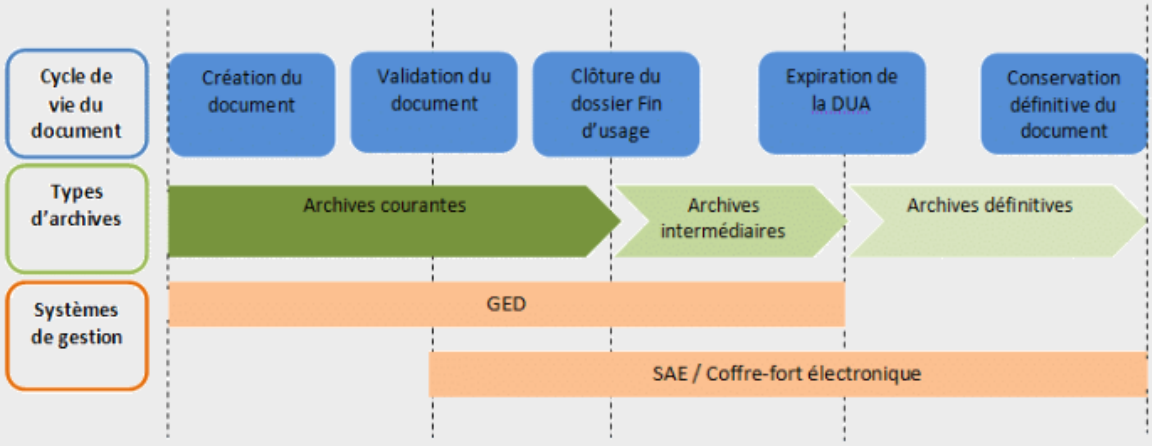
La GED est un outil informatisé dont l'objectif est de gérer les archives pour la conduite quotidienne des activités (téléchargement, modification, partage, suppression, etc.) et non d'assurer leur conservation avec les gages d'authenticité et de pérennité. Elle contribue à améliorer l'échange et la manipulation des informations au sein d'un organisme notamment en créant plusieurs versions d'un même document.

Le SAE (système d'archivage électronique) : la conservation des documents figés et validés

Le SAE va au-delà du simple stockage des données archivées. Il intègre en outre les règles de gestion documentaire définies par l'organisme (durée de conservation, typologie de document, niveau de confidentialité, etc.). Il permet la conservation, la consultation et la restitution des documents papiers ou données électroniques dans le temps en garantissant leur intégrité et leur pérennité.

Le coffre-fort électronique, un espace pour sécuriser les archives

Le coffre-fort électronique est un élément complémentaire au SAE. Il est d'ailleurs plus commun de parler de composant coffre-fort électronique (CCFN), terme utilisé dans la norme NF Z 42-020. A l'instar d'un coffre-fort physique, c'est un espace ultra sécurisé destiné à protéger les documents et à leur concéder une valeur probante. Il permet de contrôler les accès et d'assurer la traçabilité et l'authenticité d'une archive, prérequis indispensables pour qu'un document électronique soit accepté comme élément de preuve en justice. Le coffre-fort électronique ne peut se substituer à une GED car il ne permet pas la gestion courante d'un document.



Les archives versées aux Archives départementales sont-elles accessibles immédiatement à tout le monde ?

En principe, **les archives sont accessibles immédiatement** à chaque citoyen qui en fait la demande. **Mais** pour protéger certaines informations, la loi de 2008 sur les archives a **mis en place des délais de communicabilité** avant lesquels certaines archives ne sont pas communicables. Les **principaux délais** sont les suivants :

1. **Protection du secret industriel et commercial : 25 ans**
2. **Protection de la vie privée : 50 ans**
3. **Sûreté de l'Etat : 50 ans**
4. **Jugements à huis clos : 75 ans, 100 ans dans le cas d'affaires évoquant l'intimité sexuelle des personnes et des mineurs**
5. **Informations médicales : 120 ans**

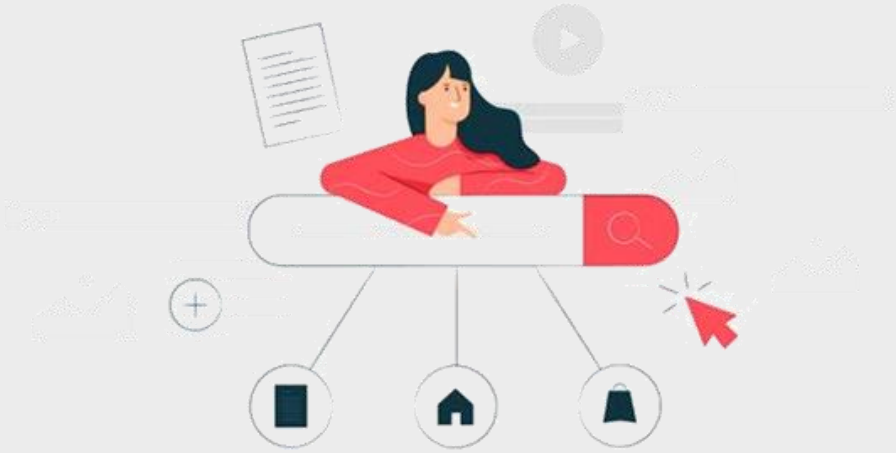
Les agents des Archives départementales sont-ils soumis au secret professionnel ?

Oui, en vertu du ***Code du Patrimoine*** qui précise que **« Tout fonctionnaire ou agent de la collecte ou conservation d'archives en application des dispositifs de la présente loi est tenu au secret professionnel en ce qui concerne tout document qui ne peut être légalement mis à la disposition du public ».**

Combien de temps les Archives départementales gardent-elles les archives ?

Ad vitam aeternam ! Seules les **archives dites définitives**, présentant un **intérêt historique ou un intérêt juridique majeur** entrent **aux Archives départementales,** pour y être **conservées indéfiniment**. Les tris sont faits en amont, en application de la réglementation.

POUR ALLER PLUS LOIN



Annuaires/contacts

- **Annuaire des Archives départementales de France**
  → https://francearchives.fr/fr/annuaire/departements
- **Prestataires agréés pour la conservation d'archives publiques courantes et intermédiaires sur support papier**
  → https://francearchives.fr/fr/article/26287438
- **Prestataires agréés pour la conservation d'archives publiques courantes et intermédiaires sur support numérique**
  → https://francearchives.fr/fr/article/26287437

Sites internet/outils

- **Site internet de la CNIL,** il propose de nombreux contenus pour ceux qui souhaiteront accéder à une documentation plus technique et plus complète
  → https://www.cnil.fr/professionnel

  - MOOC gratuit de la Cnil sur le RGPD
    https://www.cnil.fr/fr/la-cnil-lance-sa-formation-en-ligne-sur-le-rgpd-ouverte-tous
  - Modèles de courrier pour exercer ses droits
    https://www.cnil.fr/fr/modeles/courrier
  - Le guide du sous-traitant
    https://www.cnil.fr/sites/default/files/atoms/files/rgpd-guide_sous-traitant-cnil.pdf
  - Un kit d'information à destination des travailleurs sociaux pour protéger les données de vos publics
    https://www.cnil.fr/fr/travailleurs-sociaux-un-kit-dinformation-pour-proteger-les-donnees-de-vos-publics
  - Document synthétique qui résume les 6 étapes à mettre en œuvre pour se conformer au RGPD
    https://www.cnil.fr/sites/default/files/atoms/files/pdf_6_etapes_interactifv2.pdf
  - Exemple de registre des activités de traitement
    https://www.cnil.fr/fr/RGDP-le-registre-des-activites-de-traitement
  - Respecter les droits des personnes
    https://www.cnil.fr/fr/respecter-les-droits-des-personnes

- Une foire aux questions sur le RGPD
  https://www.cnil.fr/fr/cnil-direct/thematique/reglement-europeen

- **Site internet gouvernemental de cybermalveillance,** en cas de difficultés (un sinistre, une attaque informatique, etc.), ce site vous propose de l'aide en ligne ainsi qu'une liste de prestataires agréées
  → https://www.cybermalveillance.gouv.fr/
  - Les bonnes pratiques relatives à toute menace liée à la cybermalveillance
    https://www.cybermalveillance.gouv.fr/bonnes-pratiques

- **Site internet de l'association Française des Correspondants à la protection des Données à caractère Personnel (AFCDP)**
  → https://afcdp.net/

- **Site internet de l'Anap,** qui met à disposition un kit sur le RGPD avec plusieurs ressources et outils
  → http://ressources.anap.fr/numerique/publication/2727

- **Foire aux questions sur l'archivage :**
  → Novarchive *:* https://www.novarchive.fr/faq/
  → Site des Archives départementales d'Ille-et-Vilaine : https://archives.ille-et-vilaine.fr/fr/article/foire-aux-questions-sur-l-archivage

Vidéos

- RGPD : la FAQ dessinée, en collaboration avec la CNIL
  → https://www.youtube.com/watch?v=OUMGp3HHel4
- Comment mettre en place un système d'archivage électronique en 7 étapes ?
  → https://www.youtube.com/watch?v=Akl53x6D38Q
- MOOC 1 : archivage électronique : les fondamentaux
  → https://www.youtube.com/watch?v=kX2kOCoRkUA
- « La minute RGPD » (série de vidéos sur divers sujets du RGPD)
  - L'analyse d'impact sur la vie privée
    https://www.youtube.com/watch?v=BSFk9qlZmIU&list=PLoyBmLLsaxZde-8GuyUtQWW_uavmJNoEd&index=1
  - Les missions du DPO
    https://www.youtube.com/watch?v=9Q6Ik_7-oiE&list=PLoyBmLLsaxZde-8GuyUtQWW_uavmJNoEd&index=2

- Le recueil du consentement
  https://www.youtube.com/watch?v=PkVNL8YW_F0&list=PLoyBmLLsaxZde-8GuyUtQWW_uavmJNoEd&index=3
- Le droit à l'oubli
  https://www.youtube.com/watch?v=9iT1yawfHIQ&list=PLoyBmLLsaxZde-8GuyUtQWW_uavmJNoEd&index=4
- L'archivage
  https://www.youtube.com/watch?v=0t7EaibmAIs&list=PLoyBmLLsaxZde-8GuyUtQWW_uavmJNoEd&index=5
- La vidéosurveillance au travail
  https://www.youtube.com/watch?v=tJioAISODfw
- Violation de données personnelles
  https://www.youtube.com/watch?v=14apf19LOUk&list=PLoyBmLLsaxZde-8GuyUtQWW_uavmJNoEd&index=7
- Le contrat de sous-traitance
  https://www.youtube.com/watch?v=nzWxBZoXCtw

Ouvrages/guides

- HAAS Gérard, HURSTEL Alric, *Sécuriser les données personnelles dans le secteur social et médico-social,* collection Les Guides Direction(s), avril 2019

- Kit d'information à destination des établissements médico-sociaux, *Se familiariser avec le RGPD*, fiches pratiques de la Fédération Hospitalière de France, septembre 2018, disponible sur https://www.cerep-phymentin.org/Association/Qualite/Actualites_de_la_qualite/fhf_guide_medico_social.pdf

LISTE DES SIGLES

AIPD	Analyse d'Impact Relative à la Protection des Données
ANAS	Association Nationale des Assistants de service Social
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
API	Application Programming Interface (Interface applicative de programmation)
CAF	Caisse d'Allocations Familiales
CNIL	Commission Nationale de l'Informatique et des Libertés
CPME	Confédération des Petites et Moyennes Entreprises
CRPA	Code des Relations entre le Public et l'Administration
CSP	Code de la Santé Publique
DIPM	Document Individuel de Protection des Majeurs
DMP	Dossier Médical Partagé
DPF	Délégué aux Prestations Familiales
DPO	Délégué à la Protection des Données
FTP	File Transfert Protocol (Protocole de transfert de fichier)
GED	Gestion Electronique des Documents
MDPH	Maison Départementale des Personnes Handicapées
MJAGBF	Mesure Judiciaire d'Aide à la Gestion du Budget Familial
MJPM	Mandataire Judiciaire à la Protection des Majeurs
PCA	Plan de Continuité d'Activité
RGPD	Règlement Général sur la Protection des Données
RSA	Revenu de Solidarité Active
Unaf	Union Nationale des Associations Familiales
Udaf	Union Départementale des Associations Familiales
SIAF	Service Interministériel des Archives de France

GLOSSAIRE

Toutes les définitions inscrites dans ce glossaire sont issues du site internet de la CNIL et de Frances Archives.

Sélectionnez une lettre

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Archives	Documents, quels que soient leur date, leur forme et leur support matériel, produits ou reçus par toute personne physique ou morale, et par tout service ou organisme public ou privé, dans l'exercice de leur activité. Le mot archives est couramment employé dans le sens restrictif de documents ayant fait l'objet d'un archivage, par opposition aux archives courantes.
Archives courantes	Dans le cycle de vie des archives, documents qui sont d'utilisation habituelle et fréquente pour l'activité des services, établissements et organismes qui les ont produits et reçus, et qui sont conservés pour le traitement des affaires.
Archives définitives	Dans le cycle de vie des archives, documents qui, ayant subi des tris, ne sont plus susceptibles d'élimination, par opposition aux archives courantes ou intermédiaires, et qui sont conservés pour les besoins de la gestion et de la justification des droits des personnes physiques ou morales, publiques ou privées, et pour la documentation historique de la recherche.
Archives départementales	En France, l'expression « Archives départementales » désigne à la fois l'administration chargée de la gestion des archives produites dans un département et le bâtiment où ces archives sont conservées et consultables par le public.
Archives intermédiaires	Dans le cycle de vie des archives, documents qui, n'étant plus d'usage courant, doivent être conservés temporairement, pour des besoins administratifs ou juridiques (y compris les documents qui après tri seront conservés comme des archives définitives).
Archives publiques	Ce sont « les documents qui procèdent de l'activité, dans le cadre de leur mission de service public, de l'Etat, des collectivités territoriales, des établissements publics et des autres personnes morales de droit public ou des personnes de droit privé chargées d'une telle mission. […] »[79] « Les archives publiques sont imprescriptibles. Nul ne peut détenir sans droit ni titre des archives publiques.»[80] À l'expiration de leur période d'utilisation courante, les archives publiques font l'objet d'une sélection pour séparer les documents à conserver des documents dépourvus d'utilité administrative ou d'intérêt historique ou scientifique, destinés à l'élimination.

[79] Extrait du *Code du patrimoine*, art. L211-4.
[80] Extrait du *Code du patrimoine*, art. L212-1.

Archives privées	Ce sont les documents qui procèdent du fonctionnement propre des organismes privés (exemples : les dossiers individuels de personnel, les dossiers internes des associations tels que des notes stratégiques de Commissions internes, de services, des bilans annuels, des communiqués, des dossiers de réclamations ou de contentieux, des plans immobiliers, des dossiers de Mandat de Protection Future,…).
Base légale	La base légale d'un traitement est ce qui autorise légalement sa mise en œuvre, ce qui donne le droit à un organisme de traiter des données à caractère personnel. On peut également parler de « fondement juridique » ou de « base juridique » du traitement. Six bases légales sont prévues par le RGPD : • le consentement ; • le contrat ; • l'obligation légale ; • la sauvegarde des intérêts vitaux ; • l'intérêt public ; • les intérêts légitimes.
Bordereau d'élimination	Etat des documents soumis par un service producteur au visa d'élimination de l'archiviste, ou proposés pour l'élimination par un service d'archives au service dont émanent les documents.
Bordereau de versement	Pièce justificative de l'opération de versement comportant le relevé détaillé des documents ou dossiers remis à un service d'archives par un service versant ; le bordereau de versement tient lieu de procès-verbal de prise en charge et d'instrument de recherche.
Certification	C'est une procédure par laquelle un organisme d'évaluation externe (appelé également tiers certificateur) va donner l'assurance écrite qu'une personne, un produit, un processus ou un service est en conformité avec les exigences données dans un référentiel. La loi donne à la CNIL un pouvoir de certification plus étendu que celui prévu par le RGPD en ce qui concerne la certification de personnes (par exemple : le référentiel de certification des compétences du DPO). La CNIL peut directement certifier des organismes et agréer des organismes certificateurs ou, selon les cas, choisir de collaborer avec le Comité Français d'Accréditation (COFRAC). La certification est contraignante, elle donne lieu à un contrôle régulier, par le tiers certificateur, du respect du référentiel via des audits et des examens et doit être renouvelée.
CNIL *Commission Nationale de l'Informatique et des Libertés*	Autorité administrative indépendante créée en 1978, composée d'un collège pluraliste de 17 commissaires, provenant d'horizons divers (4 parlementaires, 2 membres du Conseil économique et social, 6 représentants des hautes juridictions, 5 personnalités qualifiées désignées par le Président de l'Assemblée nationale (1), par le Président du Sénat (1), par le Conseil des ministres (3). Le mandat de ses membres est de 5 ans.
Contrat de dépôt	Convention conclue entre un propriétaire d'archives privées et un service d'archives publiques auquel le premier confie pour une durée déterminée la conservation de ses archives. Cette convention énumère le cas échéant les clauses relatives à leur communication et leur reproduction.

Contrôle d'accès	Le contrôle d'accès désigne les différentes solutions techniques qui permettent de sécuriser et gérer les accès physiques à un bâtiment ou un site, ou les accès logiques à un système d'information.
Date d'élimination	Date (année) à laquelle il peut être procédé à l'élimination d'un document ou un ensemble de documents, car il est parvenu au terme de sa durée d'utilité administrative et est dénué d'intérêt historique.
Date de destruction	Date (année) à laquelle un document ou un ensemble de documents a été effectivement éliminé.
Délai de versement	Espace de temps précisé dans un tableau de gestion pendant lequel les documents doivent être conservés par le service qui les a produits avant d'être versés dans un service d'archives. En règle générale ce délai coïncide avec la durée d'utilité administrative.
Destruction	Opération matérielle d'élimination des documents dont la conservation ne se justifie plus.
Document administratif	Document défini par la législation - à l'exclusion des documents judiciaires - comme produit ou reçu par une administration ou un organisme public ou chargé d'une mission de service public. (terme générique pour désigner tout document produit par une administration.)
Donnée	Terme utilisé, en particulier en informatique, pour désigner une information.
Donnée biométrique	Caractéristique physique ou biologique permettant d'identifier une personne (ADN, contour de la main, empreintes digitales...).
Donnée personnelle	Une donnée personnelle est toute information se rapportant à une personne physique identifiée ou identifiable. Mais, parce qu'elles concernent des personnes, celles-ci doivent en conserver la maîtrise. Une personne physique peut être identifiée : • directement (exemple : nom et prénom) ; • indirectement (exemple : par un numéro de téléphone ou de plaque d'immatriculation, un identifiant tel que le numéro de sécurité sociale, une adresse postale ou courriel, mais aussi la voix ou l'image). L'identification d'une personne physique peut être réalisée : • à partir d'une seule donnée (exemple : nom) ; • à partir du croisement d'un ensemble de données (exemple : une femme vivant à telle adresse, née tel jour et membre de telle association).
Donnée sensible	Les données sensibles forment une catégorie particulière des données personnelles. Ce sont des informations qui révèlent la prétendue origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.

Le règlement européen interdit de recueillir ou d'utiliser ces données, sauf, notamment, dans les cas suivants :

- si la personne concernée a donné son consentement exprès (démarche active, explicite et de préférence écrite, qui doit être libre, spécifique, et informée) ;
- si les informations sont manifestement rendues publiques par la personne concernée ;
- si elles sont nécessaires à la sauvegarde de la vie humaine ;
- si leur utilisation est justifiée par l'intérêt public et autorisé par la CNIL ;
- si elles concernent les membres ou adhérents d'une association ou d'une organisation politique, religieuse, philosophique ou syndicale.

DPO
Délégué à la protection des données

Le délégué à la protection des données est chargé de mettre en œuvre la conformité au règlement européen sur la protection des données au sein de l'organisme qui l'a désigné s'agissant de l'ensemble des traitements mis en œuvre par cet organisme.
Sa désignation est obligatoire dans certains cas. Un délégué, interne ou externe, peut être désigné pour plusieurs organismes sous conditions. Pour garantir l'effectivité de ses missions, le délégué doit disposer de qualités professionnelles et de connaissances spécifiques et doit bénéficier de moyens matériels et organisationnels, des ressources et du positionnement adéquats.

Droit à l'information

Toute personne a un droit de regard sur ses propres données ; par conséquent, quiconque met en œuvre un fichier ou un traitement de données personnelles est obligé d'informer les personnes fichées de son identité, de l'objectif de la collecte d'informations et de son caractère obligatoire ou facultatif, des destinataires des informations, des droits reconnus à la personne, des éventuels transferts de données vers un pays hors de l'Union européenne.

Droit d'accès

Toute personne peut prendre connaissance de l'intégralité des données la concernant dans un fichier en s'adressant directement à ceux qui les détiennent, et en obtenir une copie dont le coût ne peut dépasser celui de la reproduction.

Droit d'accès indirect

Toute personne peut demander que la CNIL vérifie les renseignements qui peuvent la concerner dans les fichiers intéressant la sûreté de l'État, la Défense et la Sécurité publique.

Droit de rectification

Toute personne peut faire rectifier, compléter, actualiser, verrouiller ou effacer des informations la concernant lorsqu'ont été décelées des erreurs, des inexactitudes ou la présence de données dont la collecte, l'utilisation, la communication ou la conservation est interdite.

Droit d'opposition

Toute personne a la possibilité de s'opposer, pour des motifs légitimes, à figurer dans un fichier, et peut refuser sans avoir à se justifier, que les données qui la concernent soient utilisées à des fins de prospection commerciale.

DUA
Durée d'utilité administrative

Durée légale ou pratique pendant laquelle un document est susceptible d'être utilisé par le service producteur ou son successeur, au terme de laquelle est appliquée la décision concernant son traitement final. Le document ne peut être détruit pendant cette période qui constitue sa durée minimale de conservation.

Elimination	Procédure réglementée qui consiste à soustraire un dossier ou un ensemble de dossiers du versement auquel il appartient, ou bien encore à soustraire des documents du dossier auquel ils appartiennent, car ils sont dépourvus d'utilité administrative et d'intérêt historique. C'est l'une des trois possibilités du traitement final des documents proposée dans un tableau d'archivage.
Finalité d'un traitement	La finalité du traitement est l'objectif principal de l'utilisation de données personnelles. Les données sont collectées pour un but bien déterminé et légitime et ne sont pas traitées ultérieurement de façon incompatible avec cet objectif initial. Ce principe de finalité limite la manière dont le responsable de traitement peut utiliser ou réutiliser ces données dans le futur. Exemples de finalité : gestion des recrutements, gestion des paies, gestion des clients, enquête de satisfaction, surveillance des locaux, etc.
Fonds (d'archives)	Ensemble de documents, de toute nature, constitué de façon organique par un producteur dans l'exercice de ses activités et en fonction de ses attributions.
Gestion des archives courantes et intermédiaires	Gestion visant l'ensemble des mesures destinées à rationaliser la production, le tri, la conservation et l'utilisation des archives courantes et intermédiaires.
GED *Gestion électronique des documents*	Ensemble des systèmes d'information permettant la numérisation de documents, leur stockage, leur consultation à l'écran, leur identification, leur impression.
Numérisation	Procédé électronique de reproduction d'un document d'archives.
Protection des données personnelles	Ensemble des mesures législatives et réglementaires visant à garantir l'anonymat des informations nominatives contenues dans certaines catégories de documents, en particulier les fichiers et les enquêtes statistiques.
Registre des activités de traitement	Le registre des activités de traitement permet de recenser vos traitements de données et de disposer d'une vue d'ensemble de ce que le responsable de traitement fait avec les données personnelles. Il permet notamment d'identifier : • les parties prenantes ; • les catégories de données traitées ; • à quoi servent ces données, qui y accède et à qui elles sont communiquées ; • combien de temps les données personnelles sont conservées ; • comment elles sont sécurisées.
Responsable de traitement	Le responsable de traitement est la personne morale (entreprise, commune, etc.) ou physique qui détermine les finalités et les moyens d'un traitement, c'est à dire l'objectif et la façon de le réaliser. En pratique et en général, il s'agit de la personne morale incarnée par son représentant légal.

RGPD
Règlement Général sur la Protection des Données

Le RGPD encadre le traitement des données personnelles sur le territoire de l'Union européenne.

Le contexte juridique s'adapte pour suivre les évolutions des technologies et de nos sociétés (usages accrus du numérique, développement du commerce en ligne…).

Ce nouveau règlement européen s'inscrit dans la continuité de la Loi française Informatique et Libertés de 1978 et renforce le contrôle par les citoyens de l'utilisation qui peut être faite des données les concernant.
Il harmonise les règles en Europe en offrant un cadre juridique unique aux professionnels. Il permet de développer leurs activités numériques au sein de l'UE en se fondant sur la confiance des utilisateurs.

Sort final (des documents)

Expression d'usage courant pour désigner le traitement final des documents. Voir TRAITEMENT FINAL (DES DOCUMENTS).

Sous-traitant

Le sous-traitant est la personne physique ou morale (entreprise ou organisme public) qui traite des données pour le compte d'un autre organisme (« le responsable de traitement »), dans le cadre d'un service ou d'une prestation.
Les sous-traitants ont des obligations concernant les données personnelles, qui doivent être présentes dans le contrat :

- une obligation de transparence et de traçabilité ;
- la prise en compte des principes de protection des données dès la conception et par défaut ;
- une obligation de garantir la sécurité des données traitées ;
- une obligation d'assistance, d'alerte et de conseil (par exemple, une procédure de notification des violations de données personnelles doit être notifiée).

Tableau de gestion

État des documents produits par un service ou un organisme, reflétant son organisation et servant à gérer ses archives courantes et intermédiaires et à procéder à l'archivage de ses archives historiques. Il fixe pour chaque type de documents les délais d'utilité administrative, délai de versement au service d'archives compétent pour les recevoir, traitement final et modalités de tri à lui appliquer. Voir aussi TABLEAU DE TRI ET DE CONSERVATION, TABLEAU D'ARCHIVAGE.

Tableau de tri et de conservation (tableau d'archivage)

Document réglementaire établi par l'administration centrale des archives décrivant les types de documents produits par une administration, un service, une institution ou dans le cadre d'une fonction administrative, et fixant pour chacun d'entre eux le délai d'utilité administrative, le traitement final ainsi que les modalités de tri à leur appliquer.

Théorie des trois âges

Notion fondamentale sur laquelle repose l'archivistique contemporaine, et qui fait passer tout document par trois périodes, courante, intermédiaire et définitive, caractérisées par la fréquence et le type d'utilisation qui en est faite. Voir aussi ARCHIVES COURANTES, ARCHIVES INTERMÉDIAIRES, ARCHIVES DÉFINITIVES.

Traitement de données personnelles

Un traitement de données personnelles est une opération, ou ensemble d'opérations, portant sur des données personnelles, quel que soit le procédé utilisé (collecte, enregistrement, organisation, conservation, adaptation, modification, extraction consultation, utilisation, communication par transmission ou diffusion ou toute autre forme de mise à disposition, rapprochement).

	Un traitement de données personnelles n'est pas nécessairement informatisé : les fichiers papiers sont également concernés et doivent être protégés dans les mêmes conditions. Un traitement de données doit avoir un objectif, une finalité déterminée préalablement au recueil des données et à leur exploitation. Exemples de traitements : tenue du registre des sous-traitants, gestion des paies, gestion des ressources humaines, etc.
Traitement (des archives)	Procédures et opérations de tri, de classement, de description, d'analyse, d'indexation et de rédaction des instruments de recherche.
Traitement final (des documents)	Destination d'un document ou d'un ensemble de documents à l'expiration de son délai d'utilité administrative proposée dans un tableau d'archivage : élimination, tri ou conservation définitive.
Transfert de données	Toute communication, copie ou déplacement de données personnelles ayant vocation à être traitées dans un pays tiers à l'Union européenne.
Tri	Opération consistant à séparer, aux termes d'une évaluation, dans un ensemble de documents, ceux qui doivent être conservés en raison de leur intérêt historique ou patrimonial de ceux qui sont voués à l'élimination. C'est l'une des trois possibilités du traitement final des documents proposés dans un tableau d'archivage.
Versement	Opération matérielle et intellectuelle par laquelle la responsabilité de la conservation d'archives passe de l'administration à un service de préarchivage ou à un service d'archives, ou bien d'un service de préarchivage à un service d'archives. Ce terme désigne aussi, par extension, les documents ainsi transférés. Le fonds d'un service administratif est constitué de plusieurs versements qui peuvent être cotés selon le principe de la série continue. Voir aussi BORDEREAU DE VERSEMENT.
Visa d'élimination	Autorisation donnée par l'administration des archives à une autre administration de procéder à l'élimination de documents. Voir aussi BORDEREAU D'ÉLIMINATION.
Violation de données	Une violation de la sécurité se caractérise par la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données, de manière accidentelle ou illicite. Il s'agit de tout incident de sécurité, d'origine malveillante ou non et se produisant de manière intentionnelle ou non, ayant comme conséquence de compromettre l'intégrité, la confidentialité ou la disponibilité de données personnelles. Exemples : • suppression accidentelle de données médicales conservées par un établissement de santé et non sauvegardées par ailleurs ; • perte d'une clef USB non sécurisée contenant une copie de la base clients d'une société ; • introduction malveillante dans une base de données scolaires et modification des résultats obtenus par les élèves. Les obligations des responsables du traitement concernant les violations de données personnelles, et notamment leur notification à la CNIL et aux personnes concernées, sont prévues dans le RGPD.

REMERCIEMENTS

L'Unaf remercie tous les membres du groupe de travail qui, par leur implication, ont permis la réalisation de ce guide.

GROUPE DE TRAVAIL :

Les membres de l'Unaf :

- BERTHELOT Sarah, Chargée de mission, pôle Convention d'Objectifs, Bientraitance et Evaluation des services
- BOUILLY Marion, Chargée de mission Protection juridique des majeurs protégés, pôle Protection et Droits des Personnes
- BROUSSE Agnès, Responsable du pôle Convention d'Objectifs, Bientraitance et Evaluation des services
- DENIS Florence, Chargée de mission Protection juridique des majeurs protégés, ex-pôle Evaluation, Développements des activités, Protection et droits des personnes (2017)
- GERARD Olivier, Responsable du pôle Numérique
- REGINAL Mégane, Chargée de mission Evaluation des services, participation des personnes, pôle Convention d'Objectifs, Bientraitance et Evaluation des services
- ROOSE Eric, Responsable de service informatique
- SOCHON Lauriane, Chargée de mission Protection juridique des majeurs protégés, pôle Protection et Droits des Personnes (2020)
- URVOY Audrey, Chargée de mission Evaluation des services, participation des personnes (2019), pôle Convention d'Objectifs, Bientraitance et Evaluation des services

Un remerciement particulier à l'Udaf 93, fortement impliquée dans l'élaboration des travaux de l'Unaf, avec ses Archives départementales :

- AMROUCHE Nacera, Directrice générale, Udaf 93
- ROGER Philippe, Directeur adjoint, Udaf 93
- DACOSTA Agnès, Cheffe de service, Archives Départementales 93

Les membres des Udaf :

- ARTIS Daniel, Directeur administratif et financier, Udaf 16
- BARBERON Armelle, Archiviste GED, Udaf 25
- BIHOREAU Nathalie, Référente qualité, Udaf 60
- BORGES Claudia, Responsable qualité, ASFA 64
- DENIS Florence, Coordinatrice Famille-Gouvernante, Udaf 59
- DEODATI Catherine, Assistante de direction, Udaf 39
- DISSOH Maxime, Responsable qualité et DPO, Udaf 12
- DURAND Alexandre, Directeur général adjoint, Udaf 76
- DUVIGNAU Pascale, Directrice adjointe des services, Udaf 31
- EGLOFF Anne-Marie, Chef Unité juridique MJPM, Udaf 57
- GONNESSAT Audrey, Cheffe de service MPJM, Udaf 92
- LAHAYE Anne, Chef de services PJM, Udaf 31
- LEDOUX Valentine, Chargée de développement associatif et DPO, Udaf 25
- MERLET Jean, Archiviste, Udaf 85
- MOUILLE Emilie, Référente juridique et procédure, Udaf 78
- MURATOTI Marco, Qualiticien, Udaf 16
- MUSART Olivier, Directeur adjoint, Udaf 60
- OBRECTCH Marie-Laure, Assistante de direction, Udaf 67
- REINERT Evelyne, Directrice adjointe du service TMP, Udaf 57
- ROBERT Philippe, Directeur, Udaf 26
- ROYER Marie-Blanche, Cadre service juridique, Udaf 67
- YZAC Patricia, Archiviste, Udaf 76

Les prestataires experts en archivage et en RGPD :

- COHEN CASSUTO Françoise, Archiviste et Cheffe de projet, Un dossier une place
- TESSONNEAU Alexandre, Avocat, Squadra Avocats

Les experts de la CNIL :

- BERTAUD DU CHAZAUD Justine, Juriste au service des questions sociales et RH, direction de la conformité
- SAULNIER Stéphanie, Juriste au service des questions sociales et RH, direction de la conformité

Union Nationale des Associations Familiales
28 Place Saint Georges – 75009 PARIS
www.unaf.fr

Contact :
cobe@unaf.fr

En collaboration avec

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

CONVENTION UNAF - UDAF ÉTAT 2016-21