PROTECTION DE VOS DONNÉES

CHARTE INFORMATIQUE

- *Selon les dispositions du règlement général sur la protection des données (RGPD) ainsi qu'à celles de la loi du 6 janvier 1978 modifiée (loi « informatique et libertés » ;*
- *aux autres règle éventuellement applicables, conformément à la réglementation en vigueur, notamment le CASF et le code de la santé publique (CSP) :*

Dom'épi met en œuvre les traitements dans le cadre la la RGPD et vous assure de leur conformité. **Dom'épi**, organisme fournissant de l'accompagnement médico/social aux personnes âgées ou en situation de handicap, est inscrit dans le registre prévu à l'article 30 du RGPD.

Objectif (s) poursuivi (s) par les traitements – Finalités -

Les traitements relatif à l'accueil et l'accompagnement des personnes sont mises en œuvre afin :

a) **de fournir les prestations** définies dans le cadre d'un contrat conclu entre la structure et la personne concernée ou son représentant légal (DIPEC prévu par l'art.L.311-4 du CASF) et **d'assurer la gestion au dossier administratif de la personne concernée** (gestion des rdv médicaux ou sociaux, gestion des visites familiales, etc...) ;

b) **d'instruire, de gérer et le cas échéant, d'ouvrir les droits et/ou verser les prestations sociales légales et facultatives** ;

c) **d'offrir un 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, **d'assurer le suivi des personnes dans l'accès aux droits** notamment l'assistance dans les relations et les démarches à effectuer et, le cas échéant, **d'orienter les personnes vers les structures compétentes susceptibles de les prendre en charge** ;

d) **d'échanger et de partager les informations strictement nécessaires**, dans le respect des dispositions de l'article L.110-4 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 para-médicaux ;

e) **d'assurer la gestion administrative, financière et comptable** de l'organisme ;

f) **d'assurer la remontée des informations préalablement anonymisées aux autorités compétentes** concernant les dysfonctionnements graves ou événements ayant pour effet de menacer ou compromettre la santé, la sécurité ou le bien-être des personnes prises en charge conformément aux dispositions des art. R.331-8 et suivants du CASF, **établir 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.

Les informations recueillies pour l'une de ces finalités ne peuvent en principe être réutilisées pour poursuivre un objectif qui serait incompatible avec la finalité initiale. Tout nouvel usage des données doit en effet respecter les principes de protection des données à caractère personnel, en particulier le principe de finalité des traitements (par exemple, les traitements mis en œuvre pour les finalités énoncées ci-dessus ne doivent pas donner lieu à des interconnexions ou échanges autres que ceux nécessaires à l'accomplissement de celles-ci).

Base (s) légale (s) du traitement

Il est permis de traiter des données personnelles lorsque le traitement repose sur une des 6 bases légales mentionnées à l'article 6 du RGPD **:**

- le consentement : la personne a consenti au traitement de ses données ;
- le contrat : le traitement est nécessaire à l'exécution ou à la préparation d'un contrat avec la personne concernée ;
- l'obligation légale : le traitement est imposé par des textes légaux ;
- la mission d'intérêt public : le traitement est nécessaire à l'exécution d'une mission d'intérêt public ;
- l'intérêt légitime : le traitement est nécessaire à la poursuite d'intérêts légitimes de l'organisme qui traite les données ou d'un tiers, dans le strict respect des droits et intérêts des personnes dont les données sont traitées ;
- **la sauvegarde des intérêts vitaux** : le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée, ou d'un tiers.

Le responsable de traitement doit veiller au respect des conditions de recueil du consentement et plus particulièrement au caractère libre, spécifique, éclairé et univoque du consentement.

Selon les fonctions et finalités de **Dom'épi**, les bases légales envisagées sont :

- L'exécution du contrat ou intérêts légitimes dès lors que le traitement mis en œuvre excède ce qui est nécessaire au contrat
- Le consentement dans le cas particulier concernant les droits relatifs à la fin de vie
- La remontée des informations préalablement anonymisées aux autorités compétentes.

Données à caractère personnel

Le responsable de traitement veille à ce que seules les données nécessaires à la poursuite des finalités de traitement soient effectivement collectées et traitées à partir du moment où ce besoin se concrétise. Les données pertinentes sont relatives :

(a) à l'identification des bénéficiaires de l'accompagnement et le cas échéants de leurs représentants légaux ;
(b) à la vie personnelle ;
(c) au parcours professionnel et de formation dans le cadre de l'aide à l'insertion professionnelle des personnes ;
(d) aux conditions de vie matérielles ;
(e) à la couverture sociale ;
(f) aux coordonnées bancaires dans la mesure où cette information est nécessaire au versement d'une prestation ;
(g) à l'évaluation sociale et médico-sociale de la personne concernée ;

(h) au type d'accompagnement et aux actions mis en œuvre ;
(i) à l'identification des personnes concourant à la prise en charge sociale et médico-sociale et à l'entourage susceptible d'être contacté ;
(j) à l'identification des personnes dans le cadre de l'accompagnement numérique.

Le traitement des données sensibles

Dom'épi accorde une vigilance renforcée pour les données bénéficiant d'une protection spécifique. Elles ne peuvent être collectées et traitées que dans des conditions strictement définies par les textes. Il s'agit :

➔ **du NIR** (numéro de sécurité sociale) qui ne peut être enregistré dans le cadre des échanges avec les professionnels de santé ou les organismes de sécurité sociale, de prévoyance et les MDPH. Le décret en Conseil d'Etat n°2019-341 du 19 avril 2019 régit ce traitement.

➔ **de l'INS** (identifiant national de santé) qui ne peut être utilisé que pour répertorier et retrouver les données de santé et les données administratives rattachées à une personne bénéficiaire d'une prise en charge sanitaire ou médico-sociale. (art L.111-8-1 et R.1111-8-1 et suivants du code de la santé publique. L'INS ne peut être utilisé que par les professionnels, les établissements, services ou organismes participant à la prévention ou aux soins, par les professionne s du secteur social et médico-social, ou par les professionnels constituant une équipe de soins au sens de l'art. L.1110-12 du CSP et intervenant dans la prise en charge sanitaire ou médico-sociale de l'usager.

➔ **des données relatives aux infractions, condamnations pénales et mesures de sûreté connexes qui ne peuvent être traitées que dans certains cas, dans le respect des dispositions légales relatives aux données d'infractions (art. 46 de la LIL)** ;

Par exemple si *:*
- elles sont strictement nécessaires dans le cadre des actions mises en œuvre en faveur des personnes détenues ou placées sous main de justice, d'une part, et dans le cadre de l'aide et du soutien des victimes d'infractions ou des familles de personnes détenues ;
- elles permettent d'établir l'existence d'une situation de maltraitance passée ou en cours afin d'adapter l'accompagnement de la personne concernée (p. ex. : l'accompagnement des femmes victimes de violences conjugales par une association d'aide aux victimes agréée par le ministère de la justice conformément aux dispositions de l'article 46 al. 1 de la loi Informatique et Libertés et de l'article 76 du décret n° 2019-536 du 29 mai 2019).

➔ des données dites « données sensibles », c'est-à-dire celles qui révèlent l'origine ethnique ou prétendument raciale, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale d'une personne, les

données génétiques, les données biométriques, les données concernant la santé ou celles concernant la vie sexuelle ou l'orientation sexuelle d'une personne. Ces données ne peuvent être collectées sauf exception prévue par les textes.

A titre d'exemple, **Dom'épi** peut collecter des données relatives à la santé, sous réserve que ces données le soient à des fins :

- d'administration de soins, de traitements, de diagnostics médicaux, de médecine préventive ou de gestion des services de santé. Les traitements au sein desquels ces données sont intégrées doivent être mis en œuvre par un membre d'une profession de santé ou par une autre personne à laquelle s'impose en raison de ses fonctions, l'obligation de secret professionnel dans l'atteinte est réprimée par l'art. 226-13 du code pénal ;
- ou de délivrance d'une prestation sociale destinée aux personnes en situation de perte d'autonomie ou de handicap prévue par un texte législatif ou réglementaire, sous réserve que ces informations soient strictement nécessaires à la délivrance de ladite prestation.

Lorsque la collecte de données de santé est nécessaire à l'accompagnement social réalisé mais ne s'inscrit pas au sein de l'une ou des deux situations susvisées, celle-ci peut être réalisée après recueillement du consentement de la personne concernée ou de son représentant légal. EX : une aide à domicile peut recevoir communication de l'état de santé d'une personne dès lors que ces informations sont nécessaires à l'accompagnement social et médico-social réalisé à domicile. Le responsable de traitement veillera au respect des conditions de recueil de consentement et plus particulièrement au caractère livre, spécifique, éclairé et univoque du consentement.

Les données relatives aux convictions religieuses et/ou philosophiques peuvent être collectées sous réserve (conditions cumulatives) :

- d'être collectées auprès de la personne concernée ou de son représentant légal, après recueil du consentement exprès. De la même manière, le responsable de traitement doit veiller au respect des conditions de recueil de consentement et plus particulièrement au caractère libre, spécifique, éclairé et univoque du consentement ;
- d'être strictement nécessaires à l'accompagnement social et/ou médico-social (ex : organisation des repas, des funérailles, accompagnement des personnes victimes ou susceptibles d'être victimes de mouvements extrémistes, etc...).

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

Dans le cadre de la fonction de Dom'épi, un consentement spécifique devra être recueilli pour pouvoir traiter les informations relatives aux convictions religieuses.

Catégories de données adaptées selon les finalités du traitement

À l'identification des bénéficiaires de l'accompagnement social et médico-social, et le cas échéant de leurs représentants légaux	**Nom, prénom, genre, adresse**, courriel, n° de téléphone, date et lieu de naissance, photographie (si strictement nécessaire pour l'objectif poursuivi)
	N° d'identification de rattachement à un organisme : n° d'adhérent ou d'allocataire
	N° de sécurité sociale dans les conditions fixées par le décret n° 2019-341 du 19 avril 2019
	Nationalité du bénéficiaire sous la forme « Français/UE/Hors UE », les documents prouvant la régularité du séjour en France de la personne concernée dès lors que le bénéfice de l'aide ou de la prestation sociale est soumis à une condition de régularité du séjour **Informations relatives de la procédure de demande d'asile** sous la forme « dépôt d'une demande d'asile : oui / non et/ou la procédure de demande de titre de séjour sous la forme « dépôt d'une demande de titre de séjour oui/non », la nationalité de la personne concernée ainsi que les informations nécessaires à l'élaboration du récit de vie de la personne concernée.
	Dans des cas exceptionnels, la photocopie de la pièce d'identité de la personne concernée notamment dans le cadre de l'accompagnement relatif à la gestion budgétaire auprès des organismes publics ou privés (ex : dépôt dun dossier de surendettement auprès de la BDF, etc...)
À la vie personnelle	Situation et composition familiale du foyer, le cas échéant, l'identification d'enfants pris en charge dans le cadre de la protection de l'enfance, habitudes de vie nécessaires à l'organisation de la vie quotidienne (par ex : habitudes alimentaires, activité physique, toilette quotidienne, nbre d'heures de sommeil, etc...), centres d'intérêt, langue parlée dans la mesure où cette information est indispensable pour mentionner le besoin d'interprètes.
Au parcours professionnel et de formation dans le cadre de l'aide à l'insertion professionnelle des personnes	Scolarité, situation au regard de l'emploi, de la formation et de la qualification.
Aux conditions de vie matérielles	**Situation financière** : ressources, charges, crédits, dettes Peuvent également être collectées les informations relatives à la **liste des comptes bancaires existants, aux dates d'ouvertures desdits comptes, aux moyens de paiement, au montant du découvert autorisé ainsi qu'à l'inscription, le cas échéant, au fichier national des incidents de remboursement des crédits aux particulierts (FICP) et au fichier central des chèques (FCC)** sous réserve que ces informations soient strictement nécessaires à l'accompagnement budgétaire réalisé.
	Prestations et avantages sociaux perçus : nature, montanty, quotient familial, nb° d'allocataire
	Situation face au logement et à l'hébergement : type et caractéristiques du logement ou modalités d'hébergement (domicile personnel, familial, sans abri, hébergement de fortune, hébergement mobile, hébergement d'urgence ou d'insertion
	Moyens de mobilité

À la couverture sociale	Organismes de rattachement et régimes d'affiliation, droits ouverts
Aux coordonnées bancaires dans la mesure où cette information est nécessaire au versement d'une prestation	RIB
À l'évaluation sociale ou médico-sociale de la personne concernée	Difficultés rencontrées et appréciations sur celles-ci, évaluation de la situation de la personne afin de repérer l'aggravation de difficultés ou encore d'une perte d'autonomie
Au type d'accompagnement et aux actions mises en oeuvre	Domaine d'intervention, historique des mesures d'accompagnement, objectifs, parcours, actions d'insertion prévues, entretien et suivi
À l'identification des personnes concourant à la prise en charge sociale et médico-sociale et à l'entourage susceptible d'être contacté	Nom, prénom, qualité, organisme d'appartenance, n° de tél de l'organisme, adresse, courriel, n° de tél des aidants professionnels ou familiaux (le cas échéant, le lien familial, du médecin traitant, des médecins experts, de la personne de confiance Dans des cas exceptionnels, il est possible d'enregistrer les identifiants et mots de passe de l'espace personnel de la personne concernée lorsque celle-ci n'est pas en capacité de se connecter seule (elle ne sait pas se déplacer ou n'a pas accès à l'internet)
À l'identification des personnes dans le cadre de l'accompagnement au numérique	L'enregistrement des mots de passe de l'usager ne doit réalisé que dans le cadre d'un mandat signé entre l'usager et le professionnel (voir mandat en annexe). S'agissant du choix du mot de passe, la CNIL conseille vivement de se conformer à la *délibération n° 2017-012 du 19 janvier 2017 portant adoption d'une recommandation relative aux mots de passe modifiée.*
Informations relatives à certaines aides sociales légales (liste non exhaustive)	Aide sociale pour l'hébergement (ASH) et APA : les donnes susceptibles d'être collectées par les conseils départementaux dans le cadre de l'instruction, la gestion et le versement de l'APA et l'ASH sont listées par l'*art. R. 232-41 du CASF.* Carte mobilité inclusion : les données susceptibles d'être collectées par les MDPH et les conseils départementaux dans le cadre de l'instruction, la gestion et la délivrance des cartes sont listées par l'*art. D. 241-18-1 du CASF.* RSA : les données susceptibles d'être collectées par les CAF et les caisses de mutualité sociale agricole (MSA) dans le cadre de l'instruction, la liquidation et le versement du RSA sont listées à l'art. R.262-103 du CASF. Les informations relatives aux bénéficiaires du RSA font l'objet d'échanges entre les conseils départementaux et France Travail afin de coordonner leurs actions d'insertion professionnelles conformément à l'*art. R.262-116-2 du CASF.*

Destinataires des données et accès aux informations

Les données personnelles ne peuvent être accessibles qu'aux seules personnes habilitées à en connaître au regard de leurs attributions. D'une manière générale, les habilitations d'accès doivent être documentées par les organismes, et les accès aux différents traitements doivent faire l'objet de mesures de traçabilité. (voir le paragraphe relatif à la sécurité).

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 et au suivi des personnes dans le respect de leur vie privée ;
- les échanges doivent être réalisés dans les conditions fixés par les textes législatifs et réglementaires.

Les personnes accédant aux données pour le compte du responsable de traitement

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 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.

Les destinataires des données

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

Avant toute communication des informations, le responsable de traitement doit d'une part, s'interroger sur la finalité de la transmission pour s'assurer de la pertinence et de sa légitimité et, d'autre part, vérifier que les données communiquées sont adéquates, pertinentes et non excessives au regard de la finalité poursuivie.

Les sous-traitants

Le RGPD définit les sous-traitants comme « *la personne physique ou morale, l'autorité publique, le service ou l'organisme qui traite les données à caractère personnel pour le compte du responsable du traitement ».*

Il peut s'agir des prestataires de services informatiques (hébergement, maintenance, etc...) ou encore de tout organisme offrant un service ou une prestation impliquant un traitement de données à caractère personnel pour le compte d'un autre organisme (gestion de paie des salariés, etc...).

Le responsable de traitement qui a recours à un sous-traitant veille à ne faire appel qu'à des organismes présentant des garanties suffisantes. Un contrat définissant les caractéristique du traitement ainsi que les différentes obligations des parties en matière de protection des données est établi entre elles (art 28 du RGPD).

Les tiers autorisés

Les autorités légalement habilitées sont susceptibles, dans le cadre d'une mission particulières ou de l'exercice du droit de communication, de demander au responsable de traitement la communication de données à caractère personnel (par ex : France Travail, organismes de sécurité sociale dans le cadre de la lutte de la fraude, les administrations de la justice, de la police, de la gendarmerie, etc...).

Dans ce cas, le responsable de traitement s'assure du caractère contraignant de la disposition avancée et ne transmet que les données prévues par le texte ou les données seules indispensables au regard de la finalité du droit de communication en question.

Durée de conservation

Une durée de conservation précise des données est fixée en fonction de la finalité. Lorsqu'il est impossible de les fixer, les critères utilisés font partie des informations qui doivent être communiquées aux personnes concernées.

Les données collectées et traitées pour les besoins de l'accueil et l'accompagnement des personnes ne sont pas conservées au-delà de 2 ans à compter du dernier contact émanant de la personne ayant fait l'objet de cet accompagnement (ex : dernier courrier ou courrier envoyé par la personne concernée, etc...), sauf cas particulier. Cette durée de conservation est préconisée par la Commission s'agissant de l'ensemble des finalités.

Les données seront conservées en **archivage intermédiaire** lorsque Dom'épi en a l'**obligation légale** (ex : obligations comptables, sociales ou fiscales) ou en cas de besoin de constituer une **preuve en cas de contentieux**. **La durée de l'archivage répond à une réelle nécessité justifiée par le responsable de traitement.**

Dom'épi conserve **le dossier de données médicales du bénéficiaire** de nos services d'accompagnement médico-social **20 ans à compter de sa dernière prise en charge**. Si décès, dans les 10 ans, le dossier est conservé pendant une période de 10 ans à compter de la date du décès (art. R.1112-7 du CSP).

Si certaines données sont anonymisées, le responsable de traitement peut les conserver sans limitation de durée.

Information des bénéficiaires

L'information communiquée aux personnes doit se faire dans les conditions prévues par les articles 12, 13 et 14 du RGPD.

Dom'épi les informe de l'existence du traitement, de ses caractéristiques essentielles (dispositions de l'art. 21 du RGPD). Le bénéficiaire peut s'opposer au traitement de ses données, à condition d'invoquer des raisons tenant à sa situation particulière, et uniquement lorsque le traitement est mis en œuvre sur la base légale de l'intérêt légitime du responsable de traitement, ou pour l'exécution d'une mission d'intérêt public ou d'une mission relevant de l'autorité publique. Le responsable du traitement pourra refuser de donner suite à cette demande d'opposition s'il démontre qu'il dispose d'intérêts légitimes et impérieux qui prévalent sur les droits et libertés du demandeur.

Dom'épi doit répondre aux demandes dans un délai d'un mois maximum. Si le dossier est complexe, la personne doit être informée dans un délai d'un mois supplémentaire. Dans tous les cas, le délai ne doit excéder 3 mois.

L'exercice des droits par les personnes est gratuit. Si elles ne sont pas satisfaites du traitement de leurs données à caractère personnel, une réclamation est possible auprès de la Commission nationale de l'Informatique et des Libertés.

- **Les modalités de l'information**
  Dom'épi procède à une information écrite de manière à justifier de son contenu ainsi que du moment où elle a été délivrée (en principe au moment de la collecte des données afin de respecter les principes de loyauté et de transparence et conformément aux art. 13 et 14 du RGPD.
  Le responsable de traitement informe les personnes concernées et le cas échéant, les représentants légaux par le livret d'accueil ou le DIPEC. Pour s'assurer de la bonne compréhension par la personne concernée, l'information sera également faite par oral.

Sécurité

Dom'épi prend toutes les précautions utiles au regard des risques présentés par son traitement pour préserver la sécurité des données à caractère personnel, et notamment au moment de leur collecte, durant leur transmission et leur conservation et empêcher qu'elles soient déformées, endommagées ou que des tiers non autorisés y aient accès.

Mesures mises en place par Dom'épi

Catégories	Mesures
Sensibiliser les utilisateurs	Informer et sensibiliser les personnes manipulant les données Cette charte informatique
Authentifier les utilisateurs	Adopter une politique de mots de passe utilisateur
	Obliger l'utilisateur à changer son mot de passe après réinitialisation
	Limiter le nombre de tentatives d'accès à un compte
Gérer les habilitations	Définir les profils d'habilitation
Gérer les incidents	Prévoir les procédures pour les notifications de violation des données à caractère personnel
Sécuriser les postes de travail	Procédure de verrouillage automatique de session
	Utiliser des antivirus régulièrement mis à jour
	Installer un pare-feu logiciel
	Recueillir l'accord de l'utilisateur avant toute intervention sur son poste
Sécuriser l'informatique mobile	Prévoir des moyens de chiffrement des équipements mobiles
	Faire des sauvegardes ou des synchronisations régulières des données
	Exiger un secret pour le déverrouillage des ordinateurs ou téléphones
Protéger le réseau informatique interne	Limiter les flux réseau au strict nécessaire
	Sécuriser les accès distants des appareils informatiques nomades par VPN
	Mettre en œuvre le protocole WPA2 ou WPA2-PSK ou supérieur pour les réseaux WIFI
Sécuriser les serveurs	Limiter l'accès aux outils et interfaces d'administration aux seules personnes habilitées
	Installer sans délai les mises à jour critiques
	Assurer une disponibilité des données
Sécuriser les sites WEB	Utiliser le protocole TLS et vérifier sa mise en œuvre
	Vérifier qu'aucun mot de passe ou identifiant n'est encapsulé dans les URL

	Contrôler que les entrées des utilisateurs correspondent à ce qui est attendu
	Mettre un bandeau de consentement pour les cookies et autres traceurs non nécessaires au service
Sauvegarder et prévoir la continuité d'activité	Effectuer des sauvegardes régulières
	Stocker les supports de sauvegarde dans un endroit sûr
	Prévoir des moyens der sécurité pour le convoyage des sauvegardes
	Prévoir et tester régullèrement la continuité d'activité
Archiver de manière sécurisée	Mettre en œuvre des modalités d'accès spécifiques aux données archivées et détruire les archives obsolères de manière sécurisée
Encadrer la maintenance et la destruction des données	Encadrer par un responsable de l'organisme les interventions par des tiers
Gérer la sous-traitance	Les relations avec les prestataires qui traitent des données au nom et pour le compte du responsable de traitement (l'organisme employeur) doivent faire l'objet d'un accord écrit. L'accord doit notamment prévoir les conditions de restitution et de destruction des données. Il incombe au responsable de traitement de s'assurer de l'effectivité des garanties prévus (audits de sécurité, visites, etc..)
Sécuriser les échanges avec d'autres organismes	Ne pas transmettre des fichiers contenant les données à caractère personnel des usagers en clair via des messageries grand public
	Privilégier des moyens de communication autres que les messageries grand public pour communiquer des informations relatives aux personnes accompagnées à d'autres travailleurs sociaux ou organismes (par ex : plate-formes d'échanges sécurisées, message interne, etc..)
	Chiffrer les pièces sensibles à transmettre, si cette transmission utiliser la messagerie électronique
	S'assurer qu'il s'agit du bon destinataire
	Assurer la confidentialité des secrets (clé de chiffrement, mot de passe, etc...) en les transmettant via un canal distinct (par exemple, envoi du fichier chiffré par courriel et transmission du secret par téléphone ou par SMS
Protéger les locaux et les bureaux physiques	Restreindre les accès aux bureaux de au moyen de portes verrouillées
	Ranger tous les documents papiers relatifs aux usagers dans les armoires fermées à clé
	Verrouiller la porte d'accès au bureau en cas d'absence prolongéeUtili
Utiliser des fonctions cryptographiques	Utiliser des algorithmes, des logiciels et des bibliothèques reconnus
	Conserver les secrets et les clés cryptographiques de manière sécurisée
Sécuriser les mots de passe des usagers	Utiliser un gestionnaire de mots de passe ou un carnet stocké dans un coffre-fort pour enregistrer les mots de passe

Dom'épi s'engage dans un logiciel « DUI » pour héberger les données de santé à caractère personnel réalisé pour le compte des organismes assurant le suivi social ou médico-social par un prestataire informatique. Ce dernier est agréé et certifié pour l'hébergement le stockage, la conservation des données de santé, conformément aux dispositions de l'article de l'art. L. 1111-8 du code de la santé publique.
Ce dossier usagé informatisé « DUI » est inscrit dans un logiciel référencé SEGUR.

Droits des personnes

- **Droit d'accès** : permet à la personne concernée de savoir si des données la concernant sont traitées par le responsable de traitement et d'obtenir des précisions sur les conditions de ce traitement et, à sa demande, d'obtenir une copie de données ;

- **Droit de rectification** : si informations inexactes ou incomplètes la concernant ;

- **Droit à l'effacement** : les données sont effacées par le responsable de traitement pour respecter les délais de conservation fixés par les textes législatifs ou réglementaires ou si la personne a retiré son consentement ;

- **Droit à la limitation du traitement** : par exemple lorsque la personne concernée conteste l'exactitude de ses données. Dans ce cas, l'organisme procède au gel temportaire du traitement de ses données, le temps de faire les vérifications nécessaires ;

- **Droit à la portabilité** dans les conditions prévues au RGPD : la personne a la possibilité de récupérer une partie des données la concernant dans un format ouvert et lisible par machine afin de les réutiliser à des fins personnelles.
  3 conditions doivent être réunies :
  - limitation aux seules données à caractère personnel fournies par la personne
  - application uniquement si les données sont traitées de manière automatisée (exclusion des fichiers par voie papier)
  - consentement préalable de la personne concernée ou exécution d'un contrat conclu avec la personne (respect des droits et libertés de tiers) ;

- **Droit d'opposition**

Analyse d'impact relative à la protection des données

Les traitements ayant pour finalité l'accompagnement social et médico-social des personnes donnent lieu à la réalisation préalable d'une AIPD.

Dom 'épi garantit :

- les principes et droits fondamentaux fixés par le RGPD et la loi « Informatique et Libertés
- La gestion des risques sur la vie privée qui permet de déterminer les mesures techniques et d'organisation appropriées pour protéger les données.