PROTOCOLE DE PROTECTION DES DONNEES ET PARTAGE DES INFORMATIONS

Système national de gestion de cas de protection de l'enfant

Pour la prise en charge des enfants en situation difficile au Mali

Août 2020

Table des matières

1. INTRODUCTION ET OBJECTIVES

1.1 **L'objectif de ce protocole** de protection et partage d'information (PPPI) est de fournir des conseils pour le stockage, le partage, l'archivage et la destruction des informations relatives aux enfants et aux familles liées aux services de gestion des dossiers de protection de l'enfance (un dossier pour chaque cas).

1.2 **La protection des données** est directement liée à la sécurité et à la sauvegarde en protégeant les informations importantes des enfants et leurs familles contre la corruption, la perte. La protection des données contribue à leur intérêt supérieur en empêchant l'utilisation abusive de leurs informations personnelles à des fins qui échappent le contrôle, y compris à des fins qui pourraient conduire à l'exploitation, stigmatisation et à des abus - intentionnels ou non.

1.3 **Les interventions en gestion de cas de protection, représentent les activités de traitement de données et sensibles** car elles nécessitent le traitement de données à caractère personnelle identifiables ainsi que d'informations sensibles concernant la protection. **Le traitement de données à caractère personnelle** s'entend par : toute opération ou ensemble d'opérations effectuées à l'aide de procédés automatisés ou non et appliquées à des données, telles que la collecte, l'exploitation, l'enregistrement, l'organisation, la conservation, l'adaptation, la modification, l'extraction, la sauvegarde, la copie, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, le cryptage, l'effacement ou la destruction des données à caractère personnel[1].

1.4 Les gestionnaires de cas[2] représente le personnel spécialisé qui identifie, évalue, développe, met en œuvre, suit et clôt les dossiers individuels des enfants en situation difficile et leurs familles. Le gestionnaire de cas est le seul à connaître les détails les plus confidentiels du dossier contenant les données à caractère personnelle et à avoir une connaissance plus approfondie de l'enfant, sa famille/communauté, avec laquelle il a une relation de confiance.

1.5 Le **responsable du traitement des données** défini par la Loi[3] comme : toute personne qui, seule ou conjointement avec d'autres, prend la décision de collecter et de traiter des données à caractère personnel et en détermine les finalités. Sous la supervision du superviseur, le gestionnaire de cas doit assurer une gestion confidentielle de l'information de chaque enfant, en fonction des besoins spécifiques de chaque cas.

1.6 L'approche contenue dans le PPPI est guidée la législation nationale au Mali concernant la protection des données à caractère personnelle, par les droits internationaux de l'enfant et suit le principe de l'intérêt supérieur de l'enfant, les principes de "ne pas nuire" et les meilleures pratiques en matière de confidentialité, qui exigent tous que les informations ne soient partagées que sur la base du "besoin de savoir".

1.7 Ce protocole fait partie intégrante des procédures opérationnelles standard (POS) pour la gestion des cas au Mali. Il ne remplace pas ces procédures, mais fournit plutôt des conseils complémentaires spécifiques sur la protection des données et le partage des informations en toute sécurité et dans le respect de l'éthique.

---

[1] *Article 3 paragraphe 22 Loi n° 2013-015 du 21 mai 2013 Portant protection des données à caractère personnel en république du Mali*

2 Comme défini dans les lignes directrices et Procédures Opérationnelles standards, les gestionnaires de cas incluent différents profils (travailleur sociaux, intervenants sociaux, acteurs communautaires) avec le mandat et responsabilité d'accompagnement social individualisée des enfants (et familles) en situation difficile.

3 Article3 paragraphe 18 Loi n° 2013-015 du 21 mai 2013 Portant protection des données à caractère personnel en république du Mali

2. PRINCIPES GENERAUX

LEGISLATION NATIONALE :

Au Mali, Il est institué une autorité administrative indépendante dénommée Autorité de protection des données à caractère personnel, en abrégé (Apdp)[4]. La législation malienne relative à la protection des données à caractère personnelle se réfère essentiellement à la loi n° 2013-015 du 21 mai 2013 Portant protection des données à caractère personnel en république du Mali. La législation assure à toute personne, physique ou morale, publique ou privée, la protection de ses données à caractère personnel, sans distinction de race, d'origine, de couleur, de sexe, d'âge de langue, de religion, de fortune, de naissance d'opinion, de nationalité ou autre. La loi garantit que tout traitement, sous quelle que forme que ce soit, respecte les libertés et droits fondamentaux des personnes physiques. Elle prend également en compte les prérogatives de l'Etat, les droits des collectivités territoriales, les intérêts des entreprises et de la société civile. Les données à caractère personnel doivent :

- Être collectées et traitées, de manière loyale, licite et non frauduleuse pour des finalités déterminées, explicites et légitimes ;
- Ne pas être utilisées pour d'autres finalités ;
- Être adéquates, proportionnées et pertinentes au regard des finalités pour lesquelles elles sont collectées ou utilisées ;
- Être exactes, complètes et si nécessaire mises à jour ;
- Être conservées sous une forme permettant l'identification des personnes concernées pendant une durée qui n'excède pas celle nécessaire aux finalités pour lesquelles elles sont collectées ou utilisées.

Ces dispositions ne s'opposent pas à la conservation et à l'utilisation des données traitées à des fins de gestion des archives ou à des fins historiques, statistiques ou scientifiques selon les modalités définies par la loi[5]. Cependant la même législation prévoit des sanctions en cas de non-respect des mesures édictées[6].

PRINCIPES INTERNATIONAUX STANDARDS DE PROTECTION DE L'ENFANCE ET CONFIDENTIALITE :

- **L'intérêt supérieur de l'enfant** y compris les considérations de sécurité physique, de bien-être social et émotionnel, est la considération première dans la prise de décision sur la protection des données et le partage des informations.
- **Besoin de savoir :** L'accès aux données à caractère personnel doit être limité aux seules personnes qui ont besoin de les connaître pour fournir des services de gestion des dossiers de protection de l'enfance. Les données à caractère personnel ne doivent être connues que du travailleur social concerné, du superviseur et des autres prestataires de services dans le but de fournir des services de protection de l'enfance.
- **Finalité et proportionnalité :** La manière dont les informations sont partagées dépend principalement de la finalité et de la nécessité de partager ces informations, du type d'informations partagées (proportionnel à la finalité) et du niveau de sensibilité des informations

---

[4] ***Article 20 Loi n° 2013-015 du 21 mai 2013 Portant protection des données à caractère personnel en république du Mali***

[5] ***Article 7 Loi n° 2013-015 du 21 mai 2013 Portant protection des données à caractère personnel en république du Mali***

[6] ***Article 56 Loi n° 2013-015 du 21 mai 2013 Portant protection des données à caractère personnel en république du Mali***

3. CONSENTEMENT ECLAIRE :

3.1 Lors de l'obtention du consentement éclairé, une explication doit être donnée à l'enfant et à son parent/responsable légal, sur les raisons exactes pour lesquelles des données à caractère personnel sont collectées, sur la manière dont elles seront utilisées et par qui, ainsi que sur les limites de la confidentialité (c'est-à-dire lorsque de graves problèmes de sécurité sont identifiés et/ou que des obligations de déclaration sont imposées).

3.2 Les informations doivent être partagées avec sensibilité, dans un langage et des formats adaptés à l'âge de l'enfant et à sa capacité de compréhension, et l'enfant (et le parent/la personne qui s'occupe de lui) doit avoir la possibilité de poser des questions[7].

3.3 Les enfants doivent avoir la possibilité de mettre en évidence toute information qu'ils ne souhaitent pas voir divulguée à une personne ou à un organisme particulier. Par exemple, ils peuvent ne pas vouloir que leur famille soit informée de détails personnels les concernant qu'ils préféreraient communiquer en personne.

3.4 Les enfants/responsables d'enfants ont le droit d'accéder aux informations détenues à leur sujet et de les consulter. Les services et organisations qui détiennent des informations doivent donc prendre des dispositions pour qu'ils puissent accéder à ces informations quand ils en ont besoin (y compris après la clôture de leur dossier).

3.5 Dans des circonstances exceptionnelles, les informations divulguées par les enfants peuvent être partagées contre leur gré si l'on considère - après une évaluation minutieuse - qu'il est dans leur intérêt de le faire, généralement si l'enfant ou une autre personne risque de subir un préjudice ou si le partage des données est jugé dans l'intérêt supérieur de l'enfant. Dans de telles situations, les raisons du partage des données à caractère personnel de cette manière doivent être clairement expliquées à l'enfant concerné. Il n'y a pas de règle absolue pour la divulgation des informations partagées par un enfant. Comme il s'agit d'une question subjective, chaque cas doit être examiné individuellement, et les décisions de divulguer des informations doivent être prises au plus haut niveau de l'agence ou des agences concernées.

3.6 Les lois sur le signalement obligatoire obligent les prestataires de services à signaler les cas d'abus réels ou présumés à un organisme central. L'article58[8] du code de procédure pénale malien dispose : « Toute autorité constituée, tout fonctionnaire ou officier public qui, dans l'exercice de ses fonctions, acquerra la connaissance d'un crime ou d'un délit, sera tenu d'en donner avis sur-le-champ au procureur de la République ou au juge de paix à compétence étendue près le tribunal dans le ressort duquel le prévenu pourrait être trouvé et de transmettre à ce magistrat tous les renseignements, procès-verbaux et actes qui y sont relatifs. Toute personne qui aura été témoin d'un attentat soit contre la sûreté publique, soit contre la vie ou la propriété d'un individu, sera tenue d'en donner avis au procureur de la République ou au juge de paix à compétence étendue », l'article 73[9] du code de protection de l'enfant dispose : « Toute personne, y compris celle qui est tenue au secret professionnel, est soumise au devoir de signaler au délégué à la protection de l'enfance tout ce qui est de nature à constituer une menace à la santé de l'enfant, à son développement, à son intégrité physique ou morale au sens des dispositions de l'article 51 du présent code. L'enfant lui-même peut signaler au délégué à la protection de l'enfance sa situation ou celle de tout autre enfant ».

---

[7] *Articles 12 et 13Loi n° 2013-015 du 21 mai 2013 Portant protection des données à caractère personnel en république du Mali*

8 Article 58 de la loi n°01-80 du 20 août 2001 portant Code de procédure pénale, modifiée par la loi n°2013-016/ du 21 mai 2013

9 Article 73 du code de protection de l'enfant

Les lois relatives à l'obligation de signalement doivent être expliquées à l'enfant (et/ou à la personne qui s'occupe de lui) au cours du processus de consentement éclairé.

4. PROTECTION ET ARCHIVAGE DES DONNEES

PROTECTION DE DONNEES EN FORMAT PAPIER :

4.2 Tous les enfants sur lesquels des informations sont recueillies devraient se voir attribuer un identifiant de cas unique basé sur un format de codage standard convenu (code par agence et gestionnaire de cas), développé au niveau national dans le but d'anonymiser et de suivre le cas.

4.3 Pour les organisations et les services utilisant le système CPIMS+, les codes d'identification des cas seront automatiquement générés par le système.

4.4 L'identifiant du cas doit être utilisé pour faire référence au cas de l'enfant verbalement, sur papier et électroniquement (y compris dans les documents Word, les courriels, les conversations sur Skype, etc.

4.5 Chaque cas et tous les formulaires et documents annexes doivent être conservés dans un dossier individuel, clairement identifié par l'identifiant individuel du cas à l'extérieur du dossier. Il est impératif que le nom de l'enfant n'apparaisse pas à l'extérieur du dossier. Les dossiers doivent être stockés en fonction des identifiants attribués.

4.6 Les dossiers papier doivent être conservés dans un endroit sûr, accessible uniquement aux travailleurs sociaux et aux superviseurs responsables de l'information. Cela nécessite un classeur verrouillable, dont les clés doivent être conservées par la personne responsable de la gestion des dossiers. Personne d'autre ne doit pouvoir y accéder de manière indépendante, sauf en cas de nécessité et si une autorisation est accordée.

4.7 Les dossiers papier doivent être transférés main à main entre les seules personnes censées intervenir sur le cas (par exemple, lorsqu'ils doivent être utilisés pour des conférences de cas et des réunions d'examen de cas). Pendant les déplacements des dossiers et/ou les transferts, les dossiers doivent être conservés dans une armoire ou une enveloppe scellée.

4.8 Il n'est pas permis de conserver les documents originaux tels que les cartes d'identité ou les rapports médicaux. Les documents originaux doivent être soit photographiés, soit scannés et retournés à l'enfant ou à la famille. Les documents originaux ne doivent pas être conservés dans des dossiers papier afin que la destruction des dossiers papier puisse se faire sans aucune hésitation en cas d'évacuation/réinstallation d'urgence.

4.9 L'impression, la photocopie ou le scannage des données relatives aux enfants doivent être effectués en interne. Toute copie supplémentaire des formulaires doit être entièrement détruite afin qu'elle soit illisible et éliminée de manière confidentielle.

PROTECTION DE DONNEES EN FORMAT ELECTRONIQUE :

4.10 Les smartphones, tablettes, ordinateurs portables et ordinateurs de bureau impliqué dans la gestion des cas électronique, interconnectant et traitants des données à caractère personnelles doivent suivre un protocole de configuration préalablement déterminée. Cette procédure de configuration du matériel informatique augmentera le niveau de sécurité des appareils et réduira le risque d'utilisation non professionnelle de ces terminaux. L'interconnexion des données à caractère personnelle se défini comme : Tout mécanisme de connexion consistant en la mise en relation de données traitées pour une finalité déterminée avec d'autres données traitées pour des finalités identiques ou non ou liées par un ou plusieurs responsables de traitement[10]. Les organisations et services produiront des identifiants pour leur personnel et veilleront à ce que chaque membre du personnel utilise son propre identifiant et ne partage pas ses mots

[10] *Article3 paragraphe 14 Loi n° 2013-015 du 21 mai 2013 Portant protection des données à caractère personnel en république du Mali*

de passe. Conformément aux dispositions légales en matière de protection des données : le responsable du traitement prend toutes les précautions utiles pour préserver la sécurité des données. Il doit empêcher notamment qu'elles soient déformées, endommagées ou que des tiers non autorisés y accèdent[11].

4.11 En plus de l'ordinateur lui-même, tous les fichiers électroniques (par exemple, Word, Excel) doivent être protégés par un mot de passe. Si vous envoyez par courrier électronique un document contenant des données relatives à la gestion des dossiers de protection de l'enfance, le mot de passe doit être envoyé séparément et par un canal différent de communication (SMS…). Le personnel doit s'assurer que les courriers électroniques sont envoyés uniquement au destinataire prévu, sans que personne d'autre n'en reçoive une copie.

4.12 Des mots de passe forts doivent être utilisés, c'est-à-dire contenant au moins 8 caractères, dont un chiffre, une majuscule, une lettre et un caractère spécial difficile à craquer. Pour les utilisateurs du CPIMS+, il sera indispensable d'introduire un mot de passe avec les éléments suscités pour exporter un document au format PDF.

4.13 Les mots de passe pour les documents et les ordinateurs doivent être changés régulièrement (au minimum tous les 3 mois) et à chaque fois qu'il y a mouvement de personnel.

4.14 Les gestionnaires de cas doivent verrouiller leurs ordinateurs lorsqu'il s'en éloigne. Les ordinateurs doivent également être configurés pour un verrouillage automatique après 5 minutes d'inactivité.

4.15 Les membres du personnel ne sont pas autorisés à sauvegarder des informations relatives à la gestion des dossiers sur leur ordinateur personnel. Seuls les ordinateurs affectés au travail peuvent être utilisés pour gérer les informations relatives à la gestion des dossiers de protection de l'enfance. Cependant les utilisateurs du CPIMS+ peuvent en cas de besoin se connecter à leur compte et intervenir sur un dossier sans pour autant télécharger des documents sur leur ordinateur personnel.

4.16 Les ordinateurs contenant des données sur les enfants ne doivent être accessibles qu'au personnel autorisé et doivent être utilisés exclusivement à cette fin.

4.17 Les ordinateurs fonctionnant sur Windows doivent être équipés de logiciels anti-virus à jour afin d'éviter la corruption et la perte d'informations.

4.18 Lorsqu'un membre du personnel quitte son poste ou est affecté, il doit remettre toutes les informations relatives à la gestion des dossiers de protection de l'enfance. Toute donnée personnelle enregistrée sur l'ordinateur doit être effacée avant la remise. Pour les organisations utilisant le CPIMS+, les administrateurs doivent s'assurer de désactiver les comptes y afférents.

4.19 Les clés USB doivent être évitées ou, si nécessaire, passées en main propre entre les membres du personnel devant intervenir sur le cas. Le fichier doit être protégé par un mot de passe, et effacé immédiatement de la clé après le transfert.

5. PARTAGE D'INFORMATION PERSONNELLE

PARTAGE D'INFORMATION PERSONNELLE DANS LE CADRE D'UN REFERENCEMENT :

Le référencement de cas consiste à confier la prestation d'un service pour l'enfant ou pour sa famille à une tierce personne évoluant dans une structure publique ou privée, ou en milieu communautaire. Ce service peut être ponctuel à l'image d'un soin de santé, ou plus durable à l'image d'un placement dans un centre de formation professionnelle ou de la mise ne place d'un suivi psychologique par exemple[12].

[11] *Article 8 Loi n° 2013-015 du 21 mai 2013 Portant protection des données à caractère personnel en république du Mali*

[12] Procédures Opérationnelles Standards pour la gestion de cas de protection de l'enfance au Mali, 2020.

Quand le gestionnaire de cas est-il amené à partager des informations ?

5.1 Lorsque le gestionnaire de cas responsable du dossier a besoin d'un soutien externe d'un autre organisme ou service pour fournir un service répondant aux besoins de l'enfant ou de la famille.

Pourquoi partager certaines données ?

5.2 La raison pour laquelle les données personnelles sont partagées avec une organisation ou service qui reçoit un dossier est de permettre la fourniture de services holistiques et multisectoriels selon les besoins, en fonction de l'intérêt supérieur de l'enfant ou de la famille. Cependant, les données personnelles partagées doivent se limiter aux seules informations nécessaires à l'organisation ou au service qui reçoit la référence pour fournir ce service efficacement.

Avec qui partager certaines données ?

5.3 La personne qui reçoit les informations doit être le prestataire de services direct, par exemple un autre travailleur social, un psychologue ou un médecin.

Quel type de données partager ?

5.4 Lors de l'échange de données à caractère personnel aux fins de la prestation de services de gestion de cas, les données suivantes peuvent être partagées (si nécessaire) :

- Identification du cas (s'il s'agit d'un renvoi à un autre prestataire de services de gestion de cas de protection de l'enfance) ;
- Nom de l'enfant ;
- Adresse et coordonnées de l'enfant et/ou de la personne qui s'en occupe ;
- Organisation ou service qui effectue le référencement ;
- Nom et coordonnée du représentant de l'organisation ou du service qui effectue le référencement ;
- La date du référencement
- Type de service(s) requis.
- Informations générales pertinentes

Comment effectuer ce partage de données ?

5.5 Le formulaire de référencement interagences sur papier doit être rempli dès que possible et fourni directement sur papier ou envoyé par courrier électronique en tant que document protégé par un mot de passe. Pour les organisations utilisant le CPIMS+, le formulaire de référencement de dossier en ligne doit préalablement être rempli, avec le destinataire du référencement ainsi que le service demandé. Il est de la responsabilité du gestionnaire de cas effectuant le référencement de sélectionner les informations clés à partager avec l'organisation le recevant.

PARTAGE D'INFORMATION PERSONNELLE DANS LE CADRE D'UN TRANSFERT :

Le transfert de cas signifie que gestionnaire de cas se dessaisie du dossier de l'enfant. Lors d'un transfert, l'organisation en charge du cas confie l'entière responsabilité de celui-ci à une autre organisation de manière définitive. La gestion du cas est alors confiée à un autre travailleur social.[13]

Quand le gestionnaire de cas est-il amené à partager des informations ?

[13] Procédures Opérationnelles Standards pour la gestion de cas de protection de l'enfance au Mali, 2020

5.6 Si un nouveau gestionnaire de cas ou une nouvelle organisation ou service devient responsable du cas, il est nécessaire de transférer le contenu du dossier à la personne destinataire, à moins qu'il ne soit dans l'intérêt supérieur de l'enfant de ne pas le faire.

Pourquoi partager les données dans cette situation ?

5.7 Le transfert de cas se réalise généralement lorsque le service/l'organisation qui a identifié l'enfant et qui a pu mener les premières étapes (évaluation initiale, prise en charge d'urgence) ne peut répondre aux besoins spécifiques d'un enfant ou ne peut pas continuer à fournir les services de gestion de cas.

Avec qui partager les données ?

5.8 Le gestionnaire de cas qui recevra le dossier et qui en assumera la responsabilité.

Quel type de données partager ?

5.9 Toutes les données, sauf si elles ne sont pas dans l'intérêt supérieur de l'enfant et sauf les données relatives à des aspects du cas qui ont été résolus et n'ont pas d'autres implications en matière de protection.

Comment effectuer ce partage de données ?

5.10 L'enfant et (le cas échéant) sa famille doit être consultés et consentir au transfert. Les agences utilisant le système CPIMS+ doivent remplir le formulaire de transfert de cas dans le système CPIMS+ et l'envoyer automatiquement à un autre utilisateur du système CPIMS+ ou l'exporter en format PDF et en fournir une copie papier ou l'envoyer par courrier électronique en tant que document protégé par un mot de passe. Le transfert doit être motivé et le service recevant le transfert a la possibilité d'accepter ou de rejeter le transfert. Lorsque le transfert à partir du CPIMS+ est accepté, le gestionnaire de cas ayant effectué le transfert n'a plus accès au dossier de l'enfant. Les organisations ou services qui ne peuvent pas utiliser le CPIMS+ doivent remplir le formulaire de transfert de dossier sur papier.

Considérations supplémentaires lors du partage d'informations pendant le transfert d'un dossier

5.11 Les transferts de cas peuvent avoir un impact important sur l'enfant concerné et doivent lui être soigneusement planifiés et expliqués, ainsi qu'à sa famille et à toute personne en charge.

5.12 Avant de procéder au transfert d'un dossier, il convient de vérifier si l'organisme d'accueil est disponible et/ou a la capacité de prendre en charge ce dossier ; à cette fin, des informations anonymes doivent d'abord être fournies. Ne fournissez jamais de données à caractère personnel si l'entité requise potentielle n'est pas en mesure de prendre en charge et de mener l'affaire, et ne jamais transférer un dossier tant que l'organisation recevant le transfert n'a pas donné son accord formel pour recevoir le dossier.

6. PARTAGE D'INFORMATION ANONYME

PARTAGE D'INFORMATION ANONYME POUR FACILITER LA COORDINATION ET ANALYSE DE TENDANCES

Quand le gestionnaire de cas est-il amené à partager des informations ?

6.1 Le partage de données à caractère personnel à des fins de suivi et de coordination de la situation n'est pas autorisé parce qu'il n'est pas nécessaire et qu'il est susceptible de causer un préjudice. Il est permis de partager des données anonymes et désagrégées à des fins de suivi et de coordination de la situation.

Pourquoi partager certaines données ?

6.2 L'objectif est de comprendre les profils/caractéristiques des enfants confrontés à divers types de risques, d'incidents et de vulnérabilités dans la région. Le suivi de la situation peut être généré et comparé dans le temps. En générant régulièrement des tendances et des modèles comparables, les organisations de

protection de l'enfance peuvent identifier les lacunes et les besoins, et donc informer leurs programmes et leur réponse. Un autre objectif est de compiler des informations sur la gestion des cas et les services fournis aux enfants afin de coordonner la fourniture de services.

Avec qui partager certaines données ?

6.3 Sous-groupe de travail gestion de cas / Groupes de travail en protection de l'enfance, et tout autre services ou organisation qui fera la demande et que la DNPEF jugera nécessaire de lui partager des données.

Quel type de données partager ?

6.4 Seules des données anonymes (non identifiables) peuvent être fournies

Comment effectuer ce partage de données ?

6.5 Les données anonymes peuvent être envoyées par courrier électronique pour les mettre dans un contexte. Des données anonymes peuvent également être extraites du système CPIMS+ par l'administrateur du système ou les points focaux des organisations et des services. Ils seront exportés au format XLS, CSV ou en Graphique PNG et envoyées par courrier électronique selon le même processus.

6.6 Voir TdR GTPE et sous-groupe gestion de cas, dans les Procédures Opérationnelles standards en gestion de cas de protection de l'enfance pour plus de précisions

PARTAGE D'INFORMATION AVEC DES BAILLEURS DE FONDS POUR RAPPORTAGE

Quand le gestionnaire de cas est-il amené à partager des informations ?

6.7 Le partage des données personnelles avec les bailleurs de fonds n'est pas autorisé parce qu'il n'est pas nécessaire ou approprié et qu'il viole les principes de confidentialité, de partage des informations en cas de besoin de savoir, d'intérêt supérieur de l'enfant et, éventuellement, le principe de non-récidive. Le partage de données anonymes et agrégées dans le but de se conformer aux accords de financement et de démontrer les résultats obtenus est autorisé

Pourquoi partager certaines données ?

6.8 Le partage de données anonymes est nécessaire pour garantir la responsabilité des bailleurs de fonds quant à l'utilisation appropriée des fonds et pour montrer le processus de fourniture de services de gestion des cas de protection de l'enfance. Cette forme de partage d'informations anonymes peut également :

a) Démontrer une compréhension des profils/caractéristiques des dossiers traités par les organisations ou services sous l'égide de certains bailleurs de fonds ;
b) Permettre aux bailleurs de défendre ou de fournir un financement supplémentaire pour renforcer ou étendre les services aux enfants et aux familles ;
c) Promouvoir la durabilité des programmes de gestion des cas.

Avec qui partager certaines données ? ?

6.9 Les données anonymes peuvent être partagés avec les points focaux gestion de l'information ou des experts techniques protection de l'enfant au sein des différents bailleurs de fonds ou organisme partenaires.

Quel type de données partager ?

6.10 Lors du partage de données anonymes avec les bailleurs à des fins de compte rendu ou lors de visites, les données suivantes peuvent être partagées (si nécessaire) :

- Âge
- Sexe

- Lieu
- Statut du dossier (c'est-à-dire ouvert ou clos)
- Type de problème de protection
- Type de prise en charge
- Date d'admission
- Type de services nécessaires (actions dans le plan d'action)
- Type de services fournis
- Service fourni avec succès (o/n)
- Date de clôture d'un cas

Comment effectuer ce partage de données ?

6.11 Les données désagrégées peuvent être partagées en utilisant le modèle de rapport du bailleur ou de chaque organisation, à condition qu'elles soient conformes au contenu du présent protocole (c'est-à-dire uniquement l'ensemble de données décrit au paragraphe 6.8 et pas de données personnelles). Les données brutes désagrégés peuvent être exporté à partir du CPIMS+ en XLS ou CVS afin d'effectuer des analyses très pointues et répondre aux besoins d'informations statistiques.

7. ARCHIVAGE ET DESTRUCTION DES DONNEES PERSONNELS

7.1 Lorsqu'un dossier de protection de l'enfance est clos, la copie papier et la copie électronique sont archivées dans un lieu sûr (classeur verrouillé ou CPIMS+, respectivement) pour une durée de 7 ans. Après cette période, le dossier sera détruit. Cette information devrait être intégré dans le consentement éclairé de l'enfant et la famille.

7.2 Les organisations ou services faisant la gestion des cas et/ou utilisant le CPIMS+ s'engagent à élaborer un plan d'évacuation/réinstallation en cas d'urgence telle qu'une inondation ou une autre catastrophe naturelle. Ce plan doit comprendre un schéma de délégation expliquant qui est responsable du retrait et, si nécessaire, de la destruction des fichiers papier et électroniques, ce qui peut nécessiter la destruction des biens et l'incinération des papiers. Ce plan doit être intégré dans le plan standard d'évacuation/réinstallation de l'autorité ou de l'agence participante, mais la nature sensible des données relatives à la gestion des dossiers de protection de l'enfance doit être soulignée à l'ensemble du personnel concerné, y compris les cadres supérieurs et les responsables de la sécurité.

8. DEFINITIONS

Confidentialité	Veiller à ce que les informations divulguées par un enfant ne soient pas utilisées sans son consentement ou contre sa volonté et ne soient pas partagées avec d'autres sans sa permission, sauf dans des circonstances exceptionnelles (c'est-à-dire lorsque cela est nécessaire pour la protection et la sécurité de l'enfant ou lorsque les prestataires de services sont tenus par la loi de signaler des informations, y compris des abus).
Données à caractère personnelle	Les données à caractère personnel ou données personnelles sont des informations existant sous diverses formes et permettant d'identifier directement ou indirectement une personne, par référence à un numéro d'immatriculation ou à un ou plusieurs éléments propres à son identité physique, physiologique, biométrique, génétique, psychique, culturelle, sociale ou économique. Elles peuvent être des identifiants universels permettant de raccorder entre eux, plusieurs fichiers

	constituant des bases de données, ou de procéder à leur interconnexion[14].
Donnée nominative	Les données nominatives font parties intégrantes des données à caractère personnelle. Selon la définition issue de la loi relative à la protection des données, « Donnée nominative : elle correspond aux noms, prénoms, adresse physique ou électronique d'une personne, ses références de sécurité sociale, son numéro de carte de paiement ou de compte bancaire, de plaque d'immatriculation de véhicule, sa photo d'identité, son empreinte digitale ou son ADN[15].
Donnée sensible	Toute donnée à caractère personnel relative aux opinions ou activités religieuse, philosophique, politique, syndicale, à la vie sexuelle ou raciale, à la santé, aux mesures d'ordre social, aux poursuites, aux sanctions pénales ou administratives[16]. Les données sanitaires font intégrantes des données sensibles. Au titre de la Loi elle se définit comme toute information concernant l'état physique et mental d'une personne concernée, y compris ses données génétiques ou biologiques[17].
Fichier de données à caractère personnel	Tout ensemble structuré de données accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique[18].
Consentement éclairé	L'accord volontaire d'une personne (enfant ou parent/responsable d'enfants) qui a la capacité de donner son consentement, et qui exerce un libre pouvoir de choix. Pour donner son "consentement éclairé", la personne doit être en mesure de comprendre sa propre situation et de prendre une décision concernant celle-ci.
Consentement (assent)	La volonté exprimée de participer à des services, qui est évaluée comme ayant la capacité de donner un consentement éclairé, mais suffisamment âgée pour comprendre et accepter de participer à des services.
Signalement obligatoire	Le terme utilisé pour décrire les systèmes juridiques ou statutaires qui obligent les prestataires de services à signaler certaines catégories de crimes ou d'abus (par exemple, la violence sexuelle, la maltraitance des enfants, etc.) ; l'intérêt supérieur de l'enfant doit être pris en compte lorsque les agences envisagent de se conformer ou non à ces lois.
Besoin de savoir	Limitation des informations considérées comme sensibles, et partage de ces informations uniquement avec les personnes pour lesquelles elles seront utilisées pour la protection de l'enfant.
Violation des données à caractère personnel	Violation de la sécurité des données entraînant accidentellement ou illégalement la destruction, la perte, l'altération, la divulgation ou l'accès non autorisés de données à caractère personnel transférées, stockées ou traitées de toute autre manière.

14 Article3 paragraphe 5 Loi n° 2013-015 du 21 mai 2013 Portant protection des données à caractère personnel en république du Mali

[15] *Article3 paragraphe 8 Loi n° 2013-015 du 21 mai 2013 Portant protection des données à caractère personnel en république du Mali*

[16] *Article3 paragraphe 11 Loi n° 2013-015 du 21 mai 2013 Portant protection des données à caractère personnel en république du Mali*

[17] *Article3 paragraphe 12 Loi n° 2013-015 du 21 mai 2013 Portant protection des données à caractère personnel en république du Mali*

[18] *Article3 paragraphe 13 Loi n° 2013-015 du 21 mai 2013 Portant protection des données à caractère personnel en république du Mali*