Guide pratique pour la protection des données dans le cadre de l'assistance en espèces et sous forme de coupons

Un supplément à la boîte à outils de l'argent en espèces dans les situations d'urgence

Janvier 2021

IFRC

Sommaire

I. Introduction

Au fur et à mesure que le Mouvement international de la Croix-Rouge et du Croissant-Rouge met en œuvre ses engagements visant à intensifier les transferts monétaires (TM) mais aussi sa collecte et son traitement des données personnelles, en particulier celles des communautés vulnérables desservies. La protection des données n'est pas seulement une question de bonne gouvernance ; il s'agit également d'instaurer la confiance. En temps de crise, les bénéficiaires peuvent penser à des priorités plus urgentes et nécessaires à leur survie et à leur sécurité qu'aux risques pour leurs données personnelles transmises aux organisations humanitaires. C'est une raison de plus pour les praticiens financiers de respecter et d'être responsables de la protection des données des bénéficiaires. En outre, d'autres parties prenantes telles que les donateurs, les entités gouvernementales et d'autres partenaires voueront une confiance accrue en nos programmes de TM lorsque de bonnes normes et pratiques en matière de protection des données seront démontrées.

Public cible et objectif du document

Ce guide pratique est destiné aux **praticiens financiers** ou à ceux qui gèrent des programmes pour intégrer les principes de protection des données dans leur mise en œuvre des TM. Il existe de nombreuses références utiles en matière de protection des données disponibles pour l'humanitaire, notamment le Manuel sur la protection des données dans l'action humanitaire et les politiques respectives de protection des données de la FICR et du CICR. Bien que ces références soient de nature plus générale ou n'abordent que certains des problèmes auxquels sont confrontés les praticiens financiers à un niveau élevé, ce document vise à traduire les principes généraux de protection des données en guides pratiques et exploitables, spécifiques aux activités clés du processus de transferts monétaires. Ce guide indique les principes clés de protection des données et guideront les praticiens financiers dans leur prise de décision et leur mise en œuvre.

Ce document fait référence aux processus de la boîte à outils Cash in Emergencies (boîte à outils, transfert monétaires en situation d'urgence) et complétera la boîte à outils jusqu'à ce qu'elle soit révisée pour inclure directement les principes relatifs à la protection des données expliquées dans ce document.

IMPORTANT :
Ce guide doit être contextualisé par les Sociétés nationales pour répondre aux exigences qui leur sont propres ; en particulier, le respect de leurs lois et politiques nationales de protection des données qui peuvent s'avérer plus strictes que les normes de protection des données ci-appliquées.

Structure du document

La section suivante fournira un aperçu de la protection des données afin de présenter aux lecteurs les principes clés et les terminologies qui seront utilisés dans ce guide. Elle sera ensuite suivie de chapitres pour chacun des cinq procédures clés de TM.

Avant de développer ce guide, une analyse de la boîte à outils CiE a été effectuée pour identifier les processus dans lesquels les données personnelles des bénéficiaires sont collectées et traitées. Les procédures ont ensuite été hiérarchisées en fonction du niveau de traitement des données personnelles et des risques potentiels. Ce guide se focalise sur cinq de ces procédures prioritaires[1] :

1. Ciblage
2. Inscription des bénéficiaires
3. Recours aux prestataires de services financiers
4. Divulgation de données au gouvernement, à d'autres organismes humanitaires et donateurs
5. Suivi Post-Distribution

[1] Il s'agit d'un document évolutif et des conseils pratiques pour d'autres domaines de la boîte à outils CiE peuvent être développés dans des révisions ultérieures à mesure que nous évoluons dans notre expérience en matière de protection des données.

Chaque chapitre sera un aperçu de la manière dont les données personnelles sont utilisées ou traitées avec des exemples issus de consultations avec les Sociétés nationales. Il sera ensuite suivi d'un ensemble de dispositions relatives à la protection des données basées sur des décisions ou des questions clés du projet.

Chaque disposition commence par un encadré mettant en évidence une décision ou une question clé du projet. Une icône en forme de cloche indique les principes de protection des données concernés par la disposition. Un encadrement de la question utile du projet est ensuite fourni pour intégrer la disposition de protection des données. Ces dispositions sont expliquées plus en détail et accompagnées d'exemples simplifiés pour montrer comment les appliquer.

Le dernier chapitre concerne les généralités applicables à l'ensemble du cycle du programme de TM.

II. Aperçu de la protection des données

Traitement des données personnel

Qu'est-ce qu'une donnée à caractère personnel ? Les **données personnelles** englobent toute information pouvant conduire à l'identification d'une personne physique vivante (la personne concernée). Les données peuvent être personnelles même si à première vue, elles peuvent ne pas sembler être directement liées à une personne mais pourraient conduire à une identification indirecte par usage d'informations supplémentaires. Cela peut sembler compliqué, mais cela signifie essentiellement que la protection des données englobe un large éventail d'informations et que le terme « données personnelles » ne doit pas être interprété de manière restrictive. Dans le cadre de la TM, la plupart des données que vous recueillerez auprès des bénéficiaires seront qualifiées de données personnelles, par exemple :

- Noms et coordonnées
- Numéros ID
- Numéros de compte bancaire
- Informations professionnelles
- Situation familiale
- État de santé
- Adresse ou géolocalisation

Au contraire, les données que vous recueillez pour analyser la situation à un **niveau abstrait** (par exemple, les informations économiques de la région, etc.) ne sont généralement pas considérées comme des données à caractère personnel. Ces données sont anonymes, car elles ne traitent pas du tout des informations personnelles, ou parce que les informations sont sous forme agrégée. Les **données agrégées** sont des données créées en résumant et en combinant des données individualisées. Les individus ne sont pas identifiables dans les données agrégées (ni directement, ni indirectement), qui fournissent généralement un aperçu général à l'aide de graphiques, de tableaux, de statistiques et d'informations générales sur des groupes de personnes, et non des individus. Parmi les exemples figurent des statistiques sur les types de moyens d'existence, la taille ou le revenu moyen des ménages, les pourcentages sur les dommages causés au logement dans une zone ou le calcul du panier de dépenses minimum (MEB).

Le **traitement** des données personnelles signifie essentiellement tout ce que vous faites des données, comme le recueil, le stockage, l'organisation, la divulgation, l'évaluation, la modification, la publication, l'enregistrement, l'utilisation, la correction et même la suppression de ces données.

Base légitime

Tout traitement de données personnelles nécessite une base légitime (ou *légale*). Une base légitime couramment utilisée est le consentement. Cependant, il existe plusieurs autres motifs justifiant le traitement légitime des données personnelles, notamment :

- Respect d'une obligation légale
- Exécution d'un contrat avec la personne concernée
- Une tâche d'intérêt public
- Intérêt(s) vital (vitaux) d'une personne (menace à court terme pour sa santé mentale ou physique)
- Intérêt légitime de l'entité (il peut s'agir de la FICR, du CICR, d'une Société nationale, par exemple) traitant les données personnelles

Sur quelle base légitime s'appuyer peut parfois s'avérer difficile. Pour de plus amples renseignements sur la définition et les différences de ces bases légitimes, veuillez consulter la Politique de la FICR et le Manuel sur la protection des données dans l'action humanitaire du CICR et du Centre de confidentialité de Bruxelles.

Pour les TM, il est assez courant de s'appuyer sur le consentement. De nombreux praticiens financiers comprennent une question de consentement au début d'un sondage ou d'un formulaire de recueil de données. Cependant, pour les urgences, ce n'est pas nécessairement la meilleure option. Ceci est expliqué plus en détail dans le chapitre Inscription des bénéficiaires avec un arbre de décision pour aider à évaluer si une ou plusieurs autres bases légitimes peuvent être plus adéquates dans les circonstances en question.

Principes-clés de protection des données

Il existe plusieurs principes de protection des données à prendre en compte lors du traitement des données personnelles. Bien que les noms puissent varier en fonction de la politique ou de l'instrument international, il est généralement admis que les plus grands principes de protection des données sont : (1.) légalité, équité et transparence ; (2.) limitation de la finalité ; (3.) minimisation des données ; (4.) précision ; (5.) limitation du stockage ; et (6.) intégrité et confidentialité (sécurité). Pour de plus amples renseignements, cf veuillez consulter la Politique de la Fédération internationale sur la protection des données et le Manuel sur la protection des données dans l'action humanitaire.

Cependant, aux fins de ce guide, nous nous concentrerons sur les principes les plus importants en termes de TM (en notant que le principe de légalité, ou de « base légitime », a déjà été évoqué ci-dessus). Les principes feront souvent l'objet d'une discussion commune s'ils doivent être étudiés conjointement pour effectuer l'analyse pertinente de la protection des données, quand bien même ils sont à proprement parler considérés comme des principes distincts. Par exemple, dans la section suivante, nous discutons de deux principes distincts à la fois, à savoir « minimisation des données » et « limitation des finalités », car il n'est pas possible d'évaluer quelles données sont nécessaires sans une évaluation des finalités du recueil/traitement des données.

Minimisation des données, nécessité et limitation des finalités

Le principe de minimisation des données signifie « recueillir le moins possible et UNIQUEMENT autant que nécessaire ». Pour définir ce qui est nécessaire, il est important d'identifier clairement la *finalité* pour laquelle les données respectives doivent être utilisées. Dans le contexte des TM, le traitement des données personnelles peut servir à diverses finalités (par exemple, vérifier par rapport aux critères de ciblage, vérifier l'identité, faciliter la distribution monétaire, détecter ou éviter la fraude et surveiller l'incidence du programme). Le traitement des données personnelles doit être *nécessaire* pour atteindre la finalité en question. Avant de recueillir des informations, il est essentiel de comprendre quelles informations sont nécessaires dans le contexte spécifique. Si vous ne savez pas pourquoi vous recueillez un ensemble particulier de données ou pensez que cela peut être utile plus tard sans justification spécifique, ou si vous pensez simplement qu'il convient mieux de recueillir le plus de données auprès des bénéficiaires, alors vous allez probablement recueillir plus de données personnelles qu'il ne l'est absolument *nécessaire*. Pour identifier clairement quelles données sont nécessaires, il est suggéré de revoir les principes de minimisation / nécessité / limitation des données. Ces questions sont fondamentales pour la protection des données et reviendront souvent dans ce guide. Plus d'informations et d'exemples utiles sont fournis dans le chapitre Ciblage.

En outre, les données personnelles recueillies dans un seul but ne peuvent pas simplement être utilisées à d'autres fins. Bien entendu, un ensemble de données existant peut être utilisé à des fins futures dans certaines circonstances. Cependant, les objectifs futurs doivent généralement être « compatibles » avec l'objectif initial. Une telle compatibilité existe lorsque les finalités sont étroitement liées, et l'on peut supposer que la personne concernée ne serait pas étonnée de cette utilisation secondaire. Par exemple, à la fin d'un programme de TM, des fonds supplémentaires deviennent disponibles qui n'étaient pas attendus auparavant. Un examen des données des bénéficiaires précédemment recueillies afin de déterminer qui devrait recevoir une nouvelle assistance serait considéré comme compatible avec le but et la base juridique sur lesquels les données personnelles ont été précédemment recueillies. Dans le cas contraire, une base juridique adéquate devrait être identifiée et les personnes concernées pourraient avoir besoin de recevoir des informations mises à jour sur l'utilisation future prévue (cf. prochain principe de transparence).

Transparence

La transparence va de pair avec la justice. L'idée est d'être franc et honnête sur le traitement des données personnelles. En vertu du principe de transparence, les personnes concernées devraient toujours recevoir certaines informations clés sur ce qu'endurent leurs données, notamment :

- le fait que leurs données personnelles sont en cours de traitement et la base de ce dernier
- qui traitera les données
- dans quel(s) but(s) les données sont traitées
- comment les données sont stockées et pendant combien de temps
- si leurs données sont destinées à être communiquées avec une tierce entité
- leurs droits quant au traitement, tels que le droit de rectification et de suppression
- les coordonnées ou une personne à qui s'adresser en cas de questions ou de réclamations des personnes concernées

La forme sous laquelle ces informations sont fournies dépend du contexte. Des exemples spécifiques seront donnés tout au long du guide.

Sécurité des données (confidentialité, intégrité, limitation de stockage)[2]

Les données personnelles doivent être traitées de manière confidentielle et sécurisée. Cela peut paraître évident, mais il n'est pas toujours évident de savoir ce qu'il faut faire pour garantir la confidentialité. La loi sur la protection des données (ou la politique, le cas échéant) exige la mise en œuvre de diverses mesures de sécurité, telles que les restrictions d'accès et la prévention de la perte de données. Le but ultime est d'éviter les violations de données, c'est-à-dire *l'accès non autorisé à, ou la destruction, la perte, l'altération ou la divulgation de données personnelles.*

III. Ciblage

Usage de données personnelles

Le ciblage de l'aide monétaire s'appuie sur les objectifs du programme et sur l'évaluation des besoins. Il aligne les activités du programme sur des bénéficiaires spécifiques en utilisant des critères de ciblage définis, qui comprennent généralement des indicateurs socio-économiques et de vulnérabilité. Cf. section M3_3 de la boîte à outils CiE pour de plus amples renseignements.

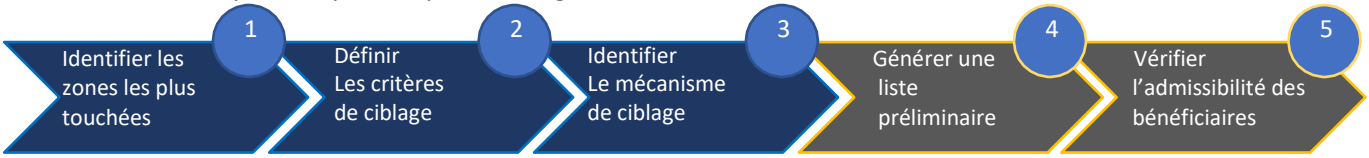

Figure 1 : Étapes du processus de ciblage

Les étapes générales du processus de ciblage sont illustrées à la *figure* 1. Cette procédure peut s'appuyer

[2] La limitation du stockage est normalement considérée comme un principe distinct.

sur des données préalablement recueillies pour éclairer la définition des critères et accélérer la création de la liste préliminaire des bénéficiaires pouvant prétendre à une aide TM.

Les étapes 1 à 3 parcourent les décisions clés du ciblage en fonction des objectifs du programme. Ces décisions peuvent être :

- Quels emplacements géographiques seront sélectionnés pour l'intervention ?
- Des distributions générales ou ciblées ?
- Que ce soit pour cibler les ménages ou les individus ?
- Quels critères de ciblage choisir en fonction de la vulnérabilité, des apports socio-économiques ou spécifiques au contexte ?
- Quel mécanisme de ciblage choisir (mécanisme de ciblage catégorique, autonome ou communautaire) ?

En général, les données personnelles ne jouent qu'un rôle peu important dans ces trois premières étapes. Les décisions sont fondées sur des informations générales ou des données agrégées sur les zones touchées et la population dans son ensemble. Ici, la situation individuelle des bénéficiaires potentiels n'est encore d'aucun intérêt, mais plutôt la situation globale sur le terrain et les objectifs du programme.

Les étapes 4 et 5, cependant, abordent les données personnelles car les bénéficiaires potentiels sont analysés, comparés aux critères fixés et une liste préliminaire des bénéficiaires est dressée avant le processus officiel d'inscription des bénéficiaires. La liste comportera au minimum les noms des bénéficiaires, et le processus d'analyse ou de vérification peut impliquer des informations détaillées sur les bénéficiaires.

À l'étape 4, la liste préliminaire est généralement élaborée en fonction du mécanisme de ciblage décidé à l'étape 3 :

- **Ciblage communautaire :** ménages vulnérables identifiés par les dirigeants et les membres de la communauté sur la base des critères convenus ; les résultats sont triangulés et vérifiés par la Société nationale. Par exemple, les dirigeants communautaires ont demandé d'identifier les ménages dont la maison était totalement détruite.
- **Ciblage par auto-sélection**: les individus sont invités à fournir des informations sur eux-mêmes et des détails relatifs aux critères convenus. Par exemple, l'équipe du programme recherche des adultes valides souffrant d'insécurité alimentaire et désireux de participer à un programme de travail contre rémunération.
- **Ciblage catégorique** : l'admissibilité est fondée sur des catégories spécifiques de vulnérabilité (par exemple, les ménages dirigés par des enfants) et potentiellement un bon registre civil pour décider des individus appartenant à une catégorie spécifique à sélectionner. Par exemple, il est demandé aux autorités locales de fournir une liste des membres de la communauté en situation d'extrême pauvreté.

Quel que soit le mécanisme de ciblage choisi, cette étape repose sur des données recueillies auprès de différentes sources (par exemple, le gouvernement, les communautés locales, d'autres organisations ou des particuliers). Bien que la liste préliminaire puisse être obtenue auprès d'une autre source, le fait de prendre cette liste constitue déjà une utilisation de données personnelles. En l'absence de liste préliminaire disponible, la Société nationale peut choisir de faire du porte-à-porte dans les communautés touchées pour dresser une telle liste demandant des données personnelles.

À l'étape 5, l'admissibilité de toutes les personnes nommées sur la liste préliminaire est vérifiée. Ce processus peut impliquer des représentants de la communauté ou des dirigeants locaux qui ont une connaissance actuelle de la population ou qui ont compilé des informations en utilisant d'autres données ou systèmes (par exemple, des listes d'état civil ou de protection sociale). Dans certains cas, une Société nationale peut vérifier directement en porte-à-porte auprès des bénéficiaires afin de vérifier qu'ils sont

effectivement admissibles sur la base des données personnelles qu'ils fournissent. La procédure de cette vérification en porte-à-porte peut être effectuée parallèlement à la création de la liste préliminaire à l'étape 4. Ce processus de vérification peut être similaire au processus d'enregistrement des bénéficiaires et peut utiliser des formulaires d'enquête et une base de données pour collecter et gérer des données personnelles structurées ou peut simplement être ad hoc avec un stylo et du papier pour cocher les critères auxquels correspond le bénéficiaire, également considérés comme données personnelles.

À la fin du processus de ciblage, la liste des bénéficiaires vérifiés peut être divulguée et publiée au sein de la communauté (c'est-à-dire que la liste est imprimée et affichée dans un espace public pour que la communauté vérifie qui est intégré dans l'intervention). La publication de cette liste est qualifiée d'utilisation (de traitement) de données personnelles, parce que vous rendez les données sous votre contrôle accessibles à d'autres : à tous les membres de la communauté, afin qu'ils puissent évaluer la liste.

Dispositions relatives à la protection des données

Le processus de ciblage impliquera le traitement des données personnelles lors de l'établissement de la liste préliminaire des bénéficiaires et lors de la vérification de cette liste. Cette section examinera les décisions clés du projet dans le processus de ciblage et les dispositions liées à la protection des données. Le principe le plus important abordé dans cette section est la **minimisation / nécessité des données**. Tous les autres principes concernent le traitement des données que vous avez recueillies, tandis que la minimisation et la nécessité des données visent à limiter le recueil de données en premier lieu. Le fait de ne pas recueillir des données dont vous n'avez pas vraiment besoin pour le programme est le moyen le plus efficace de renforcer le niveau de protection des données. Par conséquent, lors de la mise en place du programme et avant de recueillir des données sur les bénéficiaires, il est essentiel de réfléchir au cycle du programme et de décider à l'avance quelles données seront nécessaires tout au long de ce dernier.

Décision projet 1 : Doit-on utiliser les données des bénéficiaires recueillies par une source externe ?

🔔 Minimisation, nécessité et sécurité des données

Décision de projet reformulée : Ai-je besoin des données recueillies par une source externe et comment puis-je m'assurer que les données des bénéficiaires ont été recueillies de manière adéquate ?

Lors de la création de la liste préliminaire des bénéficiaires, il est courant d'utiliser les données des bénéficiaires provenant de sources externes telles que d'autres organisations ou le gouvernement. Ainsi, la question de la décision du projet peut sembler évidente et nécessaire. Cependant, la question de décision de projet reformulée recommande aux praticiens financiers d'adopter une approche nuancée pour demander et utiliser des données provenant de sources externes, en gardant à l'esprit les principes de minimisation des données et de sécurité des données, en particulier en l'absence d'accord de diffusion de données établi.

Voici les éléments clés à prendre en compte lorsque vous envisagez d'utiliser les données des bénéficiaires recueillies par des sources externes (autres ONG, le gouvernement, etc.) :

- **Cette organisation est-elle fiable et puis-je faire confiance à ses données ?** Si l'organisation offrant les données n'est pas bien reconnue, vous voudrez peut-être demander ou enquêter sur la manière dont elle a recueilli ses données, et déterminer si elle est fiable ? Le problème ici n'est pas seulement que les données peuvent être incomplètes ou erronées, mais aussi que les données peuvent avoir été obtenues de manière illégitime (par exemple, sans base juridique claire ou sans que les bénéficiaires

soient informés de la manière dont leurs données seront partagées avec d'autres, surtout si elles sont très sensibles). Selon le contexte, il serait utile de demander aux dirigeants communautaires ou à d'autres organisations actives dans la région s'ils connaissent déjà cette organisation et lui font confiance. Il est également conseillé de demander à l'organisation de vous donner des informations sur le déroulement du recueil. Il est important de savoir si les bénéficiaires savent que leurs données peuvent être vous être transmises. Si vous doutez que les choses aient été faites aussi correctement, c'est un indicateur que vous voudrez peut-être étudier d'autres sources de données.

- **Quelles données doit-on demander et accepter ?** Le fait qu'une autre organisation a recueilli une certaine quantité ou un certain type de données ne signifie pas que vous devez en prendre **la totalité ou la majeure partie**. Encore une fois, il est judicieux de réfléchir au principe de la minimisation et de la nécessité des données. Cela dépend du projet, et des données que vous devez demander ou accepter. Si l'autre organisation vous fournit plus de données que vous n'en avez besoin, il est recommandé de demander uniquement ces données, et si des données inutiles sont fournies, il convient de supprimer ces données et d'informer l'autre organisation afin qu'elle sache ce qui a été conservé. La prudence est recommandée si l'ensemble de données comporte des catégories de données très sensibles, telles que des informations sur la santé, les pratiques religieuses ou la vie intime d'un sujet, en particulier si ces données ne sont pas d'importance directe pour les besoins de votre programme. Le fait qu'une organisation fournisse librement des données de ce genre avec ou sans accord officiel de divulgation de données pourrait indiquer des critères de protection des données médiocres ou inexistantes. En outre, les données reçues de l'extérieur doivent être traitées de manière responsable.

Le cas de figure décrit ci-dessus n'implique aucun accord de divulgation de données entre les parties et, par conséquent, le contrôle des données devient une disposition importante. Pour les programmes de TM où la Société nationale est un partenaire de mise en œuvre d'une autre agence, l'échange de données doit être convenu entre les partenaires concernés, externes ou non, dispositions qui peuvent être évaluées lors de la négociation de l'accord de divulgation de données. Si, dans le cadre de ces programmes financier, vous avec des scrupules au sujet de la protection des données en ce qui concerne la divulgation de données à des tiers, faites-en part à votre responsable ou à l'équipe juridique de votre Société nationale et notez les risques / scrupules dans votre matrice des risques de TM.

Exemple :

Le critère cible est « les ménages avec enfants qui ont perdu leur maison durant l'inondation ».

L'équipe de la Société nationale demande au gouvernement local de fournir :

- des « informations importantes » sur les résidents de la zone. Cette demande est très vague et il est probable que le gouvernement fournira plus d'informations que nécessaire. Cette demande devrait être restreinte.

- « Les noms et la situation familiale de tous les habitants des zones touchées. » Cette demande est plus spécifique, mais encore trop vague. Les personnes sans enfants ne sont pas ciblées. Par conséquent, leurs noms ne seront probablement pas nécessaires.

« Seuls les noms des résidents des zones touchées qui ont des enfants. » Cela sera probablement nécessaire et suffisant.

À la suite d'un séisme, la Société nationale tente d'identifier les personnes qui ont perdu leur maison. Une association du village le plus touché propose de diffuser une liste de personnes actuellement sans abri en raison du séisme. La Société nationale examine attentivement cette offre. Ils contactent le maire du village et s'enquièrent de la réputation de l'association. En outre, ils ont contacté l'association concernant leur procédure de recueil de données. L'association explique avoir informé les résidents de la protection des données et de son intention de communiquer des données à d'autres organisations humanitaires. Les données recueillies par l'association comprenaient les noms, le nombre de membres de la famille, l'âge des enfants ainsi qu'un numéro de téléphone portable. La Société nationale prévoit une distribution générale pour tous les ménages ayant perdu leur logement. Par conséquent, ils décident que pour leur intervention, ils n'ont besoin que du nom des bénéficiaires et de leurs numéros de téléphone portable pour les contacter. L'équipe s'assure de recevoir exclusivement ces données.

Décision projet 2 : Comment vérifier l'admissibilité des bénéficiaires ?

🔔 Minimisation, nécessité et confidentialité

Décision de projet reformulée : De quelles données ai-je vraiment besoin pour vérifier l'admissibilité des bénéficiaires?

Le but de la vérification ou « contrôle d'admissibilité » est de savoir si une personne (ou un ménage) répond réellement aux critères cibles. Elle a généralement lieu à **l'étape 5** du ciblage susmentionné, où il peut s'avérer nécessaire de recueillir ou d'analyser des données relatives au bénéficiaire. Lors de cette vérification, il est important de ne pas recueillir ou traiter plus de données que nécessaire pour mener à bien la mission (principe de minimisation et nécessité des données). Différentes méthodes permettent de vérifier l'admissibilité et elles peuvent nécessiter ou traiter les données personnelles différemment :

- **Utilisation des membres de la communauté pour la vérification.** Si l'on emploie cette méthode, les bénéficiaires effectifs pourraient ne pas encore être consultés directement. Les membres de la communauté qui ont connaissance de la situation ou des détails personnels des bénéficiaires peuvent alors fournir une liste préliminaire des bénéficiaires potentiellement admissibles. Cela pourrait être suivi d'un contrôle de vérification plus officiel pendant le processus d'inscription des bénéficiaires. Si l'on emploie cette méthode, il est important que la vie privée des bénéficiaires soit protégée, en particulier si la méthode est appliquée dans un cadre public (c'est-à-dire auprès d'autres membres de la communauté), puisque les bénéficiaires réels ne peuvent pas s'opposer à la divulgation d'informations que d'autres connaissent déjà à leur sujet. Les questions posées aux dirigeants communautaires sur les données concernant les bénéficiaires doivent être réduites au minimum et les questions sensibles doivent être évitées dans un cadre public. Si des informations susceptibles d'être jugées sensibles sont nécessaires pour le programme, essayez de ne recueillir ces informations que dans un cadre privé, par vérification en porte-à-porte, par exemple.

- **Vérification en porte-à-porte.** Avant de visiter effectivement les ménages bénéficiaires pour vérifier leur admissibilité, il est important d'identifier quelles données sont absolument nécessaires à cette fin, en respectant toujours le principe de minimisation et de nécessité des données. Étant donné que le travail requis pour une vérification en porte-à-porte peut s'avérer conséquent, il peut y avoir une tendance à demander plus d'informations que ce qui est strictement nécessaire, afin d'éviter de voir rendre visite une seconde fois. Par conséquent, une préparation quant à la portée et à

l'objectif du programme est essentielle, afin de ne demander que le minimum absolu nécessaire à la vérification. Si vous ignorez si vous devez demander une certaine information, posez-vous la question suivante : Quelle incidence auront ces informations sur ma décision de cibler le bénéficiaire individuel ? Si vous n'êtes pas sûr, cela peut être inutile.

- **Publication de la liste préliminaire des bénéficiaires.** Dans le cadre de l'étape 4 ou après l'étape 5 du processus de ciblage illustré susmentionnée, la liste préliminaire des bénéficiaires est généralement diffusée et publiée dans un cadre public (par exemple, dans une salle communautaire). Il s'agit de créer de la transparence et d'informer la communauté de qui a été sélectionné sur la base de critères de ciblage convenus. Cela permet également à ceux qui ne figurent pas sur la liste mais qui satisfont aux critères de ciblage d'être sélectionnés dans le programme. Cette liste comportera des données personnelles, il sera donc important de minimiser ce qui est communiqué publiquement. En règle générale, les noms et la position approximative suffisent, et les détails ou données utilisés dans la vérification du ciblage ne sont pas nécessaires. Cependant, sachant que la liste des noms est liée à certains critères définis (même si les détails de ces critères peuvent ou non être satisfaits), elle informe le grand public de certains aspects concernant les personnes répertoriées qui pourraient porter atteinte à leur vie privée. La question de savoir si cela pose problème du point de vue de la protection des données dépend du contexte. Dans un petit village où les conditions de vie de tous les habitants sont, quoi qu'il en soit, connues de tous (ce qui signifie qu'ils correspondent ou non aux critères cibles), la publication de la liste peut ne pas être vraiment problématique en termes de respect de la vie privée. En revanche, dans un contexte où les bénéficiaires vivent dans l'anonymat relatif, la publication de la liste pourrait poser problème. La divulgation d'informations qui n'étaient pas connues du public auparavant est susceptible d'enfreindre le principe de confidentialité. Par conséquent, il est recommandé d'étudier scrupuleusement le contexte avant de décider de publier ou non la liste.

En outre, après le processus de vérification ou de contrôle d'admissibilité, les données de ceux qui ont été jugés non admissibles doivent être traitées de manière responsable (par exemple, archivées en toute sécurité en cas d'exigences d'audit, sous forme de liste simplifiée maintenue afin d'éviter une seconde vérification, ou supprimées si elles ont perdu toute utilité). Vous trouverez de plus amples renseignements à ce sujet dans le chapitre du guide général.

Exemples de nécessité et de minimisation lors des contrôles d'admissibilité:

Dans le cadre d'un programme, le critère cible est « les ménages prenant en charge des personnes handicapées ». Pour le contrôle d'admissibilité, il est nécessaire de savoir s'il y a des membres handicapés réels vivant dans ce même ménage. Il peut être utile de connaître la nature de leur handicap. Lors de la vérification des faits, cela sera révélé lors de la visite à domicile, par exemple. Cependant, il n'est probablement pas nécessaire de consulter les dossiers médicaux pour vérifier le handicap et cela pourrait révéler des données personnelles sensibles, inutiles pour le programme.

Les leaders communautaires suggèrent de cibler les mères célibataires avec au moins trois enfants à charge et sans revenu comme les plus vulnérables, une liste préliminaire étant créée sur la base de ce critère. Les informations fournies par les leaders communautaires sont vérifiées lors des visites à domicile où le bénéficiaire est identifié et interrogé sur l'âge de tous les membres du ménage. Pour vérifier les revenus, il

peut s'avérer nécessaire de se renseigner sur les sources de revenus du bénéficiaire. Cependant, il ne serait probablement pas nécessaire de recueillir des informations supplémentaires telles que son âge ou sa religion, cela n'ayant aucune influence sur la décision de cibler ou non ce bénéficiaire. Il n'est pas non plus nécessaire de l'interroger sur ses employeurs précédents, ni de demander des relevés de compte en banque pour déterminer son niveau de revenu.

Dans le contexte d'une réponse à la famine, la catégorie cible pour le programme monétaire est « les ménages avec enfants en situation d'insécurité alimentaire ». Il probablement inutile de les interroger sur le niveau d'éducation des enfants lors du contrôle d'admissibilité. Le niveau d'éducation n'influencera pas le contrôle d'admissibilité, ni le montant du transfert monétaire.

Remarque : Lors du recueil et de tout autre traitement de données, il est important de rappeler que les données personnelles doivent être traitées en toute sécurité. Que les données soient recueillies sur papier, une application mobile ou par d'autres moyens, assurez-vous que les données ne sont accessibles qu'à ceux qui en ont strictement besoin. La sécurité des données doit être prise en compte à toutes les étapes, y compris la suppression de toutes les données, pour s'assurer qu'elles ne peuvent pas être récupérées. Vous trouverez de plus amples renseignements à ce sujet dans le chapitre du guide général.

Décision projet 3 : Doit-on parler aux bénéficiaires de la gestion de leurs données à ce stade ?

Transparence

Décision de projet reformulée : Comment puis-je m'assurer que les bénéficiaires ont accès aux informations relatives au traitement de leurs données ?

Un principe important de la protection des données est la transparence. Dans le cadre du contrôle d'admissibilité, le recueil d'informations peut être moins officiel que l'inscription du bénéficiaire. Néanmoins, il est important que les bénéficiaires sachent ce qu'il advient des informations qu'ils vous transmettent. De plus amples renseignements sur la manière d'informer les bénéficiaires sont fournis dans le chapitre Inscription des bénéficiaires, mais il est déjà judicieux de respecter ces normes lors de la vérification ou des contrôles d'admissibilité. Voici quelques aspects dont il faut informer le bénéficiaire :

- Où avez-vous obtenu les principales informations à leur sujet (par exemple, via les membres de la communauté, la liste du gouvernement, d'autres organisations ?)
- Pourquoi effectuez-vous le contrôle d'admissibilité
- Que des données erronées peuvent être corrigées à tout moment
- Que vous pourriez transmettre les données fournies à d'autres institutions et dans quel but (si tel est le cas)

IV. Inscription des bénéficiaires

Usage de données personnelles

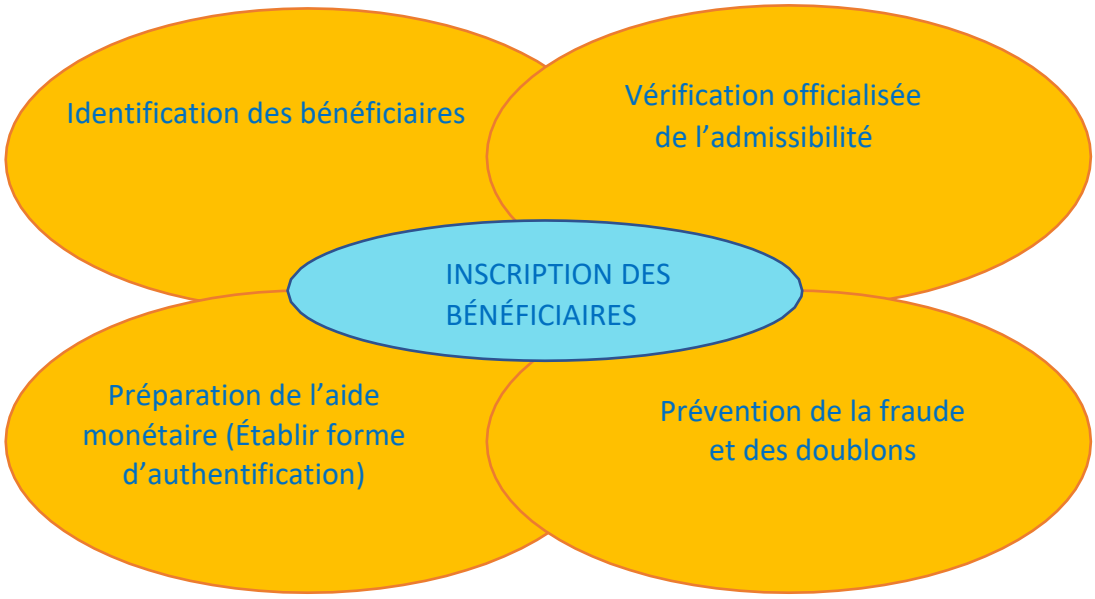

Figure 2 : Objectifs de l'inscription des bénéficiaires

Le processus d'inscription officielle des bénéficiaires se déroule généralement après la création d'une liste de bénéficiaires admissibles (voir la section M4_4 de la boîte à outils CiE pour de plus amples renseignements). Cela implique le recueil de données personnelles et la gestion de ces données pour la distribution et le suivi du programme. Figure 2 présente les finalités communes de l'inscription des bénéficiaires et les exemples ci-dessous expliquent l'utilisation des données personnelles :

- **Identification.** Au début du processus d'inscription, le chef de famille est généralement invité à présenter une pièce d'identité (par exemple, un permis de conduire, une pièce d'identité fiscale ou une carte d'électeur) pour s'assurer qu'il est bien celui qui figure sur la liste des bénéficiaires. Ces pièces d'identité doivent comporter leur nom, leur date de naissance et d'autres données personnelles susceptibles d'être saisies lors de l'inscription. Le bénéficiaire peut être invité à fournir des données biométriques (comme une empreinte digitale) pour une authentification solide et pour s'assurer qu'il n'a pas été inscrit plusieurs fois. Les données biométriques sont considérées comme personnelles et potentiellement sensibles.
- **Vérification officielle de l'admissibilité.** Le bénéficiaire devra répondre à des questions relatives aux critères de ciblage dans le cas où le processus de vérification n'a pas été effectuée officiellement auparavant, et s'il y a possibilité que les données aient évolué depuis que le ciblage a été fait ; en vue de s'assurer que le bénéficiaire est toujours admissible avant le déboursement.
- **Préparation à la distribution monétaire.** Le cas échéant, le bénéficiaire sera interrogé sur Sa connaissance de la clientèle (KYC) ou d'autres informations requises par le prestataire de services financiers (PSF) pour leur distribuer de l'argent (par exemple, numéro de téléphone mobile pour l'argent mobile ou données de compte en banque).
- **Établissement d'une forme d'authentification.** Le bénéficiaire reçoit une carte de bénéficiaire de la Croix-Rouge avec sa photo et un identifiant unique qu'il pourrait montrer au prestataire de services financiers en guise de preuve de son admissibilité et de son inscription. Cela s'avère particulièrement utile lorsque les pièces d'identité officielles ne sont pas disponibles.
- **Prévention de la fraude et des doublons.** Pour éviter la fraude et les doublons, le bénéficiaire

peut être invité à fournir des données personnelles relatives aux membres de sa famille ou des données biométriques.

Dispositions relatives à la protection des données

Le processus d'inscription des bénéficiaires impliquera le recueil et le traitement de données personnelles sur la base des objectifs communs décrits ci-dessus. Cette section examinera les décisions clés du projet dans le processus d'inscription et les dispositions liées à la protection des données.

Décision projet 1 : Comment vérifier l'identité d'un bénéficiaire ?

Minimisation, nécessité

Décision de projet reformulée : Quel mécanisme de vérification est efficace et interfère le moins avec les intérêts (y compris la vie privée) des bénéficiaires ?

Pour vérifier l'identité des personnes qui se présentent pour l'inscription, une pièce d'identité unique est nécessaire. Ces pièces d'identité uniques peuvent être sur papier (permis de conduire, carte nationale d'identité, etc.) ou biométriques (empreintes digitales ou rétiniennes, etc.). Lors de l'examen des différentes possibilités, certains aspects opérationnels devront être pris en compte, mais également la protection des données. Dans certains contextes, il serait presque inutile de demander des pièces d'identité au sein d'une communauté généralement dépourvue de tels documents. Dans d'autres contextes, le recueil de données biométriques peut sembler être le plus efficace et le seul moyen d'éviter la fraude. Du point de vue de la protection des données, il est important de garder à l'esprit que certaines données sont plus sensibles que d'autres. Dans la mesure du possible, l'objectif est de recueillir les données les moins sensibles.

Identification papier

Dans de nombreuses régions, le moyen le plus simple et le plus courant est de demander des pièces d'identité, telles que des cartes nationales d'identité ou des passeports délivrés par le gouvernement. Demander ces pièces d'identité ne présente pas un risque élevé du point de vue de la protection des données, puisque ces documents servent exactement à identifier leur détenteur. Savoir s'il est nécessaire de numériser ou de copier et de classer les pièces d'identité de chaque bénéficiaire est une question distincte. À des fins d'identification, il suffit souvent de demander au bénéficiaire de vous présenter sa pièce d'identité lors de l'inscription et de noter le numéro d'identification unique. Vous pouvez cocher la case indiquant que l'identité a été vérifiée sans conserver un exemplaire complet de la pièce d'identité. D'autres pièces d'identité ou documents comme un permis de conduire, acte de naissance, certificat de baptême, ou une facture d'électricité peuvent être acceptés à la place d'une carte d'identité nationale si de nombreux membres des communautés n'en possèdent pas. Lors du recueil de ces documents, il est à nouveau recommandé de recueillir le moins possible pour vérifier l'identité des individus. La quantité n'est pas toujours synonyme de qualité dans le contexte de la protection des données. En outre, il est recommandé de ne pas demander de documentation contenant des données sensibles (par exemple, des documents médicaux). En outre, comme il l'a été évoqué, il n'est pas forcément nécessaire de conserver des exemplaires de ces documents.

Données biométriques

Les données biométriques sont des données relatives aux caractéristiques physiologiques ou comportementales d'une personne, qui sont reconnues par des moyens technologiques. Les exemples typiques sont les empreintes digitales numériques, empreintes rétiniennes, palmaires, ainsi que la reconnaissance faciale et vocale. Ces données sont considérées comme très sensibles car elles sont très personnelles et ne peuvent pas simplement être remplacées si elles sont compromises, et méritent donc un niveau de protection plus élevé. Dans certains cas, les données biométriques sont soumises à des restrictions légales, comme une restriction ou une interdiction d'utilisation. La principale raison en est l'abus potentiel de ces données :

- **Application de la loi ou sécurité.** Les données biométriques peuvent s'avérer très utiles pour les forces de l'ordre ou les acteurs de la sécurité, car elles ne peuvent pas être modifiées. Lors du recueil de ces données dans le cadre d'un projet, vous pourriez être soumis à la pression d'autres parties de divulguer ces données à d'autres fins.
- **Usurpation d'identité.** Les données biométriques sont également plus susceptibles d'être piratées pour l'usurpation d'identité car elles sont uniques et ne peuvent pas être modifiées.
- **Source d'informations à venir.** Il est possible qu'à l'avenir, les données biométriques recueillies aujourd'hui puissent être utilisées pour en apprendre sensiblement plus sur un individu qu'il ne l'est possible actuellement. Les nouvelles solutions technologiques pourraient lire d'autres informations, telles que des détails génétiques.

Par conséquent, le recueil de données biométriques[3] présente un risque élevé et doit être considéré comme un dernier recours. Le recueil de ces données doit être évalué pour déterminer s'il est en effet absolument nécessaire ou si une solution alternative pourrait être choisie. Le contexte du projet ainsi que la responsabilité de l'organisation et sa capacité à protéger scrupuleusement ces données doivent être pris en compte. Même lorsque les données biométriques semblent être le meilleur moyen de vérifier l'identité des individus et d'éviter la fraude, les risques potentiels pour les bénéficiaires doivent encore être pris en compte. En particulier, s'il est probable que d'autres acteurs puissent revendiquer ces données à leurs propres fins, ce risque pourrait l'emporter sur les avantages pratiques des données biométriques. En outre, lors du recueil de données biométriques, les dispositions sur un stockage sûr et sécurisé sont d'autant plus importantes (voir le chapitre qui sert de guide général).

En outre, n'oubliez pas le droit de recevoir des informations (transparence). Ces informations doivent être présentées de sorte que les individus puissent les comprendre. Les connaissances générales des lettres et/ou de la biométrie peuvent être insuffisantes pour permettre de comprendre les risques associés à ce traitement (il convient de noter que des alternatives à l'inscription biométrique doivent toujours être envisagées, voir la décision de projet 3 ci-dessous).

[3] Pour de plus amples renseignements, veuillez consulter le chapitre sur la biométrie du Manuel sur la protection des données. Ainsi que celles de la Politiques des données biométriques du CICR.

Exemple :

Plusieurs zones géographiques ont été touchées par une pandémie entraînant une perte de leurs moyens de subsistance. Une intervention monétaire a été décidée pour une communauté urbaine bien développée et une autre dans une communauté rurale éloignée. Pour l'inscription, les chefs des ménages touchés dans le contexte urbain ont été invités à apporter une pièce d'identité à partir d'une liste de formulaires et de documents valides pour attester leur identité. Pour la communauté rurale, les chefs de famille ont été priés d'apporter une attestation de leurs chefs de village car ils n'ont aucune de pièce d'identité officielle. Les bénéficiaires de la zone rurale ont ensuite reçu une carte d'identité temporaire délivrée par la Société nationale à présenter au prestataire de services financiers lors de leurs démarches de demande d'argent. Dans les deux cas, le recueil de données biométriques pour l'identification a été évité et d'autres moyens de détection de fraude et de doublons ont été utilisés, tels que la vérification des noms et de l'âge des membres du ménage et l'émission d'un coupon à usage unique avec un code à barres unique qui a été scanné après la réception de l'argent auquel ils ont droit, pour indiquer qu'ils l'avaient déjà reçu.

Décision projet 2 : Quelles sont les autres données à recueillir auprès des bénéficiaires durant l'inscription ?

Minimisation, nécessité

Décision de projet reformulée : Quelles autres données sur les bénéficiaires sont essentielles au programme ?

Outre le recueil de données pour l'identification, il existe d'autres types de données recueillies lors de l'inscription à d'autres fins mentionnées ci-dessus. À ces fins, il est important de déterminer quelles données sont absolument nécessaires. Essayez de vous demander : Pourquoi ai-je besoin d'utiliser ces informations et sont-elles essentielles à mon programme ? Si vous n'êtes pas sûr ou si vous pensez pouvoir atteindre votre objectif avec d'autres données ou par d'autres moyens, envisagez de ne pas recueillir ces données. Nous avons une tendance à trop recueillir pensant que les données pourraient être utiles plus tard ou parce que nous recueillons toujours ces informations, ou nous en avons besoin pour notre base de données. La création d'une base de données n'est pas une raison recevable de recueil d'informations. Au contraire, chaque élément de données personnelles dans cette base de données doit y figurer pour une raison spécifique, bien définie et essentielle au programme.

Utilisation de modèles standard

Pour l'inscription, l'utilisation de modèles standard est très courante et utile car elle accélère le recueil de données, les types de données les plus courant ayant été identifiés. Cependant, ces modèles tendent à englober un éventail de données, car elles sont censées être un questionnaire à « taille unique ». Néanmoins en cas d'urgence, ces modèles peuvent être utilisés tels quels plutôt que d'être analysés pour des données utiles et essentielles dans le programme en cours de mise en œuvre. Recueillir des réponses à ces questions inutiles irait à l'encontre du principe de la minimisation et de la nécessité des données. Cela ne signifie pas que vous ne devez pas utiliser ces modèles. Prenez plutôt le temps de les analyser et de les adapter à chaque intervention. L'adaptation ne signifie pas recréer de nouveaux formulaires à chaque fois, mais plutôt

d'utiliser le même formulaire en omettant les questions inutiles (c'est-à-dire à ne pas poser verbalement). Dans les fichiers Excel, certaines colonnes ou lignes peuvent être masquées ; sur les modèles de format papier, certaines sections peuvent être rédigées ou rayées ; et dans le format numérique, les champs peuvent être marqués comme non obligatoires[4] ou masqués. Les membres de l'équipe qui effectuent le recueil de données devront être informés du principe de minimisation des données, afin de comprendre pourquoi certaines questions sont délibérément omises.

Exemple :

Dans le cadre d'un programme monétaire ciblant « les ménages qui ont perdu leurs moyens de subsistance ». Le jour de l'inscription, les bénéficiaires sont invités à renseigner le modèle standard publié par la Société nationale. L'équipe a analysé le modèle au préalable et a décidé que les ménages devraient répondre à toutes les questions du modèle relatives à leur situation économique. Cependant, l'équipe a effacé toutes les questions relatives à l'état de santé des différents membres de la famille. Ces informations ne seront pas fournies, car pour ce programme, les ménages recevront la même aide monétaire, quel que soit leur état de santé.

La Société nationale répond à une situation d'urgence due à la sécheresse. Elle a également mis en œuvre un grand programme de don de sang. Son équipe utilise alors un modèle standard qui comprend des questions liées au groupe sanguin des bénéficiaires. Étant donné que ces informations ne sont pas directement utiles pour l'intervention d'urgence en cas de sécheresse sur laquelle ils travaillent, ils ont décidé de ne pas demander ces informations aux bénéficiaires et les volontaires chargés du recueil de données ont été informés de la raison de cette décision. Autrement, on pourrait expliquer que les bénéficiaires pourraient éventuellement fournir des informations sur le groupe sanguin s'ils souhaitaient participer au travail de don de sang, mais qu'une telle participation n'affecterait aucun déboursement.

Les aspects suivants présentent les différents objectifs de recueil des données et les principales dispositions relatives à la protection des données :

[4] Notez ici une distinction entre les données dites « non requises » afin qu'elles n'aient pas à être posées au cas où la réponse à cette question serait nécessaire pour continuer dans un questionnaire numérique, et les données dites « facultatives » dans quel cas la question est toujours posée et il appartient à la personne interrogée d'y répondre ou non. Les questions facultatives doivent être réexaminées du point de vue de la protection des données. Premièrement, les informations qui ne sont pas nécessaires ne doivent pas être recueillies. Même si elles sont recueillies sur une base volontaire, le principe de la minimisation des données s'applique. Deuxièmement, les questions facultatives invitent toujours les interlocuteurs à donner cette information, ce qui peut laisser entendre que leurs chances d'obtenir de l'aide augmentent s'ils nous en disent davantage. Enfin, lorsque des informations sont données même si elles ne sont pas directement requises pour le projet, il faut se demander s'il existe une base légitime pour traiter ces données. Il convient également de rappeler qu'il doit être clairement expliqué aux bénéficiaires lorsque des informations dites « facultatives » sont demandées et qu'il convient de préciser que la communication de ces informations ne réduira aucunement leurs chances d'obtenir assistance.

Vérifier officiellement l'admissibilité des personnes

Bien que seuls les bénéficiaires admissibles soient invités à s'inscrire, il se peut que la vérification effectuée pendant le processus de ciblage n'ait pas été suffisamment officielle ou que la situation ait évolué, ce qui impose une nouvelle vérification d'admissibilité pendant le processus d'inscription. Dans ce cas, les données relatives aux critères de ciblage convenus devront être recueillies. Les dispositions à cet égard ont déjà été abordées dans le chapitre Ciblage. Ces dispositions s'appliquent au cours du processus d'inscription, en particulier la question de savoir si certaines informations auraient une incidence sur la décision de cibler ou non une personne. Si tel est le cas, ces informations peuvent être recueillies. Sinon, c'est inutile.

Dans les distributions générales exemptes de critères cibles précisés parce que les personnes touchées dans une zone ont toutes besoin d'assistance, le recueil de données d'admissibilité peut ne pas être nécessaire, sauf pour s'assurer qu'elles sont de la zone touchée ou pour établir une authentification pour obtenir l'aide. Dans ce cas, le processus d'inscription ne nécessite pas de poser des questions sur les indicateurs de vulnérabilité ou d'autres questions généralement utilisées pour établir l'admissibilité. Poser des questions pour recueillir des données démographiques typiques (par exemple, l'âge, le sexe, le nombre de membres du ménage) peut également ne pas être nécessaire, à moins qu'elles n'aient un objectif pertinent puisque ces données ne sont pas utilisées pour cibler les bénéficiaires.

Procéder à la distribution monétaire

Les données nécessaires pour permettre la distribution monétaire aux bénéficiaires dépendent de la méthode de distribution choisie. Pour les envois sous enveloppes, les données clés à recueillir peuvent être limitées aux informations d'identité et d'authentification de base à utiliser lors de la distribution. Lorsque vous utilisez des prestataires de services financiers (PSF), davantage de données peuvent être nécessaires, y compris les données de connaissance du client (KYC) requises par la loi pour que les PSF distribuent de l'argent. Les détails sur le recueil de données à utiliser par les PSF seront discutés plus en détail dans le chapitre suivant. Lors de l'inscription, il est important d'avoir un œil critique sur ce qui est nécessaire pour permettre la distribution monétaire (par exemple, les numéros de téléphone mobile pour recevoir de l'argent mobile).

Éviter la fraude et les doublons

Afin d'éviter la fraude et les doublons de paiements, il peut être nécessaire de recueillir des informations supplémentaires pour trianguler les informations de base sur les ménages. Par exemple, recueillir le nom, l'âge et le sexe de tous les membres du ménage et vérifier si l'un d'entre eux a tenté de s'enregistrer en tant que ménage séparé. En outre, pour les programmes qui dépendent de la taille du ménage pour déterminer le montant d'argent à débourser, une vérification détaillée des ménages peut s'avérer nécessaire (par exemple, avec des cartes familiales émises par le gouvernement). Dans ces cas, il est important de réfléchir au contexte réel pour évaluer le risque, puis de s'assurer que le recueil et le traitement des données sont adaptés au niveau de risque évalué, plutôt que de recueillir ces données de manière standardisée.

Exemple :

Un programme monétaire a été mis en place en réponse à une chaleur extrême provoquant des incendies dans un petit village. Le critère cible (ménages ayant perdu leur logement) englobe presque tous les ménages du village. Les noms des chefs de ces ménages sont indiqués et confirmés par les leaders communautaires. Le jour de l'inscription, les chefs de famille sont invités à s'identifier. L'équipe se prononce contre le recueil de données relatives aux membres de la famille. Le risque de fraude n'est pas très élevé, car la plupart des ménages recevront une assistance et les chefs de ces ménages ont été clairement identifiés et répertoriés en coopération avec la communauté. Par conséquent, il est peu probable que d'autres membres de la famille

ou des personnes d'autres villages puissent demander à tort de l'aide.

Un programme de transferts monétaires a été mis en place en réponse à l'insécurité alimentaire dans une petite communauté ciblant les ménages dirigés par des femmes. Le transfert monétaire est relatif à la taille du ménage pour répondre à ses besoins. L'équipe du programme décide de connaître le nombre de membres du ménage car il est nécessaire pour au calcul du transfert, mais il n'est probablement pas nécessaire de recueillir des informations supplémentaires sur les membres individuels de la famille. La communauté étant petite, il est peu probable que les gens essaieront d'indiquer des chiffres plus élevés pour la taille de leur ménage parce que d'autres membres de la communauté connaîtront et rapporteront probablement cet écart.

Le même programme monétaire a été déployé dans des communautés plus grandes et plus dispersées. Les transferts monétaires sont plus élevés en raison des ajustements au coût de la vie. Certains rapports faisaient état d'une taille excessive des ménages dans le cadre de programmes antérieurs gérés par d'autres ONG. L'analyse de l'équipe du programme a indiqué un risque élevé de fraude potentielle et décide de recueillir des informations supplémentaires sur les membres de la famille (nom, âge, sexe, lien de parenté ou affiliation au ménage). Des données supplémentaires ont servi pour vérifier les doublons dans la liste des bénéficiaires enregistrés.

Remarque : Pour les programmes qui utilisent l'auto-ciblage ou l'auto-inscription, où les bénéficiaires postulent sur la base de critères cibles publiés, il est important de noter que les données sont recueillies également pour ceux qui ne satisfont pas aux conditions d'admissibilité. Il est recommandé de s'assurer que lorsqu'il est évident que l'individu n'est pas admissible, ses données sont supprimées ou archivées pour empêcher les tentatives de réinscription (si nécessaire). Si une vérification supplémentaire s'avère nécessaire, stockez les données pendant une durée limitée jusqu'à ce que le processus de vérification soit terminé et, en cas d'inadmissibilité, informez le demandeur et supprimez ses données en conséquence. Voir le chapitre dispositions générales pour le stockage des données des non-bénéficiaires. Assurez-vous également que les critères cibles publiés sont pointus et détaillés pour limiter le nombre de candidats non admissibles.

Décision projet 3 : Que dire aux bénéficiaires au sujet du traitement de leurs données ?

Transparence

Décision de projet reformulée : Comment puis-je m'assurer que les bénéficiaires ont accès aux informations relatives au traitement de leurs données ?

Le principe de transparence de la protection des données signifie que les bénéficiaires en tant que personnes concernées doivent recevoir une communication claire sur les raisons pour lesquelles leurs données sont recueillies et la manière dont leurs données sont traitées. Cela englobe le but du recueil, du stockage, de la divulgation potentiel des données, des droits des bénéficiaires, etc. Informer le bénéficiaire de tout cela peut s'avérer difficile dans certains cas, en particulier dans les situations d'urgence où le temps est limité. En outre, si les besoins des bénéficiaires sont de nature urgente et plus importante que la

protection des données, ils peuvent se montrer moins intéressés par ces détails et moins prêts à comprendre leur sens. Néanmoins, ils ont droit à ces informations.

Une bonne approche consiste à donner aux bénéficiaires des **informations de base** et une **personne à contacter** s'ils souhaitent en savoir plus. Cela devrait faire partie intégrante du plan d'engagement communautaire et de redevabilité (CEA) du programme (voir le module M4_2 de la boîte à outils CiE). Des informations de base pourraient être fournies lors de la rencontre avec les communautés pour expliquer le programme et pourraient être réitérées pendant le processus d'inscription des bénéficiaires. Un avis général de confidentialité pourrait également être préparé, imprimé et partagé par la Société nationale avec les détails du programme (voir le modèle d'avis de confidentialité dans la section de référence). Les bénéficiaires peuvent consulter cette notice et, si nécessaire, contacter la Société nationale pour de plus amples renseignements s'ils en ont besoin. L'essentiel est que les bénéficiaires puissent joindre quelqu'un soit par ligne directe pour ceux qui ont accès au téléphone, soit en personne.

Lorsque l'on fournit des informations sur le traitement des données, il est utile de se mettre à la place des bénéficiaires et de se poser la question suivante : Quelles informations doit-on connaître avant de fournir mes données personnelles ? Les informations de base courantes sont répertoriées ci-dessous. Ces informations doivent être présentées clairement, d'une manière facile à comprendre et dans la ou les langues appropriées.

- **Objectif du recueil des données le jour de l'inscription.** Reportez-vous aux objectifs définis par votre programme, parmi les objectifs courants évoqués ci-dessus, citons la nécessité de prouver leur identité, de vérifier leur admissibilité, d'effectuer des distributions monétaires ou d'éviter la fraude et les doublons. Les bénéficiaires doivent connaître ces raisons et pourquoi certaines données sont nécessaires à ces fins ; cela les aide à comprendre la situation.
- **Si vous avez recueilli des données à leur sujet auprès d'autres parties** (par exemple, d'autres ONG, des dirigeants communautaires, des gouvernements). Très souvent, vous recevez des informations sur les bénéficiaires provenant d'autres sources avant de les contacter directement. Il est important que les bénéficiaires sachent d'où vous avez obtenu leurs informations personnelles, afin qu'ils puissent être sûrs que leurs données sont utilisées de manière responsable.
- **Comment faire corriger des données erronées.** Pour les bénéficiaires, il est rassurant de savoir qu'ils peuvent corriger des données erronées à tout moment. Des erreurs se produisent en particulier lorsque les interventions ont lieu dans la précipitation en cas d'urgence, à la fois de la part de l'équipe du programme chargée du recueil des données et du bénéficiaire fournissant les données préliminaires. Si les informations s'avèrent erronées, le bénéficiaire doit être en mesure de demander une correction.
- **Comment exprimer ses scrupules ou adresser une réclamation.** Les bénéficiaires doivent savoir qu'ils peuvent exprimer leurs préoccupations concernant le traitement de leurs données. Il est important pour eux de le savoir car cela leur procure une sensation de contrôle. Ils peuvent vouloir s'opposer au traitement des données ou se plaindre à ce sujet. Si tel est le cas, ils doivent savoir où aller et avec qui ils peuvent parler de leurs préoccupations et de leurs options. Cela devrait faire partie intégrante du mécanisme de réclamations et feedbacks du programme (voir le module M4_2_5 de la boîte à outils CiE).
- **Intention de diffuser des données.** Si vous savez que vous transmettrez les données recueillies avec d'autres groupes ou institutions (par exemple, d'autres ONG, PSF, gouvernement), le bénéficiaire doit en être informé ainsi que de la raison de la diffusion de ses données. Après tout, le bénéficiaire ne communique ces informations qu'à vous et vous fait confiance pour les garder en sécurité. Dans certains contextes, le bénéficiaire peut ne pas souhaiter que certains types d'informations soient partagés avec d'autres entités en raison de problèmes de sensibilité ou de sécurité. Il peut s'avérer utile de faire preuve d'une diligence raisonnable sur ces institutions afin de pouvoir communiquer leur fiabilité en termes de traitement des données des bénéficiaires. En outre, si les bénéficiaires détectent une mauvaise utilisation potentielle de leurs informations, communiquées à des entités

externes, ils devraient être encouragés à en informer la Société nationale via le service d'assistance ou un contact direct pour ces questions.

Outre les informations de base mentionnées ci-dessus, il serait bon de veiller à ce que des détails supplémentaires sur le traitement des données soient préparés au cas où les bénéficiaires poseraient davantage de questions. Les autres informations que les bénéficiaires devraient recevoir (selon le contexte) comprennent :

- Mode de stockage des données et mesures de sécurité
- Durée de conservation prévue des données
- Base légitime sur laquelle le traitement est fondé
- Toute information supplémentaire sur la finalité ou le traitement ultérieur
- Toute information supplémentaire sur la transmission de données
- Autres droits des personnes concernées qui peuvent s'appliquer, tels que le droit à l'effacement, à l'opposition et à l'accès à leurs données.

Décision projet 4 : Doit-on demander le consentement des bénéficiaires ?

Base légitime

Décision de projet reformulée : À quelle base légitime se fier ?

La question de savoir si vous devez demander à un bénéficiaire de consentir au recueil et à l'utilisation de ses données comporte plusieurs niveaux. Il est devenu courant de commencer les formulaires d'inscription des bénéficiaires par une question sur le consentement avant de continuer. À première vue, cela semble judicieux, car il est poli et respectueux d'obtenir sa permission. Toutefois, en vertu de la loi sur la protection des données, le traitement des données à caractère personnel peut être fondé sur d'autres motifs que le seul consentement, qui seront examinés plus en détail ci-dessous.

Mais ne vaut-il pas mieux demander son consentement ? Pas forcément. Cela peut sembler un signe de respect de demander au bénéficiaire d'accepter, mais cela comporte certains problèmes à prendre en compte.

Problèmes de consentement

Le consentement doit être donné librement et en toute connaissance de cause. Dans la pratique, cela signifie que le consentement n'est valable que lorsqu'il existe une réelle possibilité de refus, sinon il n'est pas vraiment « donné librement ». En cas d'urgence, l'obtention du consentement peut s'avérer impossible. Les bénéficiaires se trouvent dans une situation vulnérable et désespérée et ont besoin d'une aide immédiate. La protection des données n'est peut-être pas leur première préoccupation. Par conséquent, ils peuvent donner leur « consentement »[5] ne voyant aucune autre possibilité d'obtenir de l'aide. En effet, sans leurs données, vous ne pourrez pas les aider.

En outre, les bénéficiaires peuvent ne pas être en mesure de comprendre pleinement les conséquences de la communication de leurs données ou la manière dont celles-ci sont traitées (par exemple, via la technologie). Vous ne pouvez pas accepter pertinemment ce que vous ne comprenez pas (donc cela ne peut pas être considéré comme une « décision éclairée »).

Il faut également savoir que le consentement peut être retiré à tout moment et sans motif (s'il est librement donné, il peut aussi être librement repris). Une fois le consentement révoqué, tout traitement ultérieur des données personnelles concernées (qui a été effectué sur la base du consentement) est interdit. Cela peut devenir très problématique pour le programme, car il est important de disposer d'un ensemble de données fiable pour travailler. Une fois le consentement révoqué, il se peut qu'il ne soit plus possible de revenir en arrière pour utiliser une autre base légitime, telle que l'intérêt vital ou public. Pourquoi ? Leur droit de

rétractation est en effet sans valeur si par la suite rien ne change pour eux, et cela dépend également de la possibilité d'identifier une autre base légitime et des informations déjà communiquées au bénéficiaire. Pour toutes ces raisons, le consentement peut être problématique à utiliser comme base légitime. Pour le traitement des données à caractère personnel dans le cadre de programmes monétaires en cas d'urgence, il est recommandé d'envisager d'autres voies.

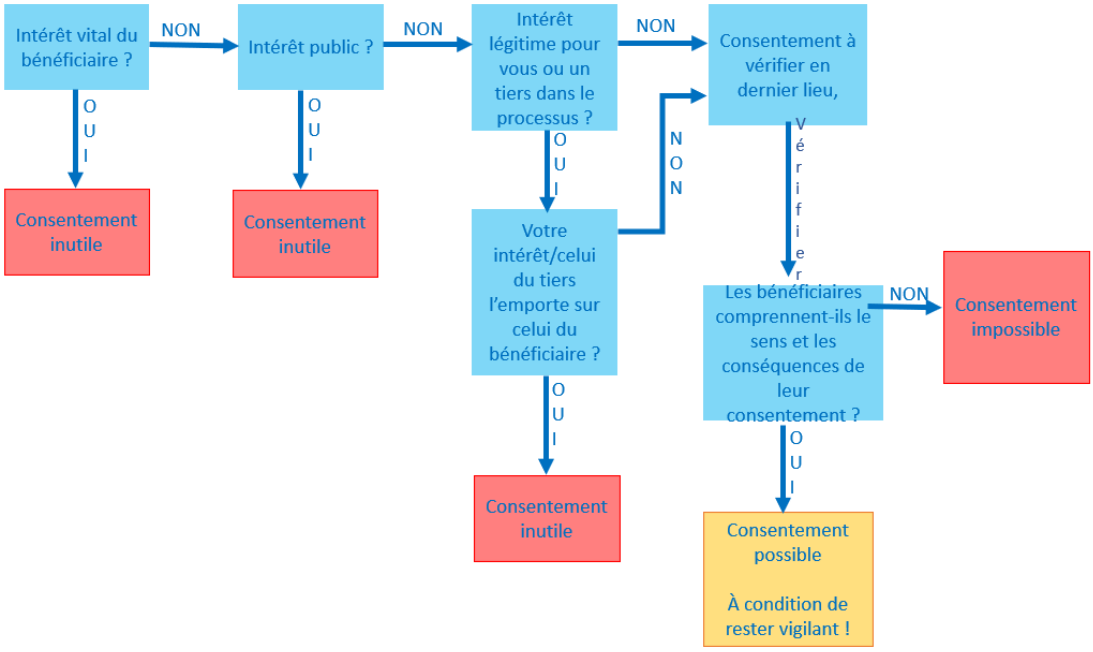

Figure 3 : Arbre de décision pour déterminer si le consentement est une base légitime adéquate

Autres possibilités

La figure 3 montre d'autres possibilités d'établir une base légitime. Deux d'entre elles sont l'intérêt vital et l'intérêt public. **L'intérêt vital** signifie que le traitement des données à caractère personnel est essentiel pour la vie, l'intégrité, la santé, la dignité ou la sécurité des bénéficiaires. Les programmes de TM conçus pour répondre à des besoins vitaux ou essentiels au début d'une situation d'urgence peuvent y être admissibles ; pour d'autres activités de TM dans un contexte non urgent, il faudra peut-être envisager d'autres options. **L'intérêt public** signifie que le traitement des données personnelles sert une finalité qui est dans l'intérêt de tous. Les Sociétés nationales qui fournissent une assistance exécutent un mandat humanitaire qui est dans l'intérêt général du public. Par conséquent, même lorsque la norme élevée d'intérêt vital n'est pas satisfaite, l'assistance par le biais des TM sera normalement toujours dans l'intérêt public[6].

[5] Le consentement est entre guillemets car si le bénéficiaire peut cocher une case ou indiquer d'une autre manière qu'il consent, il serait incorrect de dire qu'il serait légalement reconnu comme un consentement en vertu des lois et principes généraux de protection des données.

Pour éviter tout malentendu : C'est toujours aux bénéficiaires de décider s'ils veulent participer au programme ou non. Mais s'ils décident de le faire, il est possible d'utiliser leurs données personnelles sans leur demander explicitement leur consentement, à condition qu'ils soient informés du programme et de la manière dont leurs données seront utilisées. Ce qui est important, c'est que vous n'utilisiez que les données personnelles qui sont absolument nécessaires au programme. Voir également la section Programmes de transferts monétaires du Manuel sur la protection des données pour de plus amples renseignements sur les bases légitimes de TM.

Transmission de données

La divulgation de données avec d'autres entités (par exemple, d'autres ONG, le gouvernement, le PSF) peut être dans l'intérêt vital des bénéficiaires ou dans l'intérêt public. En outre, il peut exister des obligations légales de transmettre certaines données personnelles[7] et si tel est le cas, cela peut être fait sans consentement. En l'absence d'obligation légale, il peut être dans l'intérêt légitime de votre Société nationale de divulguer des données personnelles. Votre intérêt légitime peut justifier la transmission de données sans consentement si les bénéficiaires n'ont aucun intérêt supérieur et opposé. Il est essentiel d'examiner les conséquences ou les risques potentiels pour les bénéficiaires si les données sont divulguées. Ceci est expliqué plus en détail dans le chapitre sur la transmission des données. En bref, tout se résume à la nécessité et à la confidentialité.

Administration du programme

Certaines décisions de projet relatives au traitement des données peuvent ne pas être directement dans l'intérêt vital ou public mais restent raisonnables du point de vue du programme (par exemple, type de stockage, l'inclusion d'un plus grand nombre de membres de l'équipe, etc.). Là encore, l'intérêt légitime de votre Société nationale de structurer et d'organiser le programme de manière efficace entre en jeu.

Alors ?

Dans la plupart des cas, il n'est pas nécessaire d'obtenir le consentement. Cela ne veut pas dire que vos interventions sont moins justifiées, bien au contraire. Cependant, il y a deux autres aspects à prendre en compte :

[6] Veuillez noter que dans certaines juridictions, le fait de s'appuyer sur l'intérêt public peut nécessiter des considérations supplémentaires ou une approbation officielle du gouvernement. Il n'entre pas dans le cadre de ce guide de vérifier cela pour chaque juridiction. Si vous avez des doutes sur la possibilité d'invoquer l'intérêt public pour votre programme, n'hésitez pas à en parler à votre responsable ou à l'équipe juridique de votre Société nationale.

[7] Sachez que le respect d'une obligation légale est une base légitime généralement reconnue dans de nombreuses lois sur la protection des données.

- Ne pas demander le consentement ne signifie pas que vous n'avez pas à **éclairer les bénéficiaires** ! Quelle que soit la base légitime que vous souhaitez utiliser, le principe de transparence s'applique. Comme décrit dans la décision de projet 3, certaines informations de base concernant le traitement des données personnelles et un contact pour d'autres questions sont de bonnes normes.
- Vous pouvez envisager de modifier votre question de consentement pour « avez-vous des questions ou des préoccupations avant de continuer ? » ou « reconnaissez-vous avoir reçu des informations de base sur le programme, y compris où demander de plus amples renseignements sur la manière dont vos données seront traitées? » Ce n'est pas obligatoire mais pourrait être une autre façon de se montrer poli et respectueux avant de demander plus d'informations personnelles.
- Devez-vous évaluer la base légitime de chacune de vos interventions de TM ? Pas forcément. La plupart des interventions de TM peuvent se fonder sur la même base légitime, rappelez-vous simplement de ne pas utiliser le consentement par défaut. Si la nature d'un nouveau programme de TM est unique et que les répercussions sur les données des bénéficiaires ne sont pas claires, alors il serait judicieux d'évaluer officiellement la base légitime avant de continuer. Il est également recommandé de réaliser une analyse d'incidence sur la protection des données (DPIA) dans ce cas. Voir le chapitre sur les directives générales pour de plus amples renseignements à ce sujet.

V. Recours aux prestataires de services financiers

Usage de données personnelles

La distribution des transferts monétaires se fait généralement avec le soutien des prestataires de services et par conséquent, un contrat est établi avec eux. Pour les programmes de coupons, les fournisseurs peuvent être les marchands de produits de base, les vendeurs locaux, les supermarchés et les grossistes. Pour les programmes monétaires, il s'agit de prestataires de services financiers (PSF) tels que les banques, les opérateurs de réseaux mobiles ou les agents de transfert de fonds chargés de l'encaissement. Pour ce chapitre, nous nous concentrerons sur les PSF mais notons que les principes de protection des données doivent être pris en compte pour tous les types de prestataires de services. Le recours aux prestataires de services peut être examiné dans le module M4_3 de la boîte à outils CiE.

Dispositions relatives à la protection des données

Le recours aux PSF peut nécessiter la diffusion des données personnelles des bénéficiaires pour pouvoir distribuer de l'argent. Cette section examinera les décisions clés du projet lorsque vous travaillez avec les PSF et les dispositions liées à la protection des données. Les risques liés à la protection des données et aux PSF doivent être inclus dans la matrice des risques de TM de votre programme élaborée à partir des phases d'évaluation et d'analyse des réponses de votre programme. Voir Évaluation du module M2_4_3 et Analyse de la réponse du module M3_1_4 dans la boîte à outils CiE.

Décision projet 1 : Doit-on faire appel à un prestataire de services financiers ?

Minimisation, nécessité et sécurité des données

Décision de projet reformulée : Le PSF pourrait-il utiliser les données des bénéficiaires d'une manière qui serait préjudiciable à ces derniers ?

Lorsque vous envisagez de faire appel à un PSF dans votre projet, il est important d'analyser les données dont le PSF aura besoin pour assurer son service, ce qui peut impliquer de demander des informations supplémentaires aux bénéficiaires à cette fin, et d'évaluer soigneusement les conséquences potentielles pour les bénéficiaires lorsque ces données sont divulguées.[8]

Connaissance client (KYC) et filtrage de la liste de surveillance

De nombreux PSF sont soumis à la réglementation KYC, qui les oblige à recueillir des informations sur leurs clients afin de prévenir le blanchiment d'argent, le financement du terrorisme ou d'autres crimes. La quantité d'informations requises pourrait dépendre des réglementations locales, certains pays autorisant une plus grande flexibilité en fonction de ce qu'ils considèrent comme le niveau de risque associé aux transactions. Les agences humanitaires faisant appel à des PSF devront se conformer à ces réglementations KYC exigeant de divulguer certaines données des bénéficiaires.

Quelques dispositions pour garantir le respect du principe de minimisation et de nécessité :

- Examinez les réglementations KYC dans votre pays et votre contexte opérationnel. Déterminez quelles données sont requises par la loi et comparez-les à ce que demande le PSF. Des politiques internes peuvent expliquer pourquoi les PSF demandent des données supplémentaires hors de ce qui est requis par la loi; cela doit être justifié et négocié pour garantir que seul ce qui est strictement nécessaire pour apporter assistance soit divulgué.
- Dans certains cas, les organisations humanitaires pourraient plaider en faveur d'une simplification ou d'un ajustement des exigences en matière de KYC (par exemple, en réduisant les exigences pour les personnes ayant perdu leur carte d'identité, en plafonnant les montants pouvant être transférés aux bénéficiaires ou aux tiers pour le KYC, ou en autorisant les transferts en espèces pour une durée limitée). Vérifiez si, dans ces cas, les données transmises aux PSF pourraient être réduites au minimum.
- Informez les bénéficiaires et expliquez les exigences KYC ou au minimum indiquez ces exigences dans l'avis de confidentialité qui peut être consultée à tout moment.

Les PSF peuvent être tenus de vérifier les informations KYC et de divulguer des données avec des tiers (tels que les régulateurs et les autorités publiques). Ces contrôles KYC peuvent comporter la comparaison de la liste des bénéficiaires aux listes de surveillance, aux listes de sanctions ou aux listes de personnes désignées par les autorités locales qui pourraient être impliquées dans un conflit ou des violences. Certains PSF font systématiquement cette comparaison tandis que d'autres la font à la demande du gouvernement. Ce processus permet de repérer les personnes qui pourraient être soupçonnées d'être impliquées dans certaines activités criminelles (blanchiment d'argent, terrorisme, corruption, etc.) et qui ne sont donc pas admissibles à recevoir de l'argent liquide. Si le nom d'un bénéficiaire correspond à l'une de ces listes, cela peut avoir de graves conséquences pour lui. Il est donc crucial d'analyser le contexte du pays et du programme. Les questions typiques auxquelles il faut réfléchir sont :

[8] Vous trouverez un modèle de questionnaire pour PSF en section de référence de ce guide.

- Y a-t-il des rapports de persécution politique, ethnique ou religieuse par le gouvernement ?
- Certaines parties de la population bénéficiaire sont-elles considérées comme des opposants au régime ?
- Les partis politiques peuvent-ils être considérés comme des groupes terroristes ?
- Le PSF est-il étroitement lié aux autorités de l'État, telles que les services de renseignement ou les agences de sécurité ?
- Si les bénéficiaires sont des réfugiés, le PSF dispose-t-il d'une succursale ou d'un entrepôt dans le pays d'origine des réfugiés où des données pourraient être demandées par les autorités ?
- Les bénéficiaires auraient-ils de sérieuses inquiétudes ou craintes si leurs données étaient en quelque sorte échangées avec le gouvernement en raison de ces obligations ?

Si vous pensez que les données des bénéficiaires pourraient être utilisées de manière inadéquate, cela présente un risque grave pour les bénéficiaires. Dans ces circonstances, si vous ne trouvez pas moyen de contracter un PSF sans partager les données des bénéficiaires, d'autres modes de distribution, telles que l'argent liquide dans des enveloppes, des bons ou même en nature, doivent être envisagées. Cela devrait être fait dans le cadre de l'évaluation des risques pendant la phase de réponse et d'analyse de votre programme (module 3 de la boîte à outils CiE) et devrait comporter une analyse pour savoir si la persécution, l'exclusion ou d'autres sensibilités pourraient entraîner le recueil et la divulgation d'informations de KYC lors du choix de la meilleure modalité de transfert. Autres références du CaLP : Normes de Connaissances du client et recommandations de confidentialité des transferts monétaires et fiche d'astuces de réglementations KYC.

Autres objectifs

Étant donné que les PSF sont généralement des sociétés à but lucratif, ils peuvent utiliser les données des bénéficiaires à leurs propres fins, y compris les intérêts commerciaux, tels que le profilage de solvabilité, la publicité ou le marketing, et la vérification de l'admissibilité à d'autres services financiers. De tels exemples peuvent sembler relativement peu risqués pour les bénéficiaires, mais ils sont toujours considérés comme hors du but de l'aide humanitaire monétaire. La loi sur la protection des données vise également à protéger les personnes contre les actions non sollicitées des institutions privées telles que le pollupostage (spams).

Une autre incidence potentiellement plus importante de la réutilisation des données par le PSF pourrait être la compensation de dette (par exemple, le bénéficiaire doit un prêt ou de l'argent à la banque et la banque essaie de déduire son aide monétaire pour le remboursement de la dette) ou une divulgation supplémentaire des données à des tiers, comme les agents de recouvrement.

En général, une diligence raisonnable sur la réputation et les performances des PSF doit être effectuée pendant le processus d'appel d'offres ou de passation de marchés.[9] En outre, les contrats avec les PSF doivent restreindre le traitement ultérieur des données (pendant et même après la distribution monétaire), et comporter des exemples d'actions à éviter, si ceux-ci sont connus au moment de la passation de marché (voir décision de projet 3). Au cours de la mise en œuvre du programme, les bénéficiaires devraient être invités/invités à signaler à la Société nationale tout cas d'utilisation ultérieure (ou soupçonnée d'utilisation abusive) de leurs données par des PSF qui ne font pas partie du programme.

[9] Vous trouverez un modèle de questionnaire pour PSF en section de référence de ce guide.

Décision projet 2 : Quel type de compte choisir pour la distribution en espèces ?

Minimisation, nécessité et sécurité des données

Décision de projet reformulée : Quel type de compte utiliser pour la distribution monétaire protège le mieux les données des bénéficiaires ?

Il existe différents mécanismes de paiement en espèces à envisager, notamment le recours aux agences de transfert de fonds, aux fournisseurs de réseaux mobiles et aux bureaux de poste. Du point de vue de la protection des données, il est important de tenir compte, quelle que soit l'option de mécanisme de paiement choisie, comment limiter la divulgation des données personnelles. Cela pourrait essentiellement dépendre du type de compte utilisé pour la distribution monétaire. Envisagez deux types de comptes : en utilisant des comptes nommés pour des bénéficiaires individuels ou en ayant un compte virtuel géré par la Société nationale.

Comptes nominatifs

Le programme peut choisir d'utiliser directement le compte du bénéficiaire auprès du prestataire de services financiers ou d'ouvrir un compte à son nom. L'utilisation de comptes préexistants des bénéficiaires interfère moins avec la protection des données que l'ouverture de nouveaux comptes car le PSF et le bénéficiaire ont déjà une relation contractuelle que votre Société nationale exploite aux fins du programme. La création de nouveaux comptes par la Société nationale pour les bénéficiaires individuels, à supposer que cela soit réalisable, devrait être analysée plus en détail afin de déterminer les risques potentiels en matière de protection des données. Par exemple, il peut y avoir une raison spécifique pour laquelle le bénéficiaire n'a pas ouvert son propre compte individuel (par exemple, en raison de certains problèmes de connaissance du client mentionnés en section précédente). L'ouverture d'un compte au nom d'une autre personne nécessite une attention particulière dans le recueil et la divulgation des données avec le PSF, ainsi que dans la gestion de ce compte après le programme.

Comptes virtuels

Les comptes virtuels sont détenus et gérés par l'organisation humanitaire, qui peut créer des sous-comptes pour les bénéficiaires afin de leur permettre de recevoir de l'argent. Avec de tels comptes, le KYC est effectué avec l'organisation et non avec les bénéficiaires individuels. Exemples d'utilisation de comptes virtuels :

- Délivrer des cartes prépayées pour distributeurs automatiques de billets, chaque carte étant liée au compte de la Société nationale et remise aux personnes éligibles avec un code PIN pouvant être utilisé pour retirer de l'argent
- Émettre des chèques bancaires à des particuliers qui pourraient être échangés, qu'ils soient ou non titulaires d'un compte dans cette banque
- Une carte SIM mobile à usage limité émis par l'organisation afin que les bénéficiaires puissent recevoir un SMS avec des codes transactionnels qui pourraient être utilisés pour échanger de l'argent auprès des agents d'argent mobile

Il peut être nécessaire de partager les données du bénéficiaire avec le PSF à des fins d'identification au moment du versement des fonds, mais la quantité de données à communiquer au PSF est généralement réduite par rapport à la création de comptes nommés car la connaissance client n'est pas établie avec les individus. Du point de vue de la protection des données, cette voie est intéressante, mais il y a aussi des dispositions opérationnelles (par exemple, la capacité de l'équipe du programme à gérer les sous-comptes, la distribution de jetons tels que les cartes prépayées pour recueillir de l'argent aux bonnes personnes et lier les bons numéros de sous-comptes et rapprochement des transactions après déboursement). Les

risques liés à la gestion des transactions et des fonds incombent principalement à l'agence. En outre, dans le cas du recours aux comptes virtuels, la SN a accès à des données révélant comment les bénéficiaires dépensent leur argent. Ces données sont sensibles. Afin de respecter la vie privée des bénéficiaires à cet égard, reportez-vous au chapitre sur le suivi post-distribution pour de plus amples renseignements sur la confidentialité et le suivi.

Décision projet 3 : Que doit comporter le contrat avec un PSF ?

Sécurité des données

Décision de projet reformulée : Quelles dispositions doit-on inscrire dans un contrat avec le PSF pour protéger les données personnelles des bénéficiaires ?

Premièrement, il est important de déterminer quelles données sont absolument indispensables pour exécuter le service du PSF et de négocier pour minimiser la divulgation de données. Cela comprend généralement :

- Données d'identification telles que le nom du bénéficiaire et un numéro d'identification valide
- Les données requises par KYC, qui peuvent varier en fonction des réglementations nationales
- Et d'autres données, le cas échéant, nécessaires pour permettre la distribution de l'argent, telles que : Le numéro de téléphone mobile pour le transfert d'argent mobile, le numéro de compte bancaire ou le nom et la pièce d'identité de la personne autorisée à recevoir de l'argent au nom du bénéficiaire (par procuration)

Il est également important de comprendre quelles données pourraient être créées par le PSF et vous être communiquées dans le cadre des transactions effectuées avec les bénéficiaires. Par exemple, la date et l'état de l'encaissement, la signature du bénéficiaire après avoir reçu de l'argent, le solde actuel si tout l'argent n'a pas encore été retiré du compte, où l'argent aurait pu être dépensé (par exemple, épicerie), etc.

Deuxièmement, un contrat ou un accord de service devra être passé. Il doit indiquer le cadre de la prestation de service, la portée et les éléments de protection des données. Il est recommandé de préparer et de partager un modèle pour cet accord dans le cadre du processus d'appel d'offres et d'évaluer les dispositions relatives à la protection des données dans le cadre du choix du fournisseur.

Certaines des principales dispositions à inclure dans le contrat :

- **Limitation de la finalité.** Les données divulguées ne seront utilisées que dans le cadre du programme (distribution d'argent). Toute autre utilisation hors du cadre du programme ne sera pas autorisée. Comme mentionné ci-dessus, il peut également être utile d'être explicite ou d'énumérer concrètement les exemples pour lesquels les données ne doivent pas être utilisées (par exemple, la publicité et le marketing, la compensation de la dette). La liste doit porter la mention « non exhaustive ».
- **Divulgation de données à des tiers.** Le PSF ne divulguera pas les données à des tiers si cela n'est pas approuvé par la Société nationale. En outre, en cas d'obligation de divulgation (par exemple, avec les autorités), la Société nationale doit en être informée en premier lieu.
- **Sécurité des données.** Les données divulguées doivent être stockées en toute sécurité (par exemple, avec indication des contrôles d'accès, cryptage, processus de sauvegarde).
- **Confidentialité.** Elles seront traitées de manière confidentielle.
- **Aucun recueil de données supplémentaire auprès du bénéficiaire.** Le PSF ne doit pas recueillir d'autres données personnelles auprès du bénéficiaire dans le cadre du programme. Par exemple, les bénéficiaires peuvent avoir besoin de montrer leur pièce d'identité lors de la demande d'aide monétaire, mais le PSF ne doit pas copier ni scanner la

pièce d'identité et ainsi recueillir des données supplémentaires sur le bénéficiaire.

- **Suppression.** Les données transmise seront supprimées des bases de données PSF à la fin du programme ou archivées hors ligne et en toute sécurité à des fins d'audit.
- **Conséquences d'une infraction par le PSF.** Le contrat doit contenir un libellé indiquant que le PSF reconnaît qu'une violation de ces conditions peut avoir des conséquences judiciaires, mais à tout le moins nuire à la réputation de toutes les parties concernées. Indiquer que les bénéficiaires sont encouragés à informer la Société nationale de toute utilisation non liée au programme de leurs données personnelles par le PSF.

Veuillez consulter la section des références ci-dessous pour un modèle type de la FICR pour la passation de marchés avec les PSF. Il comporte les aspects importants de protection des données. Si vous sentez qu'il manque quelque chose ou que vous souhaitez résoudre un problème spécifique qui est survenu dans le contexte de votre programme, vous pouvez ajouter ces aspects dans votre propre modèle.

Dans la pratique, le PSF souhaite souvent utiliser son propre modèle de contrat. En fonction de votre position de négociation, essayez de négocier en utilisant le modèle préparé par votre Société nationale. Si vous optez pour le modèle du PSF, il est conseillé d'examiner de plus près et de comparer les éléments de protection des données et de demander qu'ils soient modifiés pour garantir une protection renforcée des données de vos bénéficiaires. Si le modèle du PSF ne contient aucune information sur la protection des données, c'est votre opportunité d'introduire les aspects de la protection des données que vous jugez importants. Vous pouvez extraire certaines clauses du modèle de la FICR. Si le PSF ne souhaite accepter aucun libellé sur la protection des données dans le contrat, cela devrait être un signal d'alarme en termes de collaboration avec ce fournisseur. Toute entité réputée devrait s'intéresser à un niveau minimal de protection des données.

Il est courant de négocier un accord-cadre avec un ou plusieurs PSF dans le cadre de la préparation des liquidités afin que vous ayez des options en fonction du contexte et des besoins. Cependant, de nouveaux programmes peuvent entrer dans de nouvelles situations qui ne font pas partie de l'accord actuel avec le PSF. Si vous avez l'impression que la protection des données n'a pas été suffisamment prise en compte dans le contrat-cadre, n'hésitez pas à en faire part au PSF ou à votre responsable pour tenter de négocier un amendement. La protection des données est devenue de plus en plus importante au cours des dernières années et la sensibilisation ne fait que commencer.

VI. Divulgation de données au gouvernement, aux autres organisations humanitaires et aux donateurs

Usage de données personnelles

Les interventions de TM nécessitent une coopération et une coordination avec des acteurs plus grands tels que le gouvernement national, d'autres organisations humanitaires (internationales et nationales) et les donateurs. Dans ces relations, il est possible que les données sur les bénéficiaires d'une Société nationale doivent être divulguées à l'extérieur (et la Société nationale peut également recevoir des données). La divulgation peut se faire officiellement via des accords de transmission de données ou de manière officieuse sans accords définis, en particulier dans les situations d'urgence où la ponctualité est essentielle.

Dans le chapitre sur le ciblage, nous avons vu des exemples de réception de données sur les bénéficiaires du gouvernement et d'autres organisations répondant à la même urgence pour établir une liste préliminaire des bénéficiaires et pour vérifier l'admissibilité de ceux qui figurent sur la liste. Ce niveau de divulgation des données est également important pour la coordination entre les différents acteurs afin d'éviter des doublons coûteux des efforts et de l'assistance. Pour les donateurs, il pourrait y avoir des obligations d'audit et de démonstration de transparence et de responsabilité en s'assurant que les bénéficiaires qui ont reçu une assistance sont de vraies personnes, qu'ils sont effectivement admissibles et qu'ils ont bien reçu l'argent

auquel ils ont droit.

Dispositions relatives à la protection des données

Dans cette section, nous examinerons les principales dispositions relatives à la protection des données lors de leur transmission à des tiers. En général, lors de la divulgation de données avec différentes parties, **il est important de s'assurer que les données sont transférées en toute sécurité via des moyens sécurisés** (par exemple, des fichiers cryptés, stockés dans des salles de données sécurisées) et accessibles uniquement par le personnel autorisé. Voir le chapitre du guide général.

Lorsque des données sont transférées vers d'autres pays, il est essentiel d'évaluer le niveau de protection des données dans ce pays. S'il est inférieur à la norme de la SN, la transmission doit être réétudiée et, si inévitable, un accord de transmission de données solide et détaillé sur les exigences en matière de protection des données doit être négocié.

Décision projet 1 : Quelles données sont à communiquer au gouvernement ?

Sécurité et nécessité des données

Décision de projet reformulée : Est-il nécessaire et sûr de divulguer des données personnelles au gouvernement ?

Les Sociétés nationales, bien qu'elles agissent en tant qu'auxiliaires du gouvernement de leur pays, ont le devoir de maintenir leur nature de neutralité, d'impartialité et d'indépendance lorsqu'il s'agit d'action humanitaire. Cependant, elles sont également soumises aux lois nationales[10] qui peuvent prévoir des obligations légales et donc l'obligation de partager certaines données avec le gouvernement. Certains des risques liés à la protection des données ont été abordés en section connaissance du client (relative à l'utilisation des PSF) en termes de signalement des personnes désignées aux autorités (listes de surveillance, listes de sanctions). Il pourrait également y avoir des risques que la Société nationale subisse des pressions de la part des autorités pour divulguer des données personnelles à d'autres fins (par exemple, la lutte contre le terrorisme). Par conséquent, une analyse est nécessaire lors de la conception de l'intervention TM, bien avant le recueil des données, et noter ces risques (en utilisant une matrice de risque ou une analyse plus structurée utilisant une DPIA).

Outre les lois nationales spécifiques, il existe d'autres finalités pour lesquelles des données peuvent être demandées par le gouvernement à l'organisation :

[10] Ceux qui ont des privilèges et immunités font exception.

- **Comprendre l'intervention des TM.** Le gouvernement souhaite souvent être informé des programmes humanitaires organisés dans sa juridiction, car il est responsable en dernier lieu de la sécurité et du bien-être des citoyens et des habitants de leur région. En outre, en cas de désaccords entre certains membres de la communauté sur les raisons pour lesquelles ils ne sont pas inclus dans le programme, ils déposent leurs plaintes auprès des autorités. En règle générale, les autorités souhaitent comprendre l'objectif, la durée, les groupes cibles et les critères de ciblage convenus, l'échelle financière, les exigences en matière de sécurité, les ressources et le soutien dont ils ont besoin. Pour que le gouvernement cerne mieux programme, il suffit normalement de fournir des informations générales et des données agrégées (critères cibles, zones, nombre de personnes soutenues, pourcentage de personnes âgées/enfants, montant de la subvention monétaire, etc.). Dans certains cas, ils pourraient être intéressés par la liste finale des bénéficiaires qui ont été ciblés. Si cette liste n'est pas déjà rendue publique par le biais de la communication et de la sensibilisation de la communauté, il est bon de comprendre pourquoi les autorités peuvent avoir besoin d'une telle liste et une négociation peut être nécessaire pour limiter les données personnelles transmises.
- **Coordination pour éviter la duplication de l'assistance.** En cas d'urgence, le gouvernement a normalement également des programmes pour soutenir les communautés touchées. Si différentes agences apportent une assistance, les gouvernements peuvent prendre en charge la coordination pour s'assurer de l'absence de doublons des agences d'assistance et de soutien afin de fournir l'aide le plus rapidement possible. Dans certains pays et contextes, le gouvernement peut demander des données sur les bénéficiaires à toutes les organisations pour vérifier l'absence de doublons, et dans certains cas, il peut même avoir besoin de valider la liste avant que l'organisation puisse procéder à la distribution. L'intention d'éviter les doublons peut être raisonnable et nécessite que le gouvernement se renseigne sur les noms des bénéficiaires. Cependant, il est inutile de divulguer d'autres données personnelles à cette fin. En outre, il n'est généralement pas nécessaire d'accorder au gouvernement l'accès à votre base de données. Dans la mesure du possible, négociez pour minimiser les données à divulguer avec les autorités afin de faciliter la coordination et les contrôles de doublons.
- **Partenariat de mise en œuvre.** La Société nationale pourrait être en partenariat avec le gouvernement pour la distribution au nom du gouvernement. Il s'agit de programmes de protection sociale et de grandes distributions pour lesquels le gouvernement peut compter sur la portée et la capacité de la Société nationale. Dans de tels partenariats, un accord officiel se noue généralement. Lors de la négociation de tels accords, veuillez garder à l'esprit les principes de protection des données et les meilleures pratiques.

Quelle que soit la finalité officielle, il convient de garder à l'esprit deux problèmes potentiels. Premièrement, dans certains contextes, il est concevable que les données personnelles, une fois divulguées, puissent être réutilisées à d'autres fins. Deuxièmement, même lorsque vous ne divulguez qu'une quantité très limitée de données personnelles, ces données peuvent éventuellement être combinées avec d'autres données que le gouvernement détient d'ores et déjà. Les conséquences possibles pour les bénéficiaires sont difficiles à prévoir. Pour atténuer ces deux risques, il peut être envisagé de ne présenter qu'une copie papier de la liste des bénéficiaires. Les données non numérisées sont plus difficiles à réutiliser. Mieux encore, n'afficher la liste que lors d'une réunion et ramener immédiatement la copie papier avec vous. Cela dépend du contexte si le gouvernement acceptera une telle approche, mais l'idée ici est d'essayer des options pour minimiser la divulgation de données.

Lorsque des données personnelles doivent être fournies au gouvernement, rappelez-vous :

- Être clair sur la finalité de la divulgation des données et les conséquences ou risques potentiels pour les bénéficiaires ; atténuez-les si possible et identifier une base légitime.
- Établir un accord de partage des données, si possible. Cet accord définira formellement l'objectif du partage des données personnelles et limitera l'utilisation des données à cet objectif précis. Il exige également que le destinataire conserve les données personnelles en toute sécurité et ne les stocke pas plus longtemps que nécessaire. Reportez-vous au modèle PSF de la FICR[11] pour obtenir un guide général. La Société nationale a un rôle auxiliaire du gouvernement, qui pourrait être important dans la négociation d'accords de divulgation de données.
- Informer les bénéficiaires que les données seront partagées avec le gouvernement et expliquer pourquoi. Préciser également avec quelles unités gouvernementales les données seront principalement partagées. Cela peut dissuader certains bénéficiaires de partager leurs données et doit être abordé par le programme.

Décision projet 2 : Quelles données sont à communiquer à d'autres ONG ?

Minimisation, nécessité et sécurité des données

Décision de projet reformulée : Est-il nécessaire de partager des données personnelles avec les autres ONG et cela peut-il être fait de manière sûre/sécurisée ?

La divulgation d'informations à d'autres ONG peut être nécessaire dans certains contextes. Voici quelques exemples et les principales dispositions relatives à la protection des données, qui devraient inclure les questions suivantes :

- Est-il dans l'intérêt des bénéficiaires de divulguer leurs données ?
- Exposerait-il les bénéficiaires à un risque ?
- Puis-je m'assurer que les données restent confidentielles et ne seront pas divulguées avec d'autres sans mon approbation ?
- L'autre organisation dispose-t-elle de normes de protection des données suffisantes ?

En tout état de cause, divulguer plus que des noms et des coordonnées sera problématique. Les indicateurs de vulnérabilité ont tendance à être très privés et, lorsque cela est possible, les bénéficiaires devraient eux-mêmes avoir la possibilité de décider à qui ils souhaitent divulguer ces données.

Au sujet de la coordination. La divulgation des données joue un rôle lorsque plusieurs acteurs humanitaires fournissent simultanément une assistance en matière de TM et il est nécessaire de travailler de manière coordonnée (par exemple, des groupes de travail monétaire locaux). Avec différents programmes exécutés simultanément, il est important d'éviter les doublons et de s'assurer que les actions des différents acteurs ne causent pas de dommages. Certains efforts de coordination visent à harmoniser les montants des subventions monétaires, les critères de ciblage et les approches. Malgré ces intentions raisonnables, il convient de garder un œil critique et de se demander s'il est vraiment nécessaire de divulguer des données personnelles, et dans quelle mesure, afin de coordonner le travail. C'est souvent une bonne alternative de divulguer des informations générales et des données agrégées (critères cibles, zones géographiques ciblées, nombre de personnes assistées, pourcentage de personnes âgées ou d'enfants, montant de l'aide

[11] Le modèle de contrat avec le PSF se trouve dans la section de référence de ce guide.

monétaire, etc.). Même lorsque le but est d'éviter les doublons, il n'est pas systématiquement nécessaire de comparer les listes de bénéficiaires. Selon le contexte, les doublons peuvent être évités en attribuant différents domaines d'activité (village A village B) ou différents groupes cibles (femmes enceintes / personnes âgées). Si vous concluez que la transmission de données des bénéficiaires est inévitable, la protection des données vous obligera à limiter au minimum la quantité de données divulguées. Par exemple, il pourrait être suffisant de comparer les listes de bénéficiaires sur papier lors d'une réunion commune avec les autres ONG. Cela est moins risqué que de donner à d'autres ONG l'accès à votre base de données ou d'envoyer des listes par courrier électronique.

Tirer parti de l'expertise et de la portée au sein d'une communauté. Dans certaines situations, une ONG peut être dotée de connaissances spécialisées d'un secteur ou de certains groupes au sein d'une communauté (par exemple, les groupes ciblant les femmes et les enfants vulnérables). Dans ce cas, une Société nationale peut avoir besoin de coopérer avec une telle ONG pour bénéficier de son expertise ou de ses connaissances de la communauté. Il est fréquent que d'autres ONG comptent sur la Société nationale locale en raison de sa présence à la base dans de nombreuses communautés et parfois du seul acteur humanitaire présent sur place.

Il peut également y avoir des situations où une autre ONG souhaite mettre en place son propre projet sur la base de votre ensemble de données préexistant sur les bénéficiaires. Cela est pratique et permet d'accélérer le recueil de données. Cependant, cela signifie une utilisation ultérieure des données personnelles qui peuvent être incompatibles avec l'objectif initial du recueil de données. Même si cela semble plus pratique du point de vue des bénéficiaires, car ils peuvent recevoir plus d'aide, la divulgation des données reste ici une exception, et non une règle, et il convient d'être prudent.

Partenariat d'implémentation. La divulgation de données est également important dans les partenariats d'implémentation dans quel cas une organisation peut être engagée pour assurer une aide / des services au nom d'une autre organisation ou pour divulguer les responsabilités dans l'implémentation des TM. Par exemple, l'agence des Nations Unies pour les réfugiés travaillant avec plusieurs ONG fournissant des services aux réfugiés. Dans le cadre de tels partenariats, la divulgation de données est normalement négociée et fait partie intégrante d'un contrat ou d'un accord. Lors de la conduite de telles négociations, il est important d'évaluer les risques pour les bénéficiaires lorsque les données sont divulguées et traitées par les partenaires, ainsi que les rôles et responsabilités des partenaires et les responsabilités partagées en matière de protection des données. Il est possible que l'agence chef de file dicte les normes de protection des données, mais si votre évaluation des risques trouve des lacunes ou si vous pensez que certaines dispositions doivent être renforcées, n'hésitez pas à les communiquer à votre responsable et/ou à l'équipe juridique au sein de votre Société nationale, afin qu'ils puissent être abordés dans le processus de négociation. Par exemple, si votre Société nationale recueille des données auprès des bénéficiaires, devez-vous transmettre toutes ces données au chef de file ou pouvez-vous réduire les données à ce qui est essentiel pour assumer vos responsabilités dans le partenariat ? Si vous avez des programmes TM parallèles ciblant les mêmes bénéficiaires dans le cadre de l'accord de partenariat d'implémentation, comment garantissez-vous la séparation de l'accès des partenaires pour les aspects hors du champ d'application de l'accord ?

Plateforme commune. Il existe certaines initiatives visant à développer une plateforme commune en termes de partage des données des bénéficiaires et potentiellement d'utilisation du même mécanisme de paiement par plusieurs organisations participantes. Cela peut impliquer d'avoir une base de données ou un mécanisme d'interopérabilité des systèmes de données appartenant aux agences pour divulguer et exposer l'ensemble convenu de données au sujet des bénéficiaires. Une telle plate-forme vise à améliorer la coordination et la collaboration entre les acteurs humanitaires et peut être soutenue par certains donateurs car elle peut améliorer l'efficacité. Il existe différentes approches pour avoir de telles plates-formes communes et la Société nationale devrait à nouveau évaluer les besoins et les risques pour les bénéficiaires

en priorité par rapport aux gains d'efficacité des organisations. Quelques questions à se poser :

- Une telle plate-forme est-elle absolument nécessaire pour que la Société nationale fournisse une aide monétaire ? Il existe différentes manières de coordonner et de collaborer avec d'autres ONG qui ne nécessitent pas d'accès direct aux données des bénéficiaires.
- Quelles données sont nécessaires pour participer à la plate-forme commune et peuvent-elles être réduites au minimum ?
- Comment les bénéficiaires doivent-ils être informés lorsque leurs données sont utilisées par d'autres agences ? Qui devrait les en informer ?
- Une fois les données diffusées via la plate-forme commune (c'est-à-dire quand les autres agences ont accès à vos données), comment les partenaires s'assurent-ils que les données sont utilisées aux fins convenues ?
- Quelles sont les fonctionnalités de sécurité de la plate-forme pour garantir que seul le personnel agréé peut accéder aux données ?
- Quel serait le contrôle de l'accès aux données par les différentes ONG ? Plus les ONG participent, plus le travail devient généralement difficile à gérer. En particulier, lorsqu'une organisation décide de cesser de participer à la plate-forme commune, comment les données divulguées seraient-elles utilisées à l'avenir ?
- Où les données seront-elles stockées et cette localité (par exemple, hors du pays cible) soulève-t-elle des problèmes de conformité en matière de protection des données ?

Si la décision est de divulguer des données personnelles avec d'autres ONG, il est tout d'abord important d'avoir en place un accord. La base légitime du traitement doit être identifiée. Lorsque la diffusion des données a lieu via une plate-forme commune, cet accord doit être encore plus solide, avec des normes de protection des données solides, la portée et les rôles et responsabilités des partenaires participants définis. Il est recommandé d'impliquer des experts en informatique et des experts juridiques dans la négociation de l'accord pour une plate-forme commune afin de garantir un niveau de protection suffisant. Deuxièmement, les bénéficiaires doivent être prévenus que les données seront transmises à d'autres agences. Si la transmission de données n'était pas prévue au moment du recueil ou de l'inscription, il vous sera difficile d'en informer chaque individu. Dans ce cas, il incombe normalement à l'autre ONG utilisant les données que vous avez divulguées pour informer ces bénéficiaires. Il est conseillé de le préciser dans l'accord de transmission de données.

Décision projet 3 : Quelles sont les données à communiquer aux donateurs ?

Minimisation, nécessité et sécurité des données

Décision de projet reformulée : Est-il nécessaire et sûr de divulguer des données personnelles aux donateurs ?

Pour les donateurs, il est important d'assurer la responsabilité et la transparence dans leurs activités de financement, et vous pourriez être invité à divulguer certaines données sur les bénéficiaires Il est à nouveau important de réfléchir aux risques potentiels pour la vie privée des bénéficiaires et d'envisager des possibilités pour limiter la quantité de données divulguées.

Les donateurs ont deux objectifs principaux de demande et d'usage des données des bénéficiaires :

- **Comprendre le programme et suivre son état d'avancement.** Le donateur souhaite généralement comprendre les circonstances sur le terrain et la manière dont l'équipe du programme réagit. Dans ce cas, il suffit généralement de divulguer des informations générales et des données agrégées (critères cibles, zones ciblées, nombre de personnes assistées, pourcentage de personnes âgées ou d'enfants, montant de l'aide monétaire, etc.). La divulgation de données comme les noms et autres données personnelles n'est généralement pas nécessaire. Le donateur peut également être intéressé par la façon dont les bénéficiaires dépensent l'argent qu'ils reçoivent.[12] Encore une fois, des données agrégées devraient suffire (par exemple, le pourcentage de personnes qui ont dépensé de l'argent pour la nourriture et d'autres produits, le pourcentage de personnes qui ont conservé l'argent plus d'une semaine, etc.).
- **Pour satisfaire aux exigences d'audit.** Le donateur a souvent besoin des données des bénéficiaires pour satisfaire à ses exigences d'audit. Les donateurs doivent s'assurer que l'argent donné est effectivement dépensé aux fins prévues. D'autres audits vérifient si les bénéficiaires sont de vraies personnes, qu'ils remplissent les critères de ciblage convenus et qu'ils ont effectivement reçu l'aide monétaire (accusé de réception). Pour ces activités liées à l'audit, il existe différentes options pour protéger la vie privée des bénéficiaires. Voici les possibilités de protection de la vie privée :

  Lors de la **diffusion d'une liste** pour effectuer les vérifications, les données comprises pourraient être limitées au minimum requis et, éventuellement, au lieu d'exposer les noms des bénéficiaires, des identifiants de référence uniques pourraient être utilisés. Pour une preuve de réception, par exemple, le nom, la date et la signature indiquant qu'ils ont reçu de l'argent liquide devraient suffire. Dans certains cas, même le nom peut ne pas être nécessaire tant que l'identifiant du bénéficiaire est fourni. Si les signatures ont été recueillies sur papier comportant plus d'informations que nécessaire, les colonnes respectives doivent être expurgées, supprimées ou masquées avant de les envoyer au donateur pour renforcer la protection des données.

[12] Sachez noter que ce type d'informations ne doit pas être recueilli automatiquement. Il doit y avoir une raison légitime de recueillir des informations sur les achats effectués par les bénéficiaires. Avant de recueillir ces informations, qui peuvent révéler des informations sensibles sur les bénéficiaires, entreprenez un examen de protection des données. Voir le chapitre sur le suivi.

Une autre approche consiste à accorder un **accès limité en lecture seule** à la base de données ou à la documentation où les auditeurs peuvent effectuer leurs vérifications ponctuelles. Les auditeurs du donateur peuvent vérifier les données ou la documentation pertinentes en personne avec vous, sans télécharger ni emporter de données avec eux. Vous pouvez discuter à l'avance avec le donateur des informations nécessaires et des méthodes pour effectuer ces vérifications. La transmission de données avec les donateurs doit faire partie intégrante du contrat ou de l'accord avec eux.[13] La base légitime devrait être identifiée et les bénéficiaires devraient être informés de la transmission de données prévue avec les donateurs.

VII. Suivi Post-Distribution

Usage de données personnelles

Pour comprendre si les objectifs du programme de TM sont atteints, une stratégie de suivi et d'évaluation est nécessaire. Une partie de cette stratégie consiste à déterminer les indicateurs nécessaires pour identifier les produits, les résultats et l'impact, ainsi que la méthodologie pour obtenir et analyser ces indicateurs. Il existe différents types de suivi, notamment la surveillance du marché, la surveillance de base, la surveillance de l'encaissement (généralement à l'aide de sondages de sortie) et le suivi post-distribution. Pour cette section, nous nous concentrerons sur le suivi post-distribution (PDM). Pour de plus amples renseignements sur le suivi et l'évaluation, voir le module M5_2 Suivi du programme de la boîte à outils CiE.

Pour les organisations humanitaires et les donateurs, il est important de savoir quand et comment les bénéficiaires dépensent l'argent qu'ils ont touché. Les PDM ont généralement lieu quelques semaines après une distribution monétaire pour permettre aux bénéficiaires de dépenser l'argent qu'ils ont touché. Les PDM sont utiles pour évaluer la qualité du programme et améliorer les futurs programmes monétaires et l'utilisation de données personnelles est très probable. Selon le programme, il pourrait y avoir plusieurs visites aux bénéficiaires pour suivre les progrès (par exemple, la construction d'abris dans le cadre d'une récupération) où différents ensembles de données devront être suivis au fil du temps.

Dispositions relatives à la protection des données

Le mot « suivi » pourrait indiquer que les bénéficiaires sont contrôlés d'une certaine manière, leur comportement, analysé. En réalité, ce n'est pas le bénéficiaire, mais le programme et son efficacité qui sont contrôlés. Cependant, cela ne signifie pas que le suivi (du programme) n'aura pas de conséquence pour le bénéficiaire. Ainsi, la vie privée des bénéficiaires doit être prise en compte.

NB : Les décisions de projet de ce chapitre se concentreront sur le PDM. Pour le suivi de base et d'encaissement, l'aspect clé est la minimisation/nécessité des données. Lors du recueil de données auprès des bénéficiaires, il est important de réfléchir aux données réellement nécessaires dans le cadre du suivi de votre programme. Si des modèles standardisés sont utilisés, ils doivent être adaptés au contexte en expurgeant les questions inutiles. Reportez-vous aux chapitres sur le ciblage et l'inscription des bénéficiaires. Une autre méthode recommandée pour augmenter le niveau de protection des données dans le suivi de référence et d'encaissement consiste à supprimer l'identification directe des bénéficiaires (par exemple, noms et identifiants personnels).

[13] Il est important de prendre en compte des questions telles que les exigences d'audit au stade de la négociation du contrat.

Décision projet 1 : Quelles sont les données personnelles à recueillir durant le suivi ?

Minimisation, nécessité

Décision de projet reformulée : Comment puis-je restreindre l'utilisation des données personnelles dans le processus de suivi ?

Selon le contexte, le suivi peut être effectué de différentes manières. Nous examinerons ici le PDM pour les transferts conditionnels et inconditionnels et les dispositions relatives à la protection des données.

Conditionnalité et restrictions

Le programme TM peut avoir certaines *conditions* à respecter (condition préalable que les bénéficiaires doivent remplir avant de toucher de l'argent, comme la présence à l'école, promotion de la santé, atelier sur les moyens de subsistance) ou des restrictions (obligeant les bénéficiaires à utiliser l'assistance pour des articles ou services spécifiques ou à obtenir un résultat tel que réparer un abri ou créer des moyens de subsistance). Le but de ce suivi est de vérifier si les conditions restent respectées ainsi que les restrictions au fil du temps. Une disposition clé est la vie privée des bénéficiaires. Cela peut être fait en réduisant la quantité d'informations recueillies à ce qui est absolument nécessaire. En outre, il est utile de fixer des intervalles de temps raisonnables pour le suivi et de limiter le nombre de personnes impliquées dans le suivi des mêmes bénéficiaires. Limitez également l'accès aux données désagrégées qui pourraient être utilisées par différents acteurs aidant ou impliquées dans le processus de suivi.

Exemple :

Dans le cadre d'un programme, les bénéficiaires doivent utiliser leur aide pour construire des abris après un ouragan dévastateur. L'équipe du programme décide de rendre visite à chaque bénéficiaire après une semaine et à nouveau après trois semaines pour voir comment la reconstruction de l'abri progresse. L'équipe posera des questions sur les matériaux achetés avec l'aide monétaire et vérifiera visuellement l'état de l'abri. Ils ne demanderont pas au bénéficiaire de remplir de longs modèles sur ses conditions de vie générales ou de prendre une photo de la construction. L'équipe du programme a également décidé de disposer de deux équipes de suivi distinctes chargées de différentes zones géographiques. Les mêmes équipes suivront les mêmes ménages après trois semaines pour assurer la cohérence du suivi puisque les photos ne sont pas prises, les mêmes membres du personnel sont en mesure de vérifier la progression de la construction.

Sans conditions et sans limite

Lorsque de l'argent est distribué aux bénéficiaires pour qu'ils dépensent pour leurs propres besoins spécifiques et non pour un produit ou une activité prédéfinis, le suivi peut être différent. Les données relatives aux bénéficiaires seront toujours nécessaires pour déterminer comment (en termes généraux, par exemple par catégorie) ils ont dépensé l'argent auquel ils ont droit et si les objectifs du programme ont été atteints. L'intention ici n'est pas de surveiller le bénéficiaire individuel, mais de comprendre l'efficacité du programme. Le comportement général des bénéficiaires participants est un indicateur important pour évaluer si les critères de ciblage et le montant d'argent versé étaient appropriés.

Une méthode de suivi typique consiste à mettre en place des groupes de discussion (FGD) avec un échantillon de bénéficiaires et de non-bénéficiaires de la communauté. Avec ces personnes, une discussion orale a lieu sur le projet en général. Ils sont généralement interrogés sur leur opinion sur le projet (les

critères de ciblage, les effets du projet, etc.). En outre, ils sont invités à faire part de leur expérience sur la manière dont l'argent a été dépensé. Du point de vue de la protection des données, les discussions orales en tant que telles sont moins problématiques que le recueil officiel d'informations sous forme papier ou numérique. Cependant, il convient d'examiner attentivement la manière dont les groupes de discussion sont enregistrés. Les enregistrements vidéo et audio peuvent fortement porter atteinte à la vie privée des participants. En général, il est préférable de rédiger un compte rendu de la réunion. Très probablement, cela permettra également aux participants d'exprimer plus facilement leur expérience et leur opinion. Lorsque vous prenez des notes de réunion, il existe plusieurs moyens de renforcer le niveau de confidentialité. Il vaut la peine d'envisager de limiter vos notes aux :

- Points de discussion généraux, plutôt que de distinguer les individus et leurs commentaires respectifs
- Nombre de participants et leurs caractéristiques clés qui en font de bons échantillons (âge, sexe, lieu de vie), plutôt que de saisir leurs noms complets

Les commentaires peuvent encore ne pas être complètement anonymes. Les participants à la discussion sauront qui a dit quoi. Cependant, pour les personnes qui consultent les notes de réunion ultérieurement, il sera plus difficile d'identifier une seule personne derrière un certain commentaire. Bien entendu, cela dépend du contexte si ces informations limitées seraient suffisantes aux fins de la surveillance.

Une autre méthode de suivi consiste à réaliser des entretiens avec un échantillon de bénéficiaires. Cela se fait généralement avec des modèles de questionnaire. Il sera important de vérifier l'identité du bénéficiaire interrogé pour s'assurer qu'il s'agit de la bonne personne et qu'il a bien reçu l'aide monétaire. Mais ces informations d'identité peuvent ne pas être nécessaires à stocker, de sorte qu'un certain niveau d'anonymat peut être maintenu. L'enquêteur connaîtra l'identité du bénéficiaire, mais les données produites après avoir rempli le questionnaire seront mieux protégées contre les autres personnes qui les consultent.

Exemple :

L'équipe du programme demande à un échantillon de bénéficiaires de participer à un PDM pour déterminer comment l'aide monétaire a servi.[14] *L'équipe vérifie les pièces d'identité des participants mais ne note pas leurs noms et autres identifiants dans le formulaire de sondage. Durant le sondage, les bénéficiaires n'ont pas caché leur mécontentement quant à l'encaissement, car ils ont dû parcourir de longues distances pour atteindre un agent monétaire, il y a eu des problèmes de liquidité avec l'agent monétaire, et les bénéficiaires ont indiqué qu'il aurait été utile de recevoir une aide en nature plutôt qu'un transfert monétaire. En raison du respect de leur vie privée, leur honnêteté a permis à l'équipe du programme d'apprendre et de s'adapter au prochain déboursement monétaire, au lieu de se dire superficiellement satisfaits de peur de ne plus toucher d'argent.*

Lorsqu'il est impossible de garder l'identité du bénéficiaire anonyme dans les questionnaires, il est important de restreindre les questions au minimum nécessaire. Les modèles ont tendance à compter un éventail de questions traitant divers scénarios (« taille unique »). Comme expliqué dans le chapitre Inscription, ces modèles standardisés doivent être adaptés aux circonstances spécifiques selon les besoins. Les questions inutiles sont à rayer ou à supprimer.

Recherchez des moyens d'éviter l'usage de données personnelles. Si des données personnelles sont utilisées à des fins de suivi, il est important d'identifier la base légitime du suivi et d'informer le bénéficiaire du traitement de ses données dans le cadre du suivi.

Décision projet 2 : Quelles données de bénéficiaires le PSF peut-il me communiquer pour suivre mon programme ?

Minimisation, nécessité et confidentialité des données

Décision de projet reformulée : Quelles données le PSF peut-il me communiquer à des fins de surveillance sans atteinte à la vie privée des bénéficiaires ?

Si les programmes monétaires ont recours à des PSF, ces prestataires peuvent disposer de données sur les bénéficiaires qui pourraient être utiles dans le processus de suivi. Selon le PSF, certaines données dont ils disposent peuvent notamment être : quand l'argent a été retiré et où (p. ex., guichet automatique ou agents financiers), l'argent a-t-il été dépensé dans certains établissements (p. ex. épicerie ou magasin de boissons alcoolisés) et signature sur l'accusé de réception. L'obtention de telles données peut aider à accélérer et à obtenir des informations précises sur le processus de surveillance, Cependant, du point de vue de la protection des données, cette approche pourrait présenter certains risques. Les données relatives au paiement et à l'achat peuvent être assez sensibles. Le recueil de ces données auprès d'une source indirecte (à savoir le PSF) plutôt que des bénéficiaires eux-mêmes pourrait être considéré comme une atteinte à leur vie privée.

Comptes personnels des bénéficiaires

Lorsque la distribution se fait via les comptes personnels (bancaires/mobiles) des bénéficiaires, la Société nationale n'a par défaut pas accès à ces comptes. Le PSF, cependant, peut suivre les événements du compte et peut-être disposé à divulguer les données de paiement utiles avec vous. La question est donc de savoir si c'est utile et quels sont les éléments nécessaires aux fins du suivi ? Vous voudrez peut-être savoir quand et comment l'argent a été dépensé. Cependant, le suivi ne se concentre pas sur le bénéficiaire individuel mais plutôt sur le comportement général de tous les bénéficiaires. Par conséquent, il vous suffira normalement de recevoir des informations de paiement agrégées. Par exemple, le PSF pourrait vous informer :

- du pourcentage de bénéficiaires qui ont dépensé leur argent la première semaine
- du pourcentage de bénéficiaires qui ont dépensé l'argent dans un établissement spécifique tel qu'un supermarché ou des pharmacies
- de la durée moyenne qu'il faut aux bénéficiaires pour dépenser tout l'argent
- des régions où l'argent a été dépensé plus rapidement
- de la position relative des agents monétaires et lesquels déboursaient plus que d'autres

En fonction du contexte de votre programme, vous pouvez convenir avec le PSF des informations qu'il doit vous fournir, en gardant à l'esprit le principe de minimisation et de nécessité des données.

[14] Sachez que les bénéficiaires doivent fournir volontairement des informations, mais ne peuvent pas y être contraints. Il doit être précisé que leur participation n'aura aucune incidence sur les distributions actuelles ou futures et qu'ils sont libres de refuser.

Exemple :

Un programme de TM distribue de l'argent au moyen de cartes prépayées où les bénéficiaires peuvent s'en servir pour acheter dans les magasins et établissements qui acceptent les MasterCard ou retirer à un guichet automatique. La Société nationale aimerait connaître les catégories de produits pour lesquelles l'argent a été dépensé et elle vérifie auprès du PSF si ces informations peuvent lui être communiquées. L'équipe du programme demande spécifiquement des données agrégées et une visualisation si (1) les espèces sont davantage utilisées pour retirer des guichets automatiques par rapport aux achats en magasin, (2) le pourcentage de bénéficiaires qui n'ont pas encore utilisé leur aide monétaire, et (3) les catégories d'établissements où les cartes ont été utilisées (p. ex., nourriture, médicaments, service). Le PSF ne transmet que les données agrégées et les visions utiles plutôt que des données spécifiques sur les achats et sur qui a effectué une transaction où et quand.

Dans la pratique, et s'il n'a pas été négocié auparavant, le PSF pourrait ne pas être disposé à créer les rapports spécifiques ou à vous donner des informations trop spécifiques, car il s'agit d'un effort supplémentaire. Si tel est le cas, une autre possibilité consiste à demander au PSF de **ne pas** vous envoyer l'ensemble complet des données de paiement et uniquement des informations transactionnelles très limitées pour protéger le vie privée des bénéficiaires. Le PSF doit être invité à supprimer les noms et numéros de carte pour chaque activité financière.

Si la seule possibilité est de recevoir les données transactionnelles brutes complètes du PSF, il est conseillé de limiter qui les reçoit et accède aux données complètes et que cette personne soit désignée comme le « gardien » au sein de votre équipe. Le PSF n'enverra les données de paiement qu'à cette seule personne. Le « gardien » ne peut alors extraire que les informations nécessaires pour que le reste de l'équipe du programme puisse les traiter. Le gardien peut alors supprimer en toute sécurité toutes les données reçues par le PSF, afin qu'elles ne soient pas utilisées par inadvertance pour autre chose. Les informations agrégées abstraites offrent un niveau de protection des données plus élevé et, dans de nombreux cas, pourraient s'avérer suffisantes.

Exemple :

Un programme monétaire consiste à distribuer de l'argent en utilisant les portefeuilles d'argent mobile des bénéficiaires. La Société nationale aimerait savoir quels agents d'argent mobile ont été utilisés pour l'encaissement afin qu'ils puissent informer les vendeurs avant la prochaine distribution en cas de problèmes de liquidité. Le PSF n'est pas en mesure de donner uniquement ces informations, mais est prêt à envoyer la liste complète des transactions avec toutes les activités financières de chaque bénéficiaire individuel et où elles encaissent. L'équipe du programme informe le PSF qu'il ne doit l'envoyer uniquement qu'au gestionnaire de la GI qui soutient le programme monétaire qui extraira ensuite les données nécessaires pour que l'équipe du programme les traite. Le gestionnaire de GI supprime le fichier après avoir extrait uniquement les données agrégées nécessaires à l'équipe.

Compte virtuel de la Société nationale

Lorsque la distribution se fait par le biais de comptes virtuels de la Société nationale (voir chapitre PSF), le PSF peut ne pas avoir de lien direct entre les données transactionnelles et les bénéficiaires réels, puisque la gestion des sous-comptes est assurée par la Société nationale. Par conséquent, avoir un accès direct aux transactions des bénéficiaires parce que vous êtes le titulaire du compte peut présenter des risques pour la vie privée. Comme nous l'avons évoqué, les données de paiement individuelles sont sensibles et aux fins du suivi, il n'est normalement pas nécessaire de connaître les bénéficiaires individuels mais plutôt le groupe de bénéficiaires dans son ensemble.

Une possibilité de protéger à nouveau la vie privée des bénéficiaires consiste à désigner un « gardien » qui aura l'accès à l'intégralité des transactions disponibles sur la plate-forme. Si une seule personne de l'équipe accède à la plateforme et transforme les informations individuelles en informations abstraites, le risque de protection des données pourrait être réduit. S'il n'est pas possible de désigner un « gardien », il incombe à tous les membres de l'équipe qui ont accès à la plateforme et à l'ensemble complet de données, de respecter la confidentialité et la vie privée des bénéficiaires et de s'assurer que les identifiants de sous-compte ne sont pas liés aux individus ; il est donc essentiel que tous les membres de l'équipe connaissent bien les pratiques et principes de protection des données.

Essayez de surveiller le programme sans recevoir de données personnelles sur les bénéficiaires du PSF. Chaque fois que vous recevez de telles données, il est important d'en informer le bénéficiaire et d'expliquer comment vous pensez protéger leur vie privée.

Décision projet 3 : Quelles données de bénéficiaires peut me donner le commerçant pour mon programme coupon ?

Minimisation, nécessité et sécurité des données

Décision de projet reformulée : Quelles données le commerçant peut-il me fournir à des fins de contrôle sans porter atteinte à la vie privée des bénéficiaires ?

Dans les programmes de coupons, les données de transaction des commerçants peuvent être utilisées dans le suivi. Le commerçant aura des enregistrements sur combien de coupons ont été échangés dans quel délai, et ils auront également des enregistrements des produits sélectionnés en échange des coupons. Cependant, il est toujours important d'assurer un niveau élevé de protection des données lors de l'utilisation de ces informations. Il suffit généralement d'examiner les données agrégées de l'utilisation générale des coupons et des produits achetés. La raison pour laquelle un seul bénéficiaire a utilisé le coupon n'a aucune importance aux fins du suivi. Ce qui est important, c'est de comprendre le comportement général des bénéficiaires participants afin d'évaluer l'efficacité du programme. Il convient donc d'éviter d'examiner les données qui permettent d'identifier quand et où un bénéficiaire particulier a acheté un certain produit. Cela est possible en demandant au marchand d'agréger les données pour vous. Si ce n'est pas possible, demandez uniquement un ensemble de données limité sans identifiant. Sinon, comme dans les sections précédentes, essayez de désigner un « gardien » au sein de votre équipe qui recevra et extraira uniquement l'ensemble de données utiles, et supprimera immédiatement la liste complète des transactions.

VII. Guide général

Cette section traite des principales dispositions relatives à la protection des données applicables tout au long du programme monétaire.

Dispositions relatives à la protection des données

Stockage des données

Lors du recueil des données personnelles des bénéficiaires, il est extrêmement important de les garder en sécurité et de les protéger. Cela signifie prendre des mesures de sécurité suffisantes pour éviter une soi-disant violation de données (perte, accès non autorisé, etc.) (voir ci-dessous des conseils sur la marche à suivre en cas de violation de données).

Les solutions informatiques pour la sécurité des données sont très techniques et nécessitent souvent des connaissances approfondies. Par conséquent, il est recommandé de développer une approche transversale cohérente avec votre direction informatique si possible. Le concept peut concerner les flux de données, les canaux et interfaces d'échange de données, les niveaux de cryptage lorsque les données sont stockées et transférées, la sauvegarde ou le stockage redondant pour éviter la perte de données, et les contrôles d'accès pour garantir que seules les personnes autorisées utilisent les données, etc.

Quoi qu'il en soit, les aspects suivants doivent être examinés attentivement :

- Pour les données numériques, dans la mesure du possible, il est essentiel d'utiliser une base de données ou une solution de gestion des données de solide. Le stockage de données dans des répertoires accessibles au public tels que Google ou Dropbox doit être constamment évité. L'utilisation de bases de données présente de nombreux avantages, car elles offrent une sécurité technique, comme le cryptage natif, les conteneurs/dossiers protégés par mot de passe, le traçage des fichiers journaux, les sauvegardes, etc. Les solutions de gestion des données (telles que RedRose et LMMS) peuvent s'intégrer à différentes données des outils de recueil tels que ODK/Kobo et des mécanismes de paiement tels que l'argent mobile ou les banques pour le transfert monétaire. Il est important d'évaluer ces solutions en termes de sécurité des données pour s'assurer que les données sont protégées, qu'elles soient en transit (par exemple, lors de l'utilisation du recueil de données mobiles comme ODK/Kobo et les données sont téléchargées du téléphone mobile vers le serveur de gestion des données) ou au repos (lorsque les données sont stockées sur le serveur Cloud). Le lieu de stockage physique des données doit également être évalué par rapport aux lois nationales (c'est-à-dire que certains pays interdisent ou imposent des limites au transfert de données personnelles hors de leur juridiction).
- Lorsque les données doivent être stockées sur ordinateur portable ou clé USB, le risque de perte et de vol est plus élevé que dans une base de données adéquate. Des mesures de sécurité supplémentaires devraient être adoptées pour limiter ce risque. Le matériel doit idéalement être protégé par un cryptage du disque dur (par exemple, Bitlocker de Microsoft). En outre, vous pouvez ajouter un niveau de protection supplémentaire en chiffrant ou en protégeant par mot de passe les documents sur le disque dur. Les ordinateurs portables et les clés USB doivent également être physiquement sécurisés par verrous d'ordinateur portable et conservés dans un tiroir verrouillé lorsqu'ils ne sont pas utilisés.
- Lors de la création d'un mot de passe, essayez d'utiliser des mots de passe compliqués, et difficiles à deviner. Une bonne pratique consiste à utiliser des lettres minuscules et majuscules, des chiffres et des caractères spéciaux et à changer régulièrement de mot de passe. Évitez de transmettre des comptes et des mots de passe. Si le compte est générique (par exemple, des boîtes de courrier électronique génériques administrées par plusieurs personnes), il est important de limiter ce nombre de personnes (voir ci-dessous - Contrôle d'accès).
- Les fichiers papier présentent un risque encore plus élevé de perte et d'accès non autorisé. Si les fichiers papier sont la seule voie possible, stockez-les dans un répertoire avec verrou. Lors de leur utilisation, cela permet de limiter la visibilité par des tiers.

Pour plus de conseils, veuillez consulter le dépliant sur la protection des données de GI de la FICR, qui énonce les choses à faire et à ne pas faire en matière de stockage et de traitement et la politique de

sécurité des informations de la FICR.

Conservation et suppression de données

Que deviennent les données personnelles du bénéficiaire une fois le programme terminé ? Idéalement, ils ne sont pas laissés dans des fichiers papier ou dans une base de données pour une durée illimitée. Une fois que les données d'un programme spécifique ne sont plus nécessaires, elles doivent être supprimées, ou du moins agrégées ou anonymisées. Si nécessaire pendant une période prolongée mais sans nécessiter un accès régulier (comme des audits), l'archivage de manière hors ligne et sécurisée pourrait être une possibilité.

Périodes de conservation

Il est recommandé d'avoir une période de conservation limitée dans le temps à l'avance, définissant la durée de conservation des données. Une fois la période de conservation expirée, les données sont supprimées. Uniquement pour des raisons impérieuses qui nécessitent une prolongation de conservation, les données peuvent être conservées pendant une période prolongée mais limitée. Les périodes de conservation peuvent être intégrées dans les bases de données pour permettre la purge automatisée des données. Si vous souhaitez en savoir plus sur ces options, adressez-vous à vos collègues informaticiens. Si les bases de données ou les périodes de rétention automatisées ne peuvent pas être utilisées, une autre option consiste à définir des rappels de calendrier. L'objectif est de réfléchir activement, à intervalles réguliers, à savoir s'il faut conserver ou détruire les données devenues inutiles. La durée des périodes de conservation dépend du programme lui-même, mais peut également être dictée par les politiques de votre propre structure. Lors de la conception de l'intervention TM, les périodes de conservation appropriées doivent être prises en compte afin d'être communiquées aux bénéficiaires. Certains aspects à prendre en compte sont :

- la durée du projet
- la sensibilité des données
- l'ampleur du suivi prévu
- la probabilité de problèmes de suivi

Autres objectifs

Même si le programme a été clos et le suivi, effectué, il peut paraître utile de conserver certaines données à d'autres fins. Premièrement, ils pourraient être utilisés pour créer **des rapports et des statistiques** supplémentaires. Cependant, à cette fin, il n'est généralement pas nécessaire de conserver des données qui identifient directement les personnes (par exemple, les noms, les numéros d'identification). Il suffit de générer un ensemble condensé de données agrégées. Deuxièmement, en particulier pour les zones sujettes aux mêmes dangers, il est probable que les données puissent être utiles pour la **préparation générale à de futurs programmes similaires** (par exemple, des ouragans ou des typhons récurrents). Dans de telles situations, il peut sembler raisonnable de simplement conserver les données. Cependant, les données ont tendance à être de durée de vie limitée. Pour les nouveaux programmes, ils doivent être mis à jour et vérifiés. Les gens quittent ou emménagent dans la région, leurs conditions de vie changent, nouvelles naissances ou décès dans la famille. Par conséquent, la conservation des données pour un nouveau programme potentiel n'est très souvent pas utile. Si vous décidez de conserver les données pour un programme futur, il est également important de se demander si la nouvelle finalité est compatible avec la finalité initiale. Les finalités humanitaires peuvent être compatibles, mais si la finalité n'est pas compatible, il est essentiel d'informer les bénéficiaires de votre intention de réutiliser les données à une autre fin et d'identifier une nouvelle base juridique pour ce nouveau traitement (voir la section Base légitime du chapitre Inscription). Troisièmement, les données pourraient devoir être stockées à des **fins d'audit**. Si tel est le cas, les exigences d'audit nomment normalement les périodes de stockage requises. Sinon, une période de stockage raisonnable peut souvent être identifiée en examinant le calendrier et/ou le but de l'audit. Les données stockées à des fins d'audit doivent être archivées séparément des autres flux de

données.

Données non-bénéficiaires

Durant le processus de ciblage, vous recueillez des données personnelles auprès de personnes qui, en fin de compte, risquent de ne pas bénéficier de l'assistance car elles ne satisfont pas au contrôle d'admissibilité (voir chapitre Ciblage). De même, lors de l'inscription des bénéficiaires, vous avez peut-être recueilli des données auprès de personnes qui s'avèrent non admissibles. Le stockage des données personnelles de ces non-bénéficiaires doit être traité avec beaucoup d'attention. Puisqu'ils ne participeront pas au programme, leurs données deviennent inutiles une fois la vérification d'admissibilité terminée. Néanmoins, il peut être dans votre intérêt et même dans l'intérêt des non-bénéficiaires de conserver leurs informations personnelles un certain temps. L'une des raisons pourrait être d'avoir des preuves des décisions si le non-bénéficiaire dépose une plainte contre la Société nationale pour avoir été exclu du programme. Dans ce cas, il peut être très utile de voir comment cela a été décidé et quels points ont été utilisés dans la décision. Si possible, dans de telles situations, stockez les informations respectives séparément du reste des autres bénéficiaires admissibles. L'idée est que ces données ne font plus partie du flux de données du programme en cours. Néanmoins, en cas de réclamation, il peut être récupéré.

Contrôle d'accès

Les informations recueillies directement auprès des bénéficiaires ou auprès d'autres sources (gouvernements, etc.) doivent être traitées de manière confidentielle. La confidentialité est étroitement liée aux principes de minimisation, de nécessité et de sécurité des données comme expliqué ci-dessus.

Les programmes monétaires impliquent généralement différents acteurs : internes (par exemple, équipes directes de programme et de terrain, services de soutien tels que des collègues des finances, de la logistique, de la GI et des TI, et des gestionnaires) et externes (par exemple, PSF, donateurs, gouvernement, autres ONG). Nous avons déjà étudié le traitement des données personnelles avec des acteurs externes (voir les chapitres sur le PSF et la transmission de données avec des externes). Pour les acteurs internes, il est important de déterminer le type d'accès et le niveau d'accès requis en ce qui concerne les données des bénéficiaires. Certaines organisations procèdent à une classification des informations. Par exemple, La politique de sécurité des informations de la FICR classe les données des bénéficiaires comme confidentielles ou hautement confidentielles selon le contexte ; cela nécessite le plus haut niveau de protection de sécurité ainsi qu'un Accès restreint sur la base du « besoin de savoir ».

Voici quelques moyens d'assurer un contrôle d'accès adéquats :

- Saisissez le nom d'utilisateur et le mot de passe pour accéder à la base de données ou à la plate-forme de gestion des données. Informez les utilisateurs de ne pas partager leur nom d'utilisateur et leur mot de passe avec d'autres personnes. Évitez également de créer des utilisateurs génériques pour lesquels plusieurs personnes peuvent se connecter en tant qu'utilisateur. Les actions de chaque utilisateur doivent être vérifiables et traçables.
- Utilisez le contrôle d'accès basé sur les rôles (RBAC), ce qui signifie que les utilisateurs se voient attribuer des rôles spécifiques et que chaque rôle donne accès à certaines fonctions et données du système. L'accès peut être aussi précis que nécessaire (par exemple, accès à la liste des bénéficiaires, possibilité de télécharger la liste des bénéficiaires ou simplement accorder l'accès à des données agrégées telles que des tableaux de bord). L'accès doit être révoqué en cas de problème de sécurité avec un utilisateur.
- Tenez un journal d'accès pour enregistrer toutes les personnes qui se connectent et accèdent à certaines pages ou données, ainsi qu'un journal de téléchargement pour ceux qui téléchargent des données directement à partir du système (en notant que cela est également considéré comme un recueil et un traitement de données personnelles et doit être traité de manière appropriée).
- Lors du téléchargement de données dans une feuille de calcul Excel, ajoutez une protection par mot de passe ou chiffrez le fichier.

- En l'absence d'une base de données, les fichiers doivent être protégés par mot de passe et seul le personnel autorisé doit avoir l'accès aux fichiers. Pour les fichiers papier, seul le personnel autorisé doit également avoir un accès direct et les fichiers doivent être conservés dans un conteneur verrouillé.

Exemple :

La mise en œuvre du programme de distribution d'argent implique 10 membres du personnel et des volontaires. Trois d'entre eux sont responsables du ciblage et de l'inscription des bénéficiaires (équipe 1), tandis que les 7 autres sont uniquement chargés de contacter les prestataires de services et de distribuer l'argent (équipe 2). L'équipe 2 n'a pas besoin de connaître la vulnérabilité des bénéficiaires. Ils ont seulement besoin de connaître ces données personnelles, qui sont nécessaires pour la partie monétaire du projet (noms, comptes bancaires, KYC). Par conséquent, une liste de bénéficiaires avec des informations limitées est générée pour eux par l'équipe 1. Toutes les autres informations sont stockées dans une base de données protégée par mot de passe, que seule l'équipe 1 possède. En outre, seule une personne a le rôle d'administrateur et peut accéder pleinement à la base de données (possibilité de lecture et écriture), tandis que les deux autres membres de l'équipe ont un accès en lecture seule.

Dans le même cas de figure, la méthode de distribution est la monnaie sous enveloppe. Il est attendu que l'équipe 2 devra justifier le choix des bénéficiaires le jour de la distribution. Si une telle situation se présente, il est nécessaire que l'équipe 2 ait accès aux informations complémentaires. Par conséquent, ils demanderont les informations supplémentaires à l'équipe 1 qui génère les informations supplémentaires limitées.

Procédure de transmission (divulgation de données)

Lors de la divulgation de données, le processus de transmission peut augmenter le risque de perte de données et d'accès non autorisé. Par conséquent, lors de la transmission de données personnelles, les mesures de sécurité jouent un rôle important.

- Idéalement, les données sont transmises à l'aide d'**outils sécurisés** tels qu'un FTP sécurisé avec nom d'utilisateur et mot de passe et un accès limité pour télécharger des données à partir de la base de données sécurisée ou de la plate-forme de gestion des données.

- Si la communication concernant les bénéficiaires doit devoir être par **courrier électronique**, il est important de se rappeler de : (1) limiter le nombre de destinataires, (2) protéger les pièces jointes par mot de passe et (3) chiffrer les e-mails (dans la mesure du possible). Cela offre une certaine protection en cas de piratage des courriels ou d'envoi accidentel d'un courriel à une mauvaise adresse. Le risque d'exposer les données des bénéficiaires à des personnes non autorisées est réduit lorsque les messages et les pièces jointes sont chiffrés. Si vous ignorez comment chiffrer des fichiers ou des messages, veuillez contacter vos collègues informaticiens. Envoyer des messages à des listes de diffusion plutôt qu'à des individus peut sembler pratique, mais peut être problématique si vous ne savez pas exactement qui figure dans les listes de diffusion. Il en va de même lors de l'envoi à des adresses électroniques génériques pouvant s'adresser à différentes personnes avec le même mot de passe ou en cas de gestion du compte de messagerie générique. Soyez également vigilant si des messages sont transmis à des tiers ou en cas de chaînes créées par des destinataires qui y répondent. Au fur et à mesure que le nombre de destinataires augmente ou évolue, assurez-vous que les nouveaux destinataires sont également autorisés à être informés des données personnelles du bénéficiaire.

  Par exemple :

  La situation de certains bénéficiaires potentiels se discute par courrier électronique avec les responsables communautaires pour décider s'ils sont admissibles au programme monétaire. Le courrier peut être envoyé au responsable de la communauté qui aide à la prise de décision, et aux collègues impliqués dans le ciblage. Cependant, il faut éviter d'envoyer le message à une adresse courriel générique telle que « info @community » ou « cashteam@ ».

- Soyez prudent si vous souhaitez envoyer des fichiers comportant des données personnelles via des **applications de messagerie mobile**, telles que WhatsApp. À moins que vous ayez confiance en la sécurité de l'application de messagerie (par exemple, Signal est considéré par beaucoup comme beaucoup plus sécurisé que WhatsApp), **abstenez-vous d'en faire usage** pour divulguer des données personnelles ou d'autres données sensibles (que ce soit du personnel, des volontaires ou des bénéficiaires).

Traitement des violations en matière de données

Malgré toutes les mesures de sécurité, il est impossible de garantir qu'une violation de données puisse être évitée dans toutes les situations. Comme défini au début de ce guide, une violation de données *signifie l'accès non autorisé, ou la destruction, la perte, l'altération ou la divulgation de données personnelles.* Une fois qu'une violation de données a eu lieu, il est important de prendre les mesures qu'il faut pour remédier aux conséquences de cette violation. Il est recommandé de vous informer ainsi que votre personnel de ces mesures par anticipation. Dès que vous avez pris connaissance d'une violation, veillez à :

- **La signaler sans plus attendre** à votre responsable ou superviseur ainsi qu'au point focal de la protection des données, à l'équipe juridique ou à une autre personne chargée de la protection des données dans votre Société nationale. Si vous ignorez qui est responsable, faites part de vos scrupules aux dirigeants de votre organisation.

Les étapes suivantes doivent ensuite être suivies en coopération avec ces experts :

- **Enquêter sur l'étendue de la violation :** De quel genre de violation s'agit-il ? De quel genre de données ? Quelle quantité de données ? Durée de la violation ? Qui sont personnes concernées ? À qui ont été divulguées les données ?
- **(<u>en parallèle</u>) Prenez des mesures d'atténuation** (en fonction du type de violation, *par exemple*,

couper les systèmes informatiques, récupérer des données de sauvegarde, demander à la personne non autorisée de mettre fin à la divulgation des données, combler les lacunes, informer les partenaires impliqués et potentiellement les donateurs.

- **Évaluez le niveau de risque pour les personnes concernées et déployez des efforts raisonnables pour informer les personnes concernées si les risques sont élevés** pour des raisons de transparence.
- En fonction des lois nationales, **pensez à informer les autorités de protection des données de votre pays.**
- **Préparez un rapport/leçons apprises et éliminer les lacunes organisationnelles ou techniques identifiées.**
- **Améliorer le plan d'intervention pour la prochaine incidence** si nécessaire en fonction de l'expérience acquise.

Briefing du personnel et des volontaires

La première étape vers une protection efficace des données est la sensibilisation. Par conséquent, il est important de sensibiliser votre personnel et vos volontaires aux principes clés de la protection des données et à la manière de les aborder dans le cycle du programme TM. Il est recommandé d'organiser régulièrement des séances de formation sur la protection des données, en particulier pour les nouvelles recrues au sein de l'organisation dans le cadre de leur intégration. Le matériel de formation pourrait être préparé à l'avance pour l'intégration et la remise à niveau, pour ceux qui ont déjà été formés. Dans cette formation, l'importance de la protection des données doit être soulignée et les principes clés, expliqués. Plus important encore, quelles sont les dispositions relatives à la protection des données à prendre en compte dans les procédures de TM et les responsabilités du personnel et des volontaires en fonction de leurs rôles. Il convient également de savoir comment agir face aux violations de données.

Analyse et suivi des risques en matière de protection des données

Pour faire de la protection des données une véritable garantie de la vie privée des bénéficiaires dans le cadre de vos programmes, il est fortement recommandé de noter les dispositions relatives à la protection des données que vous effectuez. Pourquoi ? Parce qu'il permet de mettre en place une approche structurée et cohérente pour gérer les risques et trouver un bon équilibre. En outre, l'inscription des risques et des décisions prises sera importante au cas où un audit ou une enquête serait nécessaire.

Certains outils pourraient servir pour analyser et noter les risques liés à la protection des données :

Matrice et registre des risques. La boîte à outils CiE comporte l'analyse des risques dans la préparation (module M1_1 Préparer et analyser), l'évaluation (module M2_4) et l'analyse des réponses (module M3_1_4). Les risques supplémentaires décrits pour les programmes Argent contre travail et Coupons sont également décrits. La même matrice des risques et le même registre des risques pourraient être utilisés pour garantir que les éléments de protection des données sont étudiés avec les autres types de risques. Une nouvelle catégorie de protection des données devra peut-être être créée pour catégoriser les risques de manière adéquate. L'analyse de ces risques et la création de mesures d'atténuation seront importantes. Au fur et à mesure que le programme se déroule, les risques doivent être revus et mis à jour, si nécessaire.

Analyse d'impact sur la protection des données (DPIA).[15] Il s'agit d'un outil officiel pour documenter les dispositions relatives à la protection des données pour les risques identifiés ainsi que les mesures d'atténuation prévues. Sa préparation nécessitera peut-être une consultation externe et l'implication des acteurs concernés telles que vos collègues du service juridique. Les performances d'une DPIA aussi approfondie n'est pas nécessaire dans tous les cas, en particulier lors de l'exécution de programmes TM similaires. Cela peut être nécessaire lorsque de nouvelles méthodes et technologies sont utilisées lorsque

[15] Pour de plus amples renseignements, consultez le Manuel du CICR sur la protection des données dans l'action humanitaire. En outre, un modèle de DPIA peut être trouvé en section de référence de ce guide.

les répercussions sur les bénéficiaires ne sont pas encore connues. En cas de préoccupations potentielles de la part des membres de la communauté en termes de traitement de leurs données, il serait également utile de déterminer où se trouvent les risques réels et s'ils pourraient être atténués.

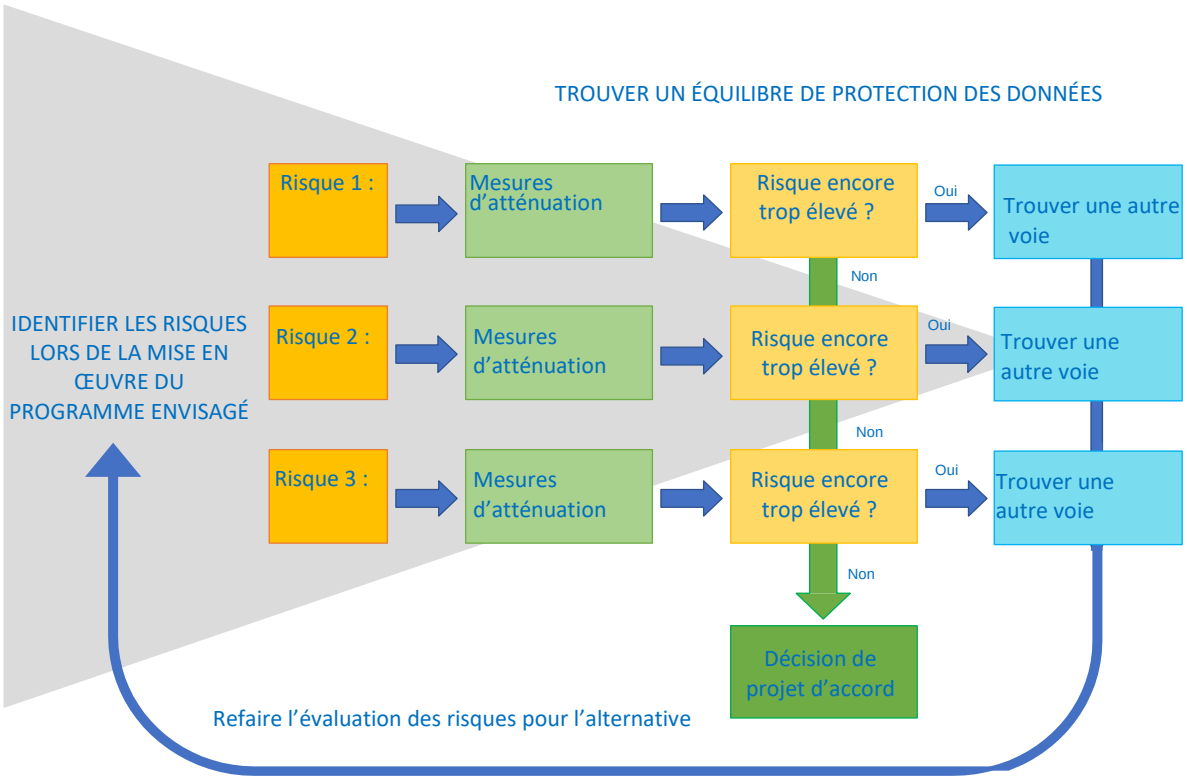

Figure 4 : Trouver un équilibre entre les risques et les actions liées à la protection des données

La figure 4 vise à favoriser la réflexion sur l'évaluation des risques liés à la protection des données. Il s'agit d'identifier et de noter les risques et les mesures d'atténuation possibles, d'évaluer le niveau des risques (en fonction de l'incidence et de la probabilité) et de trouver d'autres voies à prendre en compte. Par exemple :

Implication du PSF ?

> Risque 1 : Traitement des données à d'autres fins que celles qui ont été convenues

> Mesure d'atténuation : interdire contractuellement

> Risque encore trop élevé ? Oui, car la réputation et la fiabilité de PSF laissent à désirer

> Autre voie : autre PSF, monnaie sous enveloppe ou en nature

> refaire l'évaluation des risques autrement

Si une évaluation préliminaire des risques révèle que l'implémentation du programme présente des risques

élevés pour la protection des données, il est conseillé d'effectuer l'évaluation avec un format de DPIA officiel. L'obligation d'effectuer une DPIA officielle incombe à l'organisation qui dirige le programme, dans le cas d'un partenariat d'implémentation.

La réalisation d'une DPIA officielle doit être prise en compte (et en vertu de certaines lois sur la protection des données, elle peut être requise), par exemple, dans les situations énumérées ci-dessous. NB : Tous ces modes de traitement des données sont strictement soumis au principe de minimisation et de nécessité des données. Une DPIA ne peut justifier un traitement inutile de données.

- De nouvelles technologies sont utilisées pour recueillir, administrer ou stocker des données personnelles (stockage cloud, géolocalisation, réseaux sociaux, etc.). Ignorer comment fonctionnent les technologies modernes pourrait augmenter le risque d'accès non autorisé (piratage) et ouvrir des possibilités de surveillance non autorisée.
- Les personnes peuvent être soumises à une prise de décision automatisée ou à un profilage. La prise de décision automatique interfère fortement avec la protection des données, car les décisions sont prises au-delà du contrôle de l'individu et sans la possibilité pour ce dernier de retracer et de discuter de la décision. Le profilage est problématique car créer un profil de personnes revient à les placer dans certaines catégories sans réelle interaction préalable avec l'individu.
- Les données personnelles peuvent être transférées à un tiers (voire un pays étranger) exempt de normes de protection des données similaires. Comme indiqué, la divulgation de données peut entraîner une perte de contrôle sur la façon dont ces données sont utilisées. Cela ne devrait être possible à la seule condition que l'autre partie dispose d'une norme de protection des données adéquate. Si ce n'est pas le cas et que les données doivent tout de même être partagées, il est important de bien évaluer si cela représente un risque trop important pour les bénéficiaires (catégorie de données, norme de protection, etc.)
- Les données sensibles, telles que les données sur l'état de santé ou l'orientation religieuse ou la biométrie peuvent être traitées à grande échelle (nombre de personnes, variété des données, durée du traitement, étendue géographique, etc.). Ces données sont extrêmement sensibles car elles concernent des aspects très personnels et privés de la vie d'une personne. En outre, ce type d'informations entre de mauvaises mains peut être très préjudiciable pour les bénéficiaires.
- La surveillance de masse pourrait faire partie intégrante du programme. La surveillance de masse interfère fortement avec les droits de toutes les personnes concernées, car c'est un aspect important de la vie privée que de ne pas être soumis au contrôle constant d'autrui ou de systèmes automatisés.
- Une consolidation et un croisement de données provenant de différentes sources peuvent se produire. La combinaison de divers ensembles de données sur un individu augmente le risque pour la vie privée de l'individu.

Indépendamment du format, l'évaluation des risques doit être effectuée avant le début du programme, en même temps que l'évaluation générale des risques du programme, comme décrit dans la boîte à outils CiE.

Si vous avez des questions et des inquiétudes concernant la protection des données, n'hésitez pas à communiquer avec votre responsable et/ou votre équipe juridique. Vous pouvez également envoyer vos demandes au Centre de trésorerie, qui est une ressource à l'échelle du Mouvement pour TM. Le Centre de trésorerie soutient les praticiens de l'argent liquide et offre du matériel, y compris les leçons apprises par d'autres Sociétés nationales, et peut avoir examiné des questions similaires d'autres partenaires du Mouvement dans le passé.

Engagement communautaire et la redevabilité (CEA)

Comme indiqué dans tous les chapitres, informer les bénéficiaires et disposer d'un service d'assistance et d'un mécanisme de retour d'information sont des aspects importants d'implémentation de la protection des données. Lorsque la communication avec les bénéficiaires est effectuée par une équipe distincte du CEA, il est important qu'ils soient conscients des dispositions relatives à la protection des données et s'assurent qu'ils disposent d'informations pour répondre aux questions sur la protection des données ou qu'ils sachent comment les adresser à quelqu'un qui pourrait y répondre.

IX. Références

Politiques et guides

- Manuel sur la protection des données dans l'action humanitaire par le CICR et le centre de confidentialité de Bruxelles
- Politique de protection des données de FICR
- Règles de protection des données du CICR
- Politique du traitement des données biométriques du CICR
- Politique de sécurité de l'information de la FICR
- Dépliant de protection des données de GI de la FICR

Modèles et documents auxiliaires

Les documents suivants doivent être contextualisés par les Sociétés nationales pour répondre aux exigences qui leur sont propres ; en particulier, le respect de leurs lois et politiques nationales de protection des données qui pourraient être plus strictes que la norme de protection des données appliquée lors de la préparation de ces documents.

- Modèle de contrat standard pour prestataire de services financiers (provisoire)
- Modèle de diligence due / questionnaire précontractuel pour prestataire de services financiers (provisoire)
- Modèle de DPIA (provisoire)
- Exemple de modèle de notice de confidentialité (provisoire)