CaLP
The Cash Learning Partnership

BOÎTE À OUTILS SUR LA GESTION RESPONSABLE DES DONNÉES

GUIDE À DESTINATION DES PROFESSIONNEL-LES DU SECTEUR DES TRANSFERTS MONÉTAIRES

TABLE DES MATIÈRES ET REMERCIEMENTS

TABLE DES MATIÈRES

AVANT-PROPOS 3

POURQUOI UNE AUTRE BOÎTE À OUTILS ? 4

COMMENT CETTE BOÎTE À OUTILS EST-ELLE STRUCTURÉE ? 6

LISTE DES ACRONYMES 8

FICHE-CONSEIL 1: ÉVALUER LE CONTEXTE ET LA CAPACITÉ 9

FICHE-CONSEIL 2: CONCEVOIR ET PLANIFIER 16

FICHE-CONSEIL 3: COLLECTER/ACCÉDER AUX DONNÉES 27

FICHE-CONSEIL 4: ENVOYER/STOCKER LES DONNÉES 33

FICHE-CONSEIL 5: ANALYSER/EXPLOITER LES DONNÉES 36

FICHE-CONSEIL 6: PARTAGER LES DONNÉES 39

FICHE-CONSEIL 7: ACTUALISER/CONSERVER/SUPPRIMER LES DONNÉES 44

REMERCIEMENTS

La Boîte à outils sur la gestion responsable des données – Guide à destination des professionnel-les du domaine des transferts monétaires a été mandatée par le CaLP avec un financement du Bureau fédéral allemand des Affaires étrangères.

Les recherches étayant cette publication ont été menées entre juin et septembre 2020 par Linda Raftree, consultante indépendante.

La publication a été développée par Linda Raftree, avec l'aide et la supervision éditoriale et en matière de contenu d'Anna Kondakhchyan du CaLP. Il s'agit d'un travail collaboratif compilant les contributions inestimables d'un grand nombre d'organisations et de professionnel-les du secteur des transferts monétaires, qui ont apporté leurs idées et consacré du temps au processus de recherche par l'intermédiaire de sources de données et d'entretiens avec des informateurs/trices clés.

Nous tenons tout particulièrement à remercier les membres du Comité consultatif pour leurs conseils essentiels à la création de la boîte à outils et pour la révision des ébauches, à savoir : Amos Doornbos (World Vision International), James Eaton-Lee (Oxfam), Stuart Campo (OCHA HDX), Jenny Caswell (GSMA), Jo Burton (CICR), Gabriele Erba (UNICEF) et Rosa Akbari (Mercy Corps).

Les opinions exprimées dans la présente publication n'engagent que leurs auteur-es et ne reflètent pas nécessairement celles des bailleurs ou des agences membres du CaLP.

Le CaLP est un réseau mondial dynamique de plus de 90 organisations effectuant un travail essentiel sur les politiques, les pratiques et la recherche dans le domaine des transferts monétaires humanitaires et de l'assistance financière dans son ensemble.

Pour de plus amples informations, consultez le site Web du CaLP à l'adresse www.calpnetwork.org Suivez

le CaLP sur Twitter : @calpnetwork

AVANT-PROPOS

Tous les programmes humanitaires impliquent de recueillir de grandes quantités de données. Dans le domaine des transferts monétaires, nous recueillons des volumes de données importants qui sont souvent partagés avec plusieurs acteurs. La plupart des données collectées sont privées et très sensibles. Elles sont recueillies auprès de populations très vulnérables et concernent directement ces populations. Il est important de concevoir nos programmes et de gérer les données de sorte à réduire le risque de voir ces dernières exploitées - accidentellement ou intentionnellement - d'une manière qui porterait préjudice ou exclurait injustement des personnes ou des groupes des prestations.

Les types de préjudices associés aux données et aux technologies numériques sont les suivants :

- **Risque de blessure**, par exemple lorsque les données sont utilisées pour identifier, localiser et porter une atteinte physique, émotionnelle ou psychologique à un individu ou à un groupe[1].
- **Déni de services ou discrimination** s'appuyant sur des données, notamment pertes d'opportunités et pertes économiques lorsque les données sont utilisées pour valider l'éligibilité à certains services ou avantages[2].
- **Violations des droits humains** telles que la perte de dignité, l'atteinte à la liberté ou à la vie privée lorsque les données sont utilisées pour déshumaniser des personnes, lorsque les décisions sont prises par des algorithmes informatiques, lorsque le recueil des données est invasif ou lorsque les données sont collectées, traitées et partagées sans autorisation, ou encore lorsque les personnes ciblées doivent transmettre leurs données en échange d'un service vital ou pour bénéficier d'un autre droit[3].
- **Ciblage et harcèlement délibérés** des personnes pauvres par l'intermédiaire des nouvelles technologies. Comme indiqué dans le rapport du Rapporteur spécial sur les technologies numériques et l'État-providence, le recours aux technologies pour identifier les fraudes ou violations des conditions imposées aux bénéficiaires de transferts monétaires ou d'autres prestations sociales permet de recueillir et de stocker numériquement les informations pendant une durée indéterminée. Cela implique de conserver d'énormes quantités de données qui peuvent être utilisées indéfiniment à l'encontre d'une personne[4].
- **Érosion des structures sociales ou démocratiques**, par exemple par la manipulation, l'amplification d'un rapport de force ou la désinformation[5].

La gestion des données et le partage des informations sont des composantes essentielles des transferts monétaires. Nous travaillons en effet sur des données sensibles tout au long du processus de transferts monétaires. Par conséquent, de la même manière que la prévention, la protection et le principe « ne pas nuire » sont des éléments incontournables des projets de transferts monétaires et des autres programmes humanitaires, la gestion responsable des données doit être intégrée dans tout ce que nous entreprenons en tant que professionnel-les du secteur des transferts monétaires. La présente boîte à outils concerne les transferts monétaires, mais bon nombre des conseils prodigués peuvent également être appliqués à d'autres programmes humanitaires.

ENCADRÉ 1 : QU'EST-CE QUE LA GESTION RESPONSABLE DES DONNÉES ?

Une gestion responsable des données va au-delà de la confidentialité et de la protection des données ; elle inclut des principes, des processus et des outils qui promeuvent une gestion efficace, éthique et sûre des données[6].

1 Voir le cadre « Types de dommage » de Microsoft pour en savoir plus.
2 Voir P. Alston (2019), Rapport du Rapporteur spécial sur les droits de l'homme et l'extrême pauvreté, qui détaille le rôle des technologies numériques et de l'État-providence. Présenté à l'occasion de la Soixante-quatorzième session de l'Assemblée générale des Nations Unies sur le thème « Promotion et protection des droits de l'homme : questions relatives aux droits de l'homme, y compris les divers moyens de mieux assurer l'exercice effectif des droits de l'homme et des libertés fondamentales ».
3 Voir le Règlement général sur la protection des données (RGPD) (2018) qui répertoire les droits des personnes concernées, notamment le droit de refuser de voir ses données traitées, le droit qu'aucun profil ne soit dressé avec ses données, le droit de refuser toute prise de décision individuelle automatisée, ainsi que le droit de contester une décision automatisée et d'exiger un examen sous la forme d'une intervention humaine.
4 Alston (2019)
5 Cadre « Types de dommage » de Microsoft.
6 OCHA (2016), Think Brief: Building Data Responsibility into Humanitarian Action.

Points clés à prendre en compte :

- **Une gestion responsable des données ne se limite pas aux données.** À l'instar d'autres biens de valeur, les données sont devenues des marchandises. En général, les données individuelles sont converties en informations précieuses exploitées par divers acteurs à des fins différentes (utiles ou nuisibles). Un écosystème complet s'est développé autour des données collectées et traitées dans le cadre des transferts monétaires. Les données peuvent conférer du pouvoir et un avantage économique aux individus, aux agences humanitaires, aux autorités locales et nationales, aux prestataires de services financiers (PSF), aux agents de contrôle tiers, aux entreprises technologiques et aux acteurs non étatiques, qui gèrent toutes et tous des données en lien avec les transferts monétaires.
- **Une gestion responsable des données requiert mise en contexte, créativité, capacité et collaboration.** Divers acteurs recueillent, gèrent, utilisent et partagent des données dans le cadre des transferts monétaires. Différents mandats et motivations organisationnels, rapports de force et niveaux de compétences et de connaissances sont en jeu. Vous devrez identifier des moyens souples et adaptatifs d'atténuer les risques et les dommages associés aux données, surtout dans des contextes fragiles ou affectés par un conflit. Une gestion responsable dépendra de toutes les personnes impliquées dans le cycle de programme, des enquêteurs/trices au personnel de première ligne, en passant par les équipes de direction pays, les prestataires de services financiers, les partenaires et les bailleurs. Dans certains cas, la protection des données peut également mettre en danger le personnel humanitaire et les travailleuses et travailleurs en première ligne.
- **Une gestion responsable des données n'est pas une activité solitaire : elle requiert des équipes expérimentées.** Vous devrez impliquer plusieurs parties de votre organisation et divers types d'expertise pour déterminer comment garantir la protection des données et atténuer les dommages potentiels en lien avec les données lors des transferts monétaires. Cela requiert des compétences techniques (sécurité des informations, administration des systèmes de données, architecture et analyse des données ; administration commerciale et juridique, conformité et compréhension des mécanismes financiers ; genre, inclusion, protection et prévention, etc.) et des compétences générales (négociation et recherche d'un consensus, etc.).

Dans cette boîte à outils, nous proposons un éventail de méthodes pour intégrer la gestion responsable des données dans la planification, la conception et la mise en œuvre des programmes, ainsi que dans les activités MEAL (suivi, évaluation, redevabilité et apprentissage). La boîte à outils représente une « référence absolue » vers laquelle les organisations doivent tendre et identifie les implications éthiques et juridiques dont il faut tenir compte dans le traitement des données. Nous savons qu'il ne sera pas toujours possible d'atteindre cette référence absolue. Vous devrez toujours faire des compromis concernant la vitesse, le budget et d'autres facteurs à prendre en compte, et nous avons bien conscience que les professionnel-les du secteur des transferts monétaires seront tiraillé-es en tous sens. Lorsque nos capacités organisationnelles sont très en deçà des normes juridiques et éthiques, nous pouvons être amené-es à mettre un terme aux activités car le recueil des données pourrait causer du tort ou enfreindre la loi.

Les données sont l'extension d'une personne. Nous devons traiter les données d'une personne avec autant de respect et de soin qu'une personne qui se tient en face de nous.

POURQUOI UNE AUTRE BOÎTE À OUTILS ?

En 2016, ELAN a créé le Data Starter Kit[7], l'une des premières boîtes à outils consacrées à la gestion responsable des données dans les secteurs humanitaire et du développement. Le Data Starter Kit est une ressource centrale pour la communauté CaLP et plus généralement pour les professionnel-les de la gestion responsable des données dans le monde. Au vu de l'évolution du domaine des transferts monétaires depuis 2016, le CaLP a jugé nécessaire de mettre à jour le Data Starter Kit pour l'adapter au contexte actuel. Le volume de transferts monétaires a considérablement augmenté pour passer de 2,8 milliards de dollars en 2016 à 5,6 milliards de dollars en 2019, si bien que les transferts monétaires représentent désormais 18 % de l'ensemble de l'aide humanitaire internationale[8].

Une importance grandissante est également accordée à la qualité, et les rôles et responsabilités concernant les transferts monétaires évoluent. Les transferts monétaires requièrent une coordination accrue des divers partenaires pour allier portée et durabilité. La coordination des parties prenantes implique différents ministères, diverses agences des Nations Unies, le Mouvement de la Croix-Rouge et du Croissant-Rouge, des ONG internationales et des organisations locales, avec leurs systèmes de données respectifs. Les transferts monétaires font intervenir des partenaires plus nombreux et requièrent souvent que les partenaires de mise en œuvre recourent à des systèmes établis de grande envergure, dont plusieurs proposent d'intégrer des technologies d'identité numérique (ID numérique) ou des données biométriques aux fins d'identification. Les transferts monétaires s'appuient de plus en plus sur les technologies numériques, si bien qu'il est probable que des banques, des opérateurs de téléphonie mobile, des institutions de microfinance et divers nouveaux prestataires de technologie financière participent également.

7 ELAN (2016) 'Data Starter Kit'.
8 Cash Learning Partnership (2020) 'State of the World's Cash 2020'.

ENCADRÉ 2: QU'EST-CE QUE LE RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES ?

Le Règlement général sur la protection des données (RGPD) de l'Union européenne est entré en vigueur en mai 2018. Il est considéré comme le règlement sur la confidentialité des données le plus strict au monde. La plupart des organisations implantées dans l'Union européenne sont tenues de respecter le RGPD, et de nombreux pays dans le monde s'inspirent du RGPD dans leurs propres réglementations nationales sur la confidentialité. Les Nations Unies et le CICR ne sont pas assujettis au RGPD, car ils bénéficient de certains privilèges et immunités en raison de leur statut d'organisations internationales.

La quantité de données recueillies, enregistrées, utilisées et partagées par les partenaires engagés dans les transferts monétaires est en constante augmentation. Parallèlement, de nouvelles lois ou des lois révisées sur la confidentialité des données comme le Règlement général sur la protection des données (RGPD) de l'Union européenne sont élaborées et adoptées dans de nombreux pays du monde. Ces lois imposent de nouvelles exigences aux organisations qui gèrent des données personnelles et d'autres formes de données sensibles. On assiste également à une sensibilisation accrue concernant l'importance d'une gestion sûre des données, notre devoir de protection, notre responsabilité à l'égard des participant-es aux programmes de prévention et protection et notre obligation à ne pas porter préjudice par la manière dont nous utilisons les données.

Dans ce contexte, nous proposons une Boîte à outils sur la gestion responsable des données mise à jour pour refléter ces grands changements.

ENCADRÉ 3 : QUELS TYPES DE DONNÉES CETTE BOÎTE À OUTILS COUVRE-T-ELLE ?

Dans ces fiches-conseils (inspirées de OCHA[9] et CICR[10]), le terme « données » inclut à la fois des données sensibles et non personnelles, notamment :

1. les données sur les personnes touchées par une crise et leurs besoins (par ex., données personnelles de bénéficiaires de transferts monétaires) ;
2. les données sur le contexte dans lequel une crise s'inscrit (par ex., informations sur les communautés bénéficiaires de transferts monétaires) ;
3. les données sur la réponse apportée par les organisations et les personnes cherchant à aider (par ex., emplacements des distributions d'espèces ou plans des exercices de collecte des données).

Les **données personnelles** sont des informations en lien avec une personne physique identifiée ou identifiable.

Les **données** sensibles sont des données qui, si elles sont divulguées ou communiquées sans autorisation appropriée, pourraient :

- nuire à une personne (sanctions, discrimination et menaces de sécurité), y compris à la source d'information ou à d'autres groupes ou personnes identifiables ;
- nuire à la capacité d'une organisation à mener ses activités ou ternir l'image de cette organisation aux yeux du public.

Les données présentent différents niveaux de sensibilité selon le contexte. C'est pourquoi le présent guide ne fournit pas une liste exhaustive des points de données sensibles.

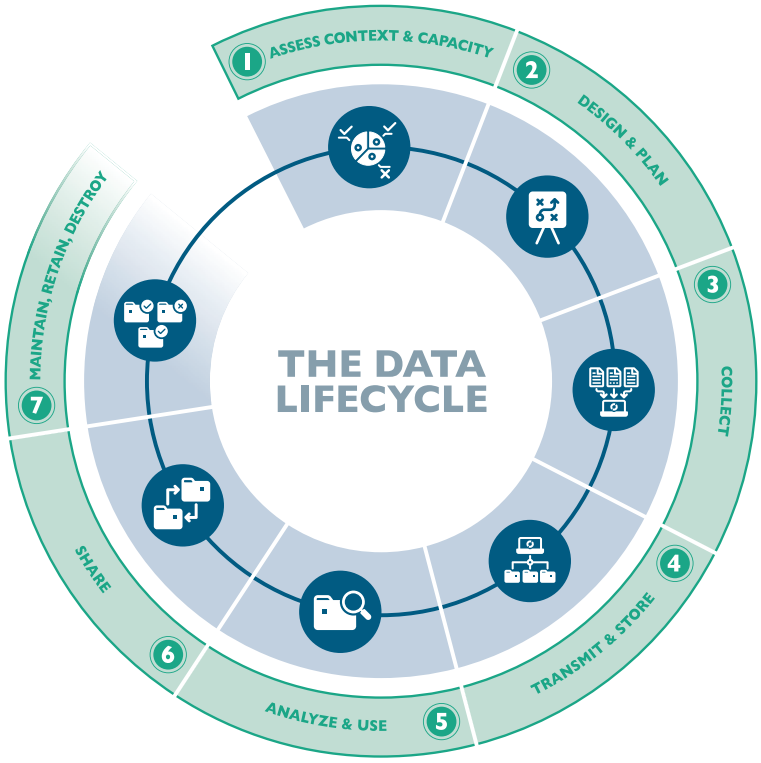
9 OCHA (2019), 'Data Responsibility Guidelines: Working Draft'.
10 CICR (2020), 'Data Protection Handbook'.

COMMENT CETTE BOÎTE À OUTILS EST-ELLE STRUCTURÉE ?

Dans cette boîte à outils, nous abordons la gestion responsable des données dans le cadre des transferts monétaires à travers le prisme du cycle de vie des données. Il convient de préciser que le cycle de vie des données n'est pas une simple boucle. Il s'agit plutôt d'une représentation visuelle contribuant à une réflexion holistique sur les données. Nous vous invitons à revoir le cycle de vie des données au fil du développement de votre programme et de la mise en œuvre d'activités supplémentaires en matière de données.

ENCADRÉ 4: LE CYCLE DE VIE DES DONNÉES

Le cycle de vie des données est utile pour orienter toutes les activités en matière de données dans le cadre d'une intervention globale et pour les activités de recueil des données individuelles au cours des différentes phases d'une intervention. (Le cycle de vie exposé ici est fourni à titre d'exemple. Les organisations peuvent disposer de leur propre version du cycle de vie des données.)



Pour faciliter son utilisation, cette boîte à outils s'articule en 7 fiches-conseils qui traitent des problématiques du contexte et de la capacité organisationnelle, de la conception et de la planification, ainsi que de la mise en œuvre. En résumé, les fiches-conseils couvrent les thématiques suivantes :

CONTEXTE ET CAPACITÉ ORGANISATIONNELLE (FICHE-CONSEIL 1)

Tôt dans le processus, des décisions de haut niveau doivent être prises pour déterminer si les organisations ont la capacité de déployer des transferts monétaires de manière éthique et sûre. Cela inclut d'évaluer le panorama des données, le contexte national, le contexte juridique et les rapports de force en lien avec les données dans les transferts monétaires. Il s'agit également d'évaluer les aspects de conformité, les rapports entre les données et les systèmes qui seront utilisés (et souvent exigés) par les bailleurs, les consortiums, les agences des Nations Unies, le Mouvement de la Croix-Rouge et du Croissant-Rouge, les ONG nationales et internationales, les gouvernements, les prestataires de services financiers et les autres partenaires engagés dans des programmes de transferts monétaires. À ce stade, l'évaluation de la capacité organisationnelle inclut les compétences, les connaissances et les ressources requises pour protéger les données et utiliser les processus et les outils numériques de manière responsable dans le contexte susmentionné. De nombreux aspects présentés dans la Fiche-conseil 1 peuvent être intégrés dans les études existantes d'analyse de la situation et de préparation aux transferts monétaires.

ENCADRÉ 5: JURIDIQUE VS ÉTHIQUE

Sur le plan juridique, la question est *pouvons-nous* faire cela ? Sur le plan éthique, la question est *devrions-nous* faire cela ? Il se peut qu'une intervention légale ne soit pas éthique.

CONCEVOIR ET PLANIFIER (FICHE-CONSEIL 2)

La phase de conception et de planification aide les organisations à définir leur approche en matière de recueil et de gestion responsables des données au cours des différentes étapes du cycle d'un programme de transferts monétaires (ciblage, inscription et enregistrement, acheminement et MEAL). Chaque étape du cycle d'un programme de transferts monétaires est susceptible d'exiger un type de recueil, de saisie et de gestion des données au cours du cycle de vie des données. Par exemple, les évaluations des besoins et de la vulnérabilité sont généralement menées à un stade précoce pour permettre aux agences de comprendre les besoins spécifiques des populations affectées. Ces évaluations doivent éclairer les décisions ultérieures quant aux modalités de transferts monétaires les plus pertinentes d'après le contexte, le volume et la fréquence des transferts, les partenariats et l'implication de tierces parties, et le processus dans son ensemble, notamment les données à recueillir et leur mode de collecte ou encore les systèmes à utiliser pour l'analyse et le stockage des données. Les aspects couverts au cours de cette phase sont conformes aux phases de conception des programmes et d'analyse d'une intervention de transferts monétaires type.

GESTION DES DONNÉES PENDANT LA MISE EN ŒUVRE (FICHES-CONSEILS 3–7)

Après les phases de conception et de planification, l'intervention passe au stade de la mise en œuvre. Lors de la phase de mise en œuvre des transferts monétaires, les organisations collectent des données auprès des populations affectées aux fins de ciblage, d'inscription, d'enregistrement et d'acheminement des transferts monétaires[11]. Elles réalisent également des activités de suivi et compilent le feedback des populations affectées pour renforcer la redevabilité et adapter les efforts déployés dans le cadre des programmes. Au cours de la phase de mise en œuvre, le recueil des données devient plus fréquent et plus détaillé. Les risques et les dommages peuvent être exacerbés par les volumes conséquents de données personnelles et d'autres formes de données sensibles ou de données groupées qui sont gérées et partagées. Les agences doivent aussi tenir compte de ce qu'il advient des données des populations affectées à la fermeture d'un programme ou si la gestion d'un programme est déléguée à une autre entité, comme lorsque les programmes de transferts monétaires humanitaires sont transférés à des organismes de protection sociale du gouvernement ou à d'autres partenaires du secteur du développement.

Le recours à une approche fondée sur le cycle de vie des données pour orienter le recueil et la gestion des données générales du programme et pour planifier et mettre en œuvre les processus de recueil et de gestion des données spécifiques aux différentes étapes de la mise en œuvre des transferts monétaires peut aider les organisations à optimiser les avantages des données et à identifier et atténuer les risques et les dommages pendant la mise en œuvre. Les organisations peuvent utiliser les Fiches-conseils 3–7 pour élaborer des plans pour chaque étape du cycle de vie, puis reprendre la finalisation de la conception et de la planification des données (Fiche-conseil 2).

11 Les programmes avec des espèces ont tendance à impliquer le recueil et le traitement de volumes de données plus importants, une plus grande coordination interinstitutions et un plus haut niveau de partage des données, tandis que ceux basés sur des coupons impliquent un moindre partage des données car ils sont souvent gérés en interne et requièrent moins de partage des données et de coordination avec les autres acteurs des transferts monétaires.

LISTE DES ACRONYMES

AAP	Redevabilité vis-à-vis des populations affectées (de l'anglais Accountability to Affected Populations)
AML	Lutte contre le blanchiment d'argent (de l'anglais Anti Money Laundering)
CaLP	Cash Learning Partnership
CDR	Enregistrements des détails des appels (de l'anglais Call Detail Record)
CTM	Mesures anti-terroristes (de l'anglais Counter-Terrorism Measures)
CVA	Transferts monétaires (de l'anglais Cash and Voucher Assistance)
CWG	Groupe de travail sur les transferts monétaires (de l'anglais Cash Working Group)
DPIA	Évaluation de l'impact sur la confidentialité des données (de l'anglais Data Privacy Impact Assessment)
DPO	Agent de protection des données (de l'anglais Data Protection Officer)
FATF	Groupe d'action financière
FSP	Prestataire de services financiers
GDPR	Règlement général sur la protection des données
ICRC	Comité international de la Croix-Rouge
ID	Identification
INGO	Organisation non gouvernementale internationale
KYC	Connaissance de la clientèle (de l'anglais Know Your Customer)
LI	Intérêts légitimes
MEAL	Suivi, évaluation, redevabilité et apprentissage (de l'anglais Monitoring, Evaluation, Accountability and Learning)
MNO	Opérateur de téléphonie mobile (de l'anglais Mobile Network Operator)
NGO	Organisation non gouvernementale
OCHA	Bureau pour la coordination des affaires humanitaires (de l'anglais Organization for the Coordination of Humanitarian Affairs)
PEA	Analyses d'économie politique (de l'anglais Political Economy Analyses)
PI	Mission d'intérêt public
PIA	Évaluation de l'impact sur la confidentialité (de l'anglais Privacy Impact Assessment)
RCRCM	Mouvement de la Croix-Rouge et du Croissant-Rouge (de l'anglais Red Cross Red Crescent Movement)
RBA	Évaluation des risques et des avantages (de l'anglais Risk Benefits Assessment)
SCOPE	Système d'enregistrement des bénéficiaires du Programme alimentaire mondial
SOP	Procédures opérationnelles standard
WFP	Programme alimentaire mondial
UN	Organisation des Nations Unies
UNHCR	Haut Commissariat des Nations Unies pour les réfugiés
UNICEF	Fonds des Nations Unies pour l'enfance (de l'anglais United Nations Children's Fund)

FICHE-CONSEIL 1

ÉVALUER LE CONTEXTE ET LA CAPACITÉ

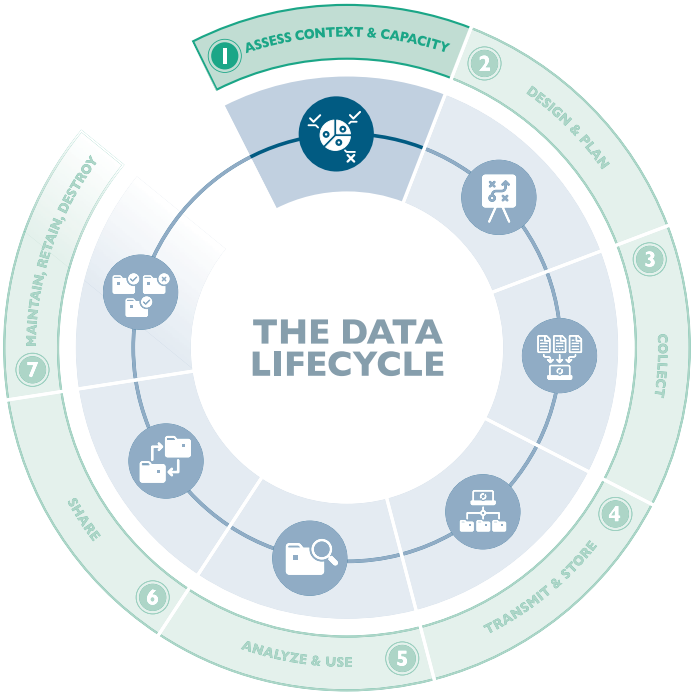
Lors de la planification d'un programme, notamment d'un programme impliquant des transferts monétaires, vous devrez évaluer le contexte global dans lequel vous intervenez et la capacité de votre organisation avant de passer à une planification plus détaillée. À ce stade, vous devrez déterminer si votre organisation peut mener un programme de façon sûre et éthique dans un contexte particulier.

Cette évaluation de haut niveau doit inclure un examen de vos obligations et capacités à recueillir et à gérer de manière responsable les données requises aux fins du programme. Elle devrait aussi inclure des évaluations réglementaires, des évaluations de la faisabilité, une analyse des services financiers et de la liquidité, un examen des stratégies des bailleurs et d'autres considérations importantes.

À ce stade, l'évaluation du contexte et des capacités en lien avec les données permet de s'assurer que vous pouvez recueillir, traiter et gérer de façon responsable les données nécessaires au déploiement du programme, ainsi que d'identifier d'éventuels compromis dans l'optique de prendre des décisions importantes. Une évaluation de haut niveau des points spécifiés ci-dessous contribue à déterminer si vous êtes à même de formuler une proposition ou d'entreprendre une intervention de manière responsable. Si, à l'occasion du premier examen, les risques et les dommages en lien avec les données (pour les populations affectées, votre organisation, les partenaires ou le personnel) l'emportent sur les avantages, il convient de revoir toutes les étapes du programme (conception, négociation, réflexion) avant de soumettre une proposition. Les domaines clés ci-dessous sont peut-être déjà inclus dans vos processus habituels de recherche avant proposition et de prise de décisions. Nous les répertorions toutefois ici, car les organisations accordent rarement une attention suffisante à la gestion responsable des données dans le cadre de leurs processus précédant une proposition.

IDENTIFIER LES PRINCIPES DE HAUT NIVEAU QUI DÉFINISSENT L'APPROCHE DE VOTRE ORGANISATION

Les acteurs humanitaires ont déjà développé ou adopté plusieurs séries de principes susceptibles de vous aider dans votre réflexion de haut niveau sur la gestion responsable des données dans les programmes de transferts monétaires. Votre organisation peut suivre un ou plusieurs de ces principes, ou suivre ses propres principes. Les principes de haut niveau peuvent vous aider à définir ultérieurement les « lignes rouges » au niveau opérationnel que votre organisation refuse de franchir, ainsi que les aspects qui entrent en jeu dans vos décisions « feu vert/feu rouge ».



La fiche-conseil 1 oriente sur la façon d'évaluer le contexte et la capacité en lien avec les données avant de se lancer dans un programme de transferts monétaires. La capacité et les ressources de votre organisation détermineront le niveau de détail et de rigueur de votre approche lors de ces évaluations. Même si vos ressources sont limitées, il est important d'inclure a minima chacun de ces domaines dans des évaluations rapides, car votre évaluation du contexte et de la capacité peut révéler qu'il ne serait pas judicieux de poursuivre.

- *Protéger la vie privée des bénéficiaires : Principes et normes opérationnelles (2013)*
- *Principles for Digital Payments in Humanitarian Response (2015)*
- *UN Personal Data Protection and Privacy Principles (2018)*
- *EU's General Data Protection Regulation (GDPR) Data Protection Principles (2018)*
- *ICRC Data Processing Principles (2020), pages 35–43*

Les principes doivent être intégrés dans les processus opérationnels. À mesure que vous explorez cette boîte à outils, examinez et déterminez si les principes et les politiques de votre organisation sont conformes à vos opérations. Y a-t-il des documents translationnels ou des étapes (listes de contrôle, cadres d'évaluation des risques ou outils de tri en lien avec une gestion responsable des données, par ex.) à intégrer dans les processus existants ? Avez-vous identifié une personne susceptible de vous conseiller en cas de questions ?

Certaines organisations peuvent envisager de créer un comité éthique interne sur la question des données qui examine les programmes afin de déterminer, entre autres aspects, si les données sont utilisées de manière éthique. Voici quelques recommandations pour **créer un comité éthique** afin de déterminer si la technologie et les données sont utilisées de façon responsable.

COMPRENDRE L'ÉCONOMIE POLITIQUE DES DONNÉES DANS VOTRE CONTEXTE OPÉRATIONNEL

Les données confèrent un pouvoir. Dans la plupart des contextes humanitaires, l'entité qui contrôle la majorité des données a le plus de pouvoir et prend le contrôle de l'intervention. Autrement dit, les agences peuvent se livrer concurrence sur les données et promouvoir l'adoption de certains systèmes afin de centraliser leur gestion. Les agences qui détiennent le plus de données ou qui promeuvent leurs systèmes comme modèle par défaut sont en meilleure posture pour obtenir un financement. Les entités qui disposent de grandes quantités de données sont également mieux placées pour négocier plus facilement avec les autorités locales lorsque des transferts monétaires humanitaires sont intégrés dans les efforts publics de protection sociale. Face à la raréfaction des fonds consacrés à l'aide, les données sont une source de tension du fait du pouvoir et des financements qu'elles peuvent attirer.

ENCADRÉ 6: QU'EST-CE QU'UNE « ANALYSE DE L'ÉCONOMIE POLITIQUE » ?

Une analyse de l'économie politique (PEA) permet d'examiner de manière structurée les rapports de force et l'influence des forces économiques et sociales dans un contexte particulier. Il s'agit d'un processus visant à comprendre les dynamiques contextuelles et la façon dont les différentes interventions ou interventions prospectives (y compris dans le domaine humanitaire) peuvent interagir et influer sur ces dynamiques. La PEA intègre une réflexion sur les aspects suivants :

- influences fondamentales (histoire ou géographie, par ex.) ;
- impact des acteurs et des événements immédiats (changements de leadership ou catastrophes naturelles, par ex.) ;
- et cadre institutionnel (englobant la législation formelle et les pratiques informelles) façonnant les comportements et les résultats observés.

Une PEA encourage les professionnel-le-s à tenir compte de ces dynamiques, motivations et intérêts et à réfléchir sur la façon dont ces facteurs peuvent éclairer les pratiques opérationnelles. Les acteurs des transferts monétaires peuvent vouloir couvrir le contexte national ou régional, ainsi que les rapports de force et les forces économiques et sociales en jeu au sein d'une intervention humanitaire, y compris dans le cas de transferts monétaires[12].

Les données intéressent également les gouvernements, pour diverses raisons. Ceux-ci peuvent en faire un usage bénéfique pour améliorer les programmes et éclairer la prise de décisions, ou plus discutable pour manipuler les listes de destinataires des transferts monétaires, engager une lutte de pouvoir avec les acteurs non étatiques lors de conflits, ou encore pour cibler des groupes ou des personnes en vue de leur nuire. Le secteur privé et les prestataires de services financiers (PSF) peuvent également souhaiter accéder aux données pour cibler de nouveaux prospects avec des produits et des services, mener des travaux de R&D pour de nouveaux produits ou monétiser des données en les revendant à d'autres.

Il est important de comprendre le rôle joué par les données dans votre contexte professionnel pour identifier les risques et les dommages potentiels pouvant découler de la collecte, du traitement et du partage des données. Cela peut à son tour contribuer à mettre en lumière des domaines présentant une marge de négociation pour une gestion plus responsable des données. La réalisation d'une analyse de l'économie politique (PEA) des données en lien avec les transferts monétaires permet d'identifier les dynamiques sous-jacentes qui influent sur l'accès aux données et leur contrôle. Une PEA des données peut être réalisée par un agent de contrôle indépendant, un-e consultant-e externe ou, dans certains cas, un partenaire du secteur privé. Des groupes de travail sur les transferts monétaires opérationnels peuvent servir de terrain neutre

12 Menocal, A. et. al (2018) 'Thinking and Working Politically through Applied Political Economy Analysis: A Guide for Practitioners'. USAID.

pour discuter des PEA des données et pour convenir d'approches collectives des données qui bénéficient aux populations affectées, plutôt que d'adopter des approches qui servent les priorités de certains gouvernements ou d'agences spécifiques. Les agences moins influentes souhaiteront éventuellement mener leur propre PEA des données et l'utiliser pour élaborer des stratégies leur permettant de mieux gérer les rapports de force dans le cadre des transferts monétaires. Il est aussi possible de réaliser une PEA du contexte général au sens large. Le cas échéant, celle-ci devra inclure une composante consacrée à la PEA des données.

ENCADRÉ 7: EXEMPLES DE QUESTIONS POUR MENER UNE PEA DES DONNÉES EN LIEN AVEC DES TRANSFERTS MONÉTAIRES[13]

- **Rôles et responsabilités.** Qui sont les parties prenantes clés ? Quels sont les mandats et les rôles formels et/ou informels des différents acteurs ? Comment s'articule le contrôle des données entre les différents acteurs ?
- **Financement et structure de propriété.** Quelle est la structure d'un programme de transferts monétaires ? Comment s'articulent l'accès aux données et leur contrôle entre les agences, les gouvernements et d'autres acteurs ? Comment les transferts monétaires sont-ils financés et par qui ? Quels sont les intérêts des entités qui financent les transferts monétaires ? Comment sont-ils influencés par d'autres intérêts (par ex., austérité, considérations relatives à la fraude et au financement par les contribuables, alliances au niveau mondial et intérêts particuliers de certains pays dans le développement ou la situation politique d'autres pays) ? Si une agence détient et finance tous les transferts monétaires, qu'est-ce que cela signifie en termes de gestion responsable des données ?
- **Rapports de force.** Dans quelle mesure le pouvoir conféré est-il aux mains de personnes, d'agences ou de groupes spécifiques ? Comment les différents groupes d'intérêts (PSF, agences des Nations Unies, RCRCM, ONGI, ONG, entreprises spécialisées dans les technologies ou les données, populations affectées, gouvernements, médias, régulateurs, etc.) cherchent-ils à influer sur la façon dont les données sont gérées et sur qui y accède et les contrôle ?
- **Héritages historiques.** Quels sont les antécédents des différents acteurs dans ce contexte de programmation ou dans le pays ? Quelles sont les relations historiques des différents acteurs ? Comment cela influence-t-il les perceptions actuelles des parties prenantes ?
- **Corruption et recherche de profits.** La corruption, la fraude et la recherche de profits sont-elles répandues dans le secteur humanitaire, dans les programmes de transferts monétaires ou dans le pays en général ? Quel rôle les données jouent-elles à cet égard ? Quand ces pratiques sont-elles les plus fréquentes (par ex., au moment du ciblage, de l'inscription, de l'acheminement ou de l'approvisionnement) ? À qui la situation profite-t-elle le plus ? Cela donne-t-il lieu à du népotisme ?
- **Acheminement des transferts monétaires.** Qui sont les principaux bénéficiaires de l'acheminement de transferts monétaires ? Certains groupes sociaux, régionaux ou ethniques sont-ils inclus et/ou exclus ? Des subventions sont-elles accordées, et quels groupes en bénéficient le plus ?
- **Idéologies et valeurs.** Quelles sont les idéologies et les valeurs dominantes qui façonnent les opinions dans le secteur humanitaire ou dans les transferts monétaires ? Dans quelle mesure celles-ci peuvent-elles être utilisées pour influer sur le mode d'acheminement des transferts monétaires ?
- **Prise de décisions.** Comment les décisions sont-elles prises dans le secteur humanitaire ou dans les transferts monétaires ? Qui participe à ces processus décisionnels ?
- **Questions tenant à la mise en œuvre.** Une fois les décisions prises, sont-elles mises en œuvre. Quels sont les principaux goulots d'étranglement du système ? L'échec de la mise en œuvre est-il dû à des capacités insuffisantes ou à d'autres raisons d'économie politique ?
- **Potentiel de réforme.** Qui devraient être les « gagnant-e-s » et les « perdant-e-s » des décisions prises concernant l'accès aux données et leur contrôle ? Qui est susceptible de remettre en cause le statu quo et qui pourrait s'opposer au changement, et pourquoi ? Quels éléments pourraient être négociés pour surmonter cette opposition ?

Selon la situation, vous pouvez mener une PEA plus formelle (par ex., en recrutant un tiers ou en vous entendant avec des partenaires pour en réaliser une conjointement). Sinon, si votre équipe est expérimentée dans les transferts monétaires et selon le contexte, vous pouvez organiser un atelier PEA auquel participe un groupe diversifié d'acteurs des transferts monétaires pour identifier et évaluer les thèmes clés.

Idéalement, une PEA des données (ou les enseignements qui en découlent) doit être intégrée dans votre analyse de la situation des transferts monétaires, dans l'étude de faisabilité et de l'adéquation des transferts monétaires, ainsi que dans l'évaluation des risques-avantages-dommages. Elle doit guider les décisionnaires de votre organisation sur les questions en lien avec les données à prendre en compte avant de signer un contrat ou un accord et de s'engager dans une intervention (par ex., une décision « feu vert/feu rouge »). Un certain degré de plaidoyer pourra être nécessaire en interne pour aider les décisionnaires à mieux appréhender la nécessité d'être « prêt sur le plan des données » avant de s'engager dans des transferts monétaires.

13 Adapté du document Guidance Note on Use of Political Economy Analysis for ADB Operations de la Banque asiatique de développement (2009). Reportez-vous à la publication complète pour plus d'informations sur la PEA. Sources : J. Moncrieffe et C. Luttrell (2005), An Analytical Framework for Understanding the Political Economy of Sectors and Policy Arenas. Londres : Overseas Development Institute ; V. Fritz, K. Kaiser et B. Levy (2009), Problem-Driven Governance and Political Economy Analysis: Good Practice Framework. Washington, DC : Banque mondiale.

IDENTIFIER LES CADRES NATIONAUX SUR LA CONFIDENTIALITÉ DES DONNÉES ET LES AUTRES CADRES JURIDIQUES EN VIGUEUR

De plus en plus de pays développent ou mettent à jour des lois sur la confidentialité des données pour s'adapter aux nouvelles réalités des sociétés numériques. Les acteurs des transferts monétaires doivent connaître ces lois et veiller à les respecter. L'examen des réglementations sur les données fait peut-être partie de votre évaluation réglementaire standard. Dans le cas contraire, veuillez parcourir les domaines ci-dessous. Bien que les mécanismes de redevabilité relatifs aux lois sur la confidentialité des données puissent être faibles dans certains contextes, toute violation d'une loi sur la confidentialité des données peut entraîner des sanctions ou des interdictions d'exploitation pour une organisation.

Les agences implantées en Europe peuvent être assujetties au Règlement général sur la protection des données (RGPD) de l'Union européenne, qui est considéré comme offrant le cadre de protection des données le plus strict au monde. Les agences comme les Nations Unies et le CICR jouissent de cadres de protection juridique spécifiques qui les aident à garantir la confidentialité et la neutralité de leurs opérations14. Si cette immunité les affranchit du RGPD, les Nations Unies et le CICR disposent de leurs propres politiques de protection des données qu'ils sont tenus de respecter.

La gestion de plusieurs juridictions dans une même intervention peut se révéler complexe. La concertation des équipes juridiques, la cartographie des données transfrontalières et l'identification des populations concernées peuvent vous aider à respecter ces lois et combinaisons de lois. Certains pays (comme le Bangladesh et les Philippines) sont soumis à des exigences contraires au RGPD. Par ailleurs, certaines réglementations exigent que des évaluations de l'impact sur la confidentialité des données (DPIA) soient réalisées si certains seuils sont atteints, selon le type et la quantité de données recueillies et traitées, ainsi que le degré de sensibilité des données, ou si les données sont collectées auprès de populations vulnérables. Elles peuvent également exiger des évaluations qui démontrent que le recueil et le traitement des données ne causent pas de dommages ni n'enfreignent d'autres droits, notamment en matière de confidentialité.

Certaines législations nationales incluent des réglementations en lien avec la transmission des données. La transmission des données peut s'effectuer au sein ou entre les bureaux dans un même pays ou entre plusieurs pays. Dans tous ces cas, des règles spéciales existent pour protéger la confidentialité et la sécurité des données personnelles et sensibles qui sont transférées. Lorsque les transferts de données traversent les frontières, on parle de transfert de données transfrontalier. Certains pays ont adopté des lois qui visent à restreindre les transferts de données transfrontaliers. Par exemple, le Kenya a adopté une loi sur la localisation des données qui restreint les types de données qui peuvent être transférées en dehors du pays. L'UE dispose également de règles spécifiques quant au lieu et au moment où les données des citoyen-ne-s européen-ne-s peuvent être transférées en dehors de l'UE. Certains pays exigent qu'une copie des données soit stockée localement, que les données soient traitées dans le pays ou qu'un consentement du gouvernement soit obtenu avant que les données ne soient transférées. Les organisations internationales suivent également des règles quant au moment et à la façon dont un transfert transfrontalier peut survenir.

Dans certains cas, les organisations peuvent faire face à des risques associés avec la conservation des données enregistrées dans un pays, par exemple si un gouvernement persécute des personnes ou des groupes particuliers et si les données collectées peuvent être utilisées par les autorités pour identifier ou localiser ces groupes ou si la situation sécuritaire s'est détériorée au point que l'organisation n'estime plus pouvoir assurer la sécurité et la protection des données dans le pays. Le cas échéant, les organisations doivent arbitrer entre contrevenir à la législation ou exposer des personnes à des risques. Elles peuvent également décider d'éviter de recueillir des données dans ces cas précis.

ENCADRÉ 8: PRINCIPAUX ASPECTS À PRENDRE EN COMPTE CONCERNANT LA SÉCURITÉ ET LA CONFIDENTIALITÉ DES DONNÉES DANS LES RÉGLEMENTATIONS SUR LA CONFIDENTIALITÉ

- Types de données couverts dans les lois et les politiques
- Restrictions sur les types de données pouvant être collectées
- Nécessité de comprendre et d'évaluer le risque et l'impact sur les droits des personnes
- Règles spécifiques relatives aux données sur les enfants ou à d'autres données spéciales (comme les données biométriques)
- Spécifications sur le partage des données
- Responsabilités des personnes recueillant les données versus responsabilités des personnes traitant les données
- Restrictions déterminant si les données peuvent être transférées en dehors du pays
- Restrictions sur l'emplacement et le mode d'enregistrement admis des données ou sur la durée de conservation
- Règles déterminant si les gouvernements sont autorisés à accéder aux données
- Orientation sur la manière de recueillir et d'enregistrer un consentement
- Pénalités ou autres sanctions applicables en cas de mauvaise utilisation des données
- Droits des « sujets des données » (les personnes dont les données sont collectées ou traitées)
- Mécanismes requis pour gérer les réclamations
- Indications concernant quand, comment et à qui signaler une violation des données
- Obligations de recruter ou de désigner un agent de protection des données

14 Les privilèges et l'immunité dont jouissent le CICR et les agences des Nations Unies mettent ces dernières à l'abri de toute procédure judiciaire. Leurs locaux, documents et données sont également protégés de tout accès par les gouvernements dans les territoires où ils interviennent. Leur personnel est exempté de témoigner ou d'apporter des preuves lors des actions judiciaires. Voir par exemple la Convention sur les privilèges et immunités des Nations Unies (1946) et consulter Le point sur le statut juridique du CICR.

Outre les lois sur la confidentialité, la législation nationale résultant du travail du groupe d'action financière (GAFI)[15] ou les règles de diligence raisonnable vis-à-vis des consommateurs comme les exigences en matière de Connaissance de la clientèle (Know your customer ou KYC) peuvent imposer de collecter certaines informations pour réaliser des transferts d'espèces (reportez-vous à la Fiche-conseil 3 pour plus d'informations sur le GAFI et les exigences KYC).

Collaborez avec vos équipes juridiques, IT et de protection de la vie privée pour identifier les options en matière de stockage et de transmission des données. Déterminez où et comment les tiers avec lesquels vous travaillez transmettent et stockent les données.

La publication de l'ITIF **Cross-Border Data Flows: Where are the Barriers and What Do They Cost?** fournit une liste (en date de 2017) des pays ayant adopté des lois ou des politiques sur la localisation des données. Vous pouvez également consulter la page **Data Protection Laws of the World** (actualisée en permanence) de DLA Piper ou le document **Privacy is Paramount: Personal Data Protection in Africa** de Deloitte (2017).

Vous pouvez être amené-e à pondérer compromis et choix difficiles, par exemple si vous êtes légalement tenu-e de partager des données avec les gouvernements, mais craignez que cela expose les populations affectées à des risques ou influe sur le degré de confiance envers votre organisation. Reportez-vous au document du CaLP **Partage responsable des données avec les gouvernements**.

RECHERCHER LES EXIGENCES DE CONFORMITÉ DES SUBVENTIONS, DES SYSTÈMES ET DES DONNÉES DES BAILLEURS

Les bailleurs ont de plus en plus besoin que les acteurs des transferts monétaires se coordonnent et partagent des données. Les bailleurs peuvent également avoir des exigences spécifiques quant aux types de données que les agences doivent collecter et partager et quant à la manière dont est assurée la protection des données. En général, ces points sont mentionnés dans les contrats de subvention et influent sur la façon dont vos données sur les transferts monétaires peuvent être gérées et conservées. Par exemple, certains bailleurs publics exigent un contrôle des bénéficiaires de transferts monétaires ou la mise en conformité avec les mesures anti-terroristes ou les réglementations concernant la lutte contre le blanchiment d'argent, ce qui peut exposer des bénéficiaires de transferts monétaires à un risque en raison de la somme de données personnelles et sensibles collectées pour réaliser ces contrôles, d'un manque de clarté quant aux personnes/entités autorisées à accéder à ces bases de données, et du risque d'erreurs d'inclusion ou d'exclusion. D'autres exigent que certaines données programmatiques soient partagées dans des formats particuliers et selon un échéancier spécifique. Les organisations devront alors anonymiser les données ou intervenir sur celles-ci par un autre moyen avant de les partager afin de protéger les bénéficiaires de transferts monétaires. La recherche des exigences des bailleurs concernant les données peut déjà faire partie de vos évaluations de faisabilité. Il arrive toutefois que des organisations n'étudient pas assez rigoureusement les exigences spécifiquement en lien avec les données.

Par ailleurs, pour certains partenariats ou certaines subventions, les partenaires doivent saisir les données dans des systèmes propres aux Nations Unies, comme le système SCOPE du Programme alimentaire mondial[16], le système PRIME/ProGres du HCR[17] et/ou le système Primero de l'UNICEF[18]. Dans d'autres cas, le partage des données s'effectuera de manière bilatérale parmi les ONG par l'intermédiaire d'accords sur les mandats de consortiums, les structures de gouvernance et le partage des données. Les systèmes des Nations Unies sont souvent paramétrés pour collecter des données biométriques. Le partage des données et l'utilisation de ces systèmes sont sources de tension entre les agences des Nations Unies et certains partenaires de mise en œuvre qui doutent de la robustesse de ces plateformes en matière de protection et de sécurité des données. Certaines ONG ont exprimé leurs frustrations concernant les rapports de force déséquilibrés, la marge de négociation sur les exigences des Nations Unies et les privilèges et immunités des Nations Unies. La question du partage des données et l'utilisation de ces systèmes de données sont omniprésentes dans les conversations et négociations en cours. À l'heure actuelle, le PAM, le HCR et l'UNICEF cherchent des moyens de rendre leurs systèmes interopérables entre eux et avec les gouvernements, suscitant l'inquiétude des partenaires de mise en œuvre en matière de gestion responsable des données.

En amont de toute proposition, il est important de comprendre les exigences des bailleurs et si ces dernières sont conformes à ce que votre organisation souhaite ou ne souhaite pas mettre en place. En menant vos recherches avant de formuler la proposition, vous pouvez décider ou non de poursuivre et/ou d'entamer des négociations sur les exigences des bailleurs.

De nombreux bailleurs se déclarent ouverts et disposés à revoir leurs exigences en matière de données face à des préoccupations légitimes. En effectuant vos recherches, puis en structurant et en documentant vos préoccupations, vous disposerez de plus d'arguments pour négocier avec un bailleur.

Vous pouvez rencontrer une certaine résistance de la part d'autres services de votre organisation qui sont moins sensibilisés aux risques que les données peuvent poser lors de la mise en œuvre. Il est important de créer des alliances au sein de votre organisation afin de promouvoir une meilleure protection et une gestion responsable des données, et d'identifier des moyens d'inclure des équipes alliées (prévention et protection, juridique, IT et cybersécurité, par ex.) pour soutenir davantage une gestion responsable des données.

15 Voir Groupe d'action financière (2012), Normes internationales sur la lutte contre le blanchiment de capitaux et le financement du terrorisme et de la prolifération : Les Recommandations du GAFI.
16 Voir WFP SCOPE.
17 Voir la page Guidance on Registration and Identity Management - 3.6 Registration tools - Population Registration and Identity Management Eco-System (PRIMES) du HCR.
18 Voir le site Web Primero de l'UNICEF.

ANALYSER LA CAPACITÉ DE GESTION DES DONNÉES DANS L'ORGANISATION

Les interventions humanitaires, notamment les transferts monétaires, dépendent de plusieurs facteurs, et le maillon le plus faible détermine le niveau de sécurité de la protection des données. Il devient primordial de renforcer les pratiques et les politiques de protection des données car les organisations et les interventions deviennent de plus en plus numérisées, avec un recueil et un partage de plus grands volumes de données sensibles.

Les capacités de gestion des données varient selon les organisations. Cela ne dépend pas de l'envergure de l'organisation, mais plutôt de l'importance qu'elle accorde à ce domaine et de son accès durable à un financement institutionnel afin d'améliorer les systèmes et l'infrastructure des données. **Il est essentiel que les organisations s'abstiennent de collecter des données dont elles ne peuvent pas assurer la sécurité. Il s'agit là d'une règle d'or en matière de gestion responsable des données.**

Une analyse organisationnelle peut vous aider à déterminer si votre organisation et vos partenaires potentiels ont la capacité de gérer les données de manière responsable dans le contexte où vous intervenez. Cette analyse doit être réalisée avant tout engagement formel à acheminer des transferts monétaires dans un contexte donné.

Vous pouvez réaliser une évaluation approfondie de la maturité de votre organisation (ou de celles de vos partenaires) en matière de données à l'aide du **modèle de maturité relatif à la gestion responsable des données pour les organisations humanitaires et de développement** développé pour CARE. Une analyse organisationnelle élargie et un plan de renforcement requièrent du temps et des investissements à long terme.

Si votre organisation n'est pas à même de mener une évaluation complète ou distincte, vous devez inclure une section dédiée aux capacités de gestion responsable des données dans votre évaluation générale de la faisabilité des transferts monétaires. Le modèle dans l'Encadré 9 ci-dessous peut vous aider à identifier les questions clés à inclure.

Cette **liste de contrôle imprimable d'Electronic Frontier Foundation** peut vous aider à évaluer la capacité d'un partenaire en charge du traitement des données en matière de confidentialité et de sécurité des données. Elle peut également servir à évaluer un tiers ou un PSF.

Cette **série de questions** aide à déterminer la conformité d'un tiers ou d'un prestataire à l'égard du RGPD.

DÉCIDER D'UN « FEU VERT/FEU ROUGE »

À la lumière des recherches et des évaluations susmentionnées, qui visent à mieux cerner votre contexte et vos capacités, déterminez à un haut niveau s'il convient ou non de faire une proposition, d'entamer un partenariat ou de s'engager dans une intervention donnée.

Comme indiqué plus haut, si votre organisation mène déjà des évaluations de la faisabilité, de la capacité ou des risques, les points ci-dessus peuvent y être intégrés. Il est important d'évaluer tout particulièrement la gestion responsable des données pour s'assurer qu'elle est prise en compte dans le processus décisionnel. Il peut s'agir d'un nouveau point à étudier pour votre organisation, susceptible d'exiger un plaidoyer auprès des décisionnaires afin qu'il soit débattu avant la phase de proposition. **Il est important de souligner que certains projets peuvent être interrompus après cette analyse initiale ou devront identifier des modalités qui n'impliquent pas de recueillir des données sensibles si l'organisation ou l'intervention ne dispose pas des capacités requises pour les collecter en toute sécurité.**

Si votre organisation n'a pas encore défini un modèle ou un processus pour déterminer la marche à suivre d'après la capacité et le contexte en matière de données, vous pouvez utiliser le modèle fourni dans l'Encadré 9 ci-après. Lorsque vous complétez le modèle, déterminez votre position actuelle et recommandez des mesures d'atténuation susceptibles de faire la différence entre un « feu rouge » et un « feu vert ». Si un processus est en place, les questions ci-dessous peuvent être intégrées pour s'assurer que vos évaluations initiales couvrent la gestion responsable des données.

ENCADRÉ 9: ÉVALUATION RAPIDE POUR DONNER UN « FEU VERT/FEU ROUGE »

Si aucun processus n'est en place dans votre organisation ou si vous avez besoin d'un modèle d'évaluation rapide, cet outil « feu vert/feu rouge » peut être utile. Utilisez-le pour évaluer votre niveau de confiance dans le fait que votre organisation peut gérer les données de manière responsable dans le contexte de cette intervention. Dans les cases, indiquez pourquoi vous êtes confiant-e (ou non) et suggérez des stratégies à mettre en place pour renforcer la confiance, par exemple en évaluant les compétences, la capacité et les ressources. Utilisez les réponses pour éclairer vos décisions « feu vert/feu rouge » ou partagez-les avec les personnes qui négocient une participation à une subvention. Vous devez essayer d'obtenir les contributions d'un groupe diversifié, avec du personnel des équipes juridique, prévention et protection, IT et cybersécurité, données ou MEAL, et du personnel de première ligne. Votre agent de protection des données et le comité d'éthique (ou autre entité similaire) doivent réviser ce modèle et l'utiliser pour éclairer la prise de décisions. Ce modèle peut également être utilisé pour évaluer vos niveaux de confiance en vos partenaires.

NIVEAUX DE CONFIANCE (compétences, capacité, ressources)	**FAIBLE**	**MOYEN**	**ÉLEVÉ**
Nous savons comment les données seront utilisées et avons identifié toutes les parties qui accéderont aux données			
Nous avons étudié la faisabilité d'une intervention dans ce contexte sans exposer les bénéficiaires des transferts monétaires, notre organisation ou le personnel à des niveaux inacceptables de dommages imputables aux données			
Nous pouvons nous conformer aux cadres juridiques nationaux et mondiaux			
Nous pouvons garantir la sécurité des données tout en respectant les cadres juridiques nationaux et mondiaux			
Nous pouvons nous conformer aux exigences des bailleurs en matière de protection des données			
Nous pouvons garantir la sécurité des données tout en fournissant aux bailleurs les données dont ils ont besoin			
Nous pouvons garantir la sécurité des données dans les systèmes que les bailleurs ou les partenaires nous demandent d'utiliser			
Nous savons gérer les systèmes que l'on nous demande d'utiliser			
Nous sommes en mesure de gérer les données de manière responsable dans ce contexte			
Nos partenaires sont en mesure de gérer les données de manière responsable dans ce contexte			

FICHE-CONSEIL 2

CONCEVOIR ET PLANIFIER

Une fois une décision de haut niveau prise pour déterminer si le contexte opérationnel, la capacité organisationnelle et les conditions en lien avec les données permettent de déployer un programme de transferts monétaires responsable (d'après la Fiche-conseil 1), il convient d'élaborer un plan de collecte et de gestion des données pour l'intervention globale. Les évaluations du contexte et de la capacité évoquées dans la Fiche-conseil 1 seront exploitées lors de cette phase, pendant laquelle vous allez concevoir votre proposition de transferts monétaires et déterminer la façon dont les données seront gérées tout au long de l'intervention (les Fiches-conseils 3–7 permettent de définir en détails chaque étape du cycle de vie des données). Lors de cette phase, vous pouvez également être amené-e à réaliser des évaluations de la faisabilité des transferts monétaires, à procéder à un autre examen de la réglementation, à évaluer le marché, le PSF, les besoins et la vulnérabilité, et à prendre des décisions quant aux modalités de transferts monétaires les mieux adaptées et les plus sûres dans le contexte[19].

Il s'agira d'identifier les partenaires et les autres tierces parties avec lesquels vous travaillerez, les systèmes que vous utiliserez, la conception du processus global et si les transferts monétaires humanitaires peuvent être reliés aux systèmes de protection sociale du gouvernement. Tous ces efforts doivent s'accompagner d'une évaluation de la gestion responsable des données.

Parallèlement, divers facteurs en lien avec une gestion responsable des données doivent éclairer les décisions sur la conception et la mise en œuvre d'un programme et permettre de déterminer si le recueil de certains types de données est sûr ou si le risque associé aux données est trop élevé pour les populations affectées, le personnel de première ligne, les enquêteurs/trices ou pour votre organisation dans son ensemble.

Lors de la phase de conception et de planification, vous définirez chacun des processus de traitement des données prévus tout au long de l'intervention, de l'évaluation des besoins au feedback des populations affectées, en passant par le ciblage, l'inscription et l'enregistrement ou encore le transfert à l'équipe MEAL, et vous préciserez comment vous allez gérer les données de façon responsable. La conception et la planification d'une gestion responsable des données vous permettra de cerner ce à quoi ressemblera votre intervention avec une approche mature et responsable de la gestion des données, de procéder à des ajustements en fonction du temps et du financement dont vous disposez et d'identifier les domaines qui doivent être progressivement améliorés.

Idéalement, à mesure que vous renforcez les capacités, les compétences et les pratiques, la gestion responsable des données devrait s'apparenter davantage à un état d'esprit qu'à une contrainte.

La Fiche-conseil 2 couvre la conception et la planification. Vous aurez réalisé le gros du travail dans la Fiche-conseil 1. Vous devez désormais entrer dans les détails pour définir ce à quoi ressemblera votre intervention dans la pratique. Ces éléments seront utilisés dans l'élaboration de la proposition, la budgétisation, la sélection des partenaires et d'autres décisions en lien avec la planification.

19 Reportez-vous au document « Cash Minimum Standards Policy » de Mercy Corps pour avoir une vue d'ensemble des différentes évaluations et normes que Mercy Corps intègre à chaque phase d'un programme de transferts monétaires.

DÉTERMINER SI VOUS UTILISEREZ LES DONNÉES EXISTANTES OU COLLECTEREZ DE NOUVELLES DONNÉES

Dans le cadre de votre processus de conception et de planification, vous devrez déterminer s'il est nécessaire de collecter de nouvelles données ou si les listes ou les ensembles de données existants peuvent être utilisés pour le ciblage, l'inscription ou l'acheminement. Si ces listes sont obsolètes ou de piètre qualité, si elles ont été altérées de manière non autorisée ou si elles ne couvrent qu'une partie de la population, elles doivent être complétées par des données supplémentaires ou par un nouveau recueil de données. Le risque de doublons entre les données des listes nouvelles et existantes peut poser problème. Le cas échéant, vous devrez comparer les listes et évaluer la situation. Si les systèmes ne sont pas interopérables, cette comparaison peut être compliquée. Dans certaines interventions, une organisation ou une agence a peut-être déjà comparé et compilé des listes et des données. Il peut toutefois être judicieux de demander que ces données soient mises à jour, que leur qualité soit examinée ou qu'elles soient plus inclusives.

Si votre intervention est associée à un programme de protection sociale existant, il sera indispensable d'harmoniser les données humanitaires et les données du gouvernement. Cette situation soulève des préoccupations quant à l'accès du gouvernement aux listes humanitaires. Par exemple, les listes de personnes déplacées internes (PDI), de réfugié-e-s ou de migrant-e-s peuvent exposer ces populations à des risques (ciblage, détention, expulsion) ou à d'autres formes d'abus de la part des gouvernements. Si vous prévoyez d'utiliser des données existantes, il est important d'examiner les aspects juridiques en matière d'accès et d'exploitation des données collectées à une fin pour servir une autre fin. (Reportez-vous à la Fiche-conseil 2 et aux Encadrés 12 et 13 sur les bases légales pour le traitement des données).

La COVID-19 a incité de nombreuses agences à utiliser des ensembles de données existants et à innover dans les domaines de la protection sociale et des transferts monétaires humanitaires. Certaines de ces innovations sont détaillées sur le site SocialProtection.org et dans cet **article de blog**.

Mercy Corps fournit **des orientations sur les différents types de données pouvant être utilisées ou réutilisées pour le ciblage distant**, en précisant les **avantages et inconvénients** de chaque source.

Reportez-vous à **l'étude de cas du CaLP sur les approches émergentes relatives à l'exploitation de données non traditionnelles pour le ciblage des transferts monétaires**.

GovLab décrit comment il a réalisé un **assemblage de données** pour mieux cerner les situations dans lesquelles les résident-e-s de la ville de New York seraient disposé-e-s à ce que leurs données puissent être consultées et utilisées pendant la crise de la COVID-19. Cette méthodologie peut également être utilisée dans d'autres contextes.

DÉSIGNER LES ENTITÉS CHARGÉES DU CONTRÔLE ET DU TRAITEMENT DES DONNÉES

Au début d'un programme de transferts monétaires, il est indispensable de savoir qui contrôlera et qui traitera les données ou de déterminer s'il y aura plusieurs entités de contrôle des données. L'entité en charge du contrôle des données prend des décisions sur la manière dont les données personnelles sont traitées. Elle indique à l'entité en charge du traitement des données quelles données personnelles sont collectées et comment elles seront traitées. Lorsque plusieurs organisations assurent conjointement le contrôle des données, elles décident ensemble des fins et des moyens pour traiter les mêmes données personnelles.

ENCADRÉ 10: RÔLES ET RESPONSABILITÉS DES ENTITÉS EN CHARGE DU CONTRÔLE ET DU TRAITEMENT DES DONNÉES

Concernant les données, les obligations d'une organisation dépendent de son rôle dans le recueil et le traitement des données. En vertu du RGPD, par exemple, les personnes et les autorités de surveillance peuvent demander des comptes aux entités en charge du contrôle et du traitement des données en cas de non-respect de leurs responsabilités dans le cadre du RGPD.

Entité en charge du contrôle des données : entité qui, seule ou avec d'autres, exerce un contrôle sur les fins et les moyens de traitement des données personnelles. Ces entités assument le niveau de responsabilité le plus élevé concernant les données. Elles doivent respecter les principes de protection des données et d'autres exigences du RGPD. Elles sont également responsables de la conformité des entités en charge du traitement des données sous leur supervision. Les personnes et les autorités de surveillance peuvent prendre des mesures contre une entité en charge du contrôle des données qui ne respecte pas ses obligations. Les entités en charge du contrôle des données sont celles qui :

- décident de collecter ou de traiter des données personnelles ;
- décident de la finalité ou du résultat du traitement des données ;
- décident des données personnelles à collecter ;
- décident au sujet de quelles personnes collecter des données personnelles ;

ENCADRÉ 10: RÔLES ET RESPONSABILITÉS DES ENTITÉS EN CHARGE DU CONTRÔLE ET DU TRAITEMENT DES DONNÉES (SUITE)

- obtiennent un avantage commercial ou tirent un autre avantage du traitement des données, à l'exception de tout paiement de services assurés par une autre entité de contrôle des données ;
- traitent les données personnelles suite à un contrat entre nous et le sujet des données ;
- prennent des décisions sur les personnes concernées dans le cadre ou à la suite du traitement des données ;
- apportent un jugement professionnel lors du traitement des données personnelles ;
- entretiennent une relation directe avec les sujets des données ;
- sont entièrement autonomes quant au mode de traitement des données personnelles ;
- désignent les entités en charge du traitement des données personnelles pour leur compte.

Entités assurant conjointement le contrôle des données : plusieurs entités de contrôle des données qui déterminent ensemble les fins et les moyens pour traiter les mêmes données personnelles. En revanche, elles ne sont pas considérées comme conjointes si elles traitent les mêmes données à des fins différentes. Les entités assurant conjointement le contrôle des données doivent déterminer ensemble celle qui assumera la responsabilité principale face aux obligations du RGPD, notamment sur la transparence et les droits des personnes. Toutes les entités assurant conjointement le contrôle des données sont tenues de respecter les obligations de l'entité en charge du contrôle des données en vertu du RGPD. Les personnes et les autorités de surveillance peuvent prendre des mesures contre une entité en charge du contrôle des données qui ne respecte pas ces obligations. Les organisations sont des entités assurant conjointement le contrôle des données si :

- elles partagent les mêmes objectifs que d'autres en matière de traitement ;
- elles traitent les données personnelles aux mêmes fins qu'une autre entité de contrôle ;
- elles utilisent le même groupe de données personnelles (par ex., une base de données) qu'une autre entité de contrôle pour ce traitement ;
- elles ont élaboré ce processus avec une autre entité de contrôle ;
- elles partagent les mêmes règles de gestion des informations qu'une autre entité de contrôle.

Entité en charge du traitement des données : une entité qui traite les données personnelles pour le compte ou sous la supervision d'une entité en charge du contrôle des données. Ces entités ne traitent pas les données à leurs propres fins. Elles ne sont pas soumises aux mêmes obligations que les entités en charge du contrôle des données en vertu du RGPD et n'ont pas à payer de frais de protection des données. Elles ont toutefois des obligations directes propres en vertu du RGPD. Les personnes et les autorités de surveillance peuvent prendre des mesures contre une entité en charge du traitement des données qui ne respecte pas ces obligations. Les entités en charge du traitement des données sont celles qui :

- suivent les instructions d'un tiers concernant le traitement de données personnelles ;
- reçoivent les données personnelles de la part d'un client ou d'une tierce partie ou reçoivent des instructions sur le type de données à collecter ;
- ne décident pas de collecter des données personnelles auprès d'individus ;
- ne décident pas du type de données personnelles à collecter auprès d'individus ;
- ne décident pas de la base légale pour l'utilisation de ces données ;
- ne décident pas des fins auxquelles les données seront utilisées ;
- ne décident pas de divulguer ou non les données, ni auprès de qui ;
- ne décident pas de la durée de conservation des données ;
- prennent certaines décisions sur le mode de traitement des données, mais mettent en place ces décisions dans le cadre d'un contrat avec un tiers ;
- ne sont pas intéressées par le résultat final du traitement.

(Les définitions et les listes de contrôle sont extraites de l'Information Commissioner's Office du Royaume-Uni et ont été légèrement adaptées)[20]

La définition des rôles (entité de contrôle et entité de traitement) est essentielle pour les étapes suivantes, par exemple dans le cadre des accords de partage des données et des protocoles de transfert d'informations. Il est également important de savoir, à mesure que l'intervention est déployée, qui est responsable et redevable de tels ou tels aspects du traitement des données. Vous aurez également besoin de ces informations pour informer les personnes et les communautés sur la façon dont vous traiterez leurs données.

Reportez-vous à cette explication détaillée des responsabilités des entités en charge du contrôle et du traitement des données en vertu du RGPD.

20 Information Commissioner's Office du Royaume-Uni (2018), 'Guide to the General Data Protection Regulation: Controllers and Processors'.

ENCADRÉ 11: SCÉNARIOS COURANTS POUR LES ENTITÉS EN CHARGE DU CONTRÔLE ET DU TRAITEMENT DES DONNÉES

Pour déterminer qui est l'entité en charge du contrôle des données et celle en charge du traitement des données, vous devrez répondre à la question suivante : Qui décide des systèmes à utiliser et des données à collecter ? Divers scénarios illustrant la relation entre les entités en charge du contrôle et du traitement des données sont fournis ci-après.

Si un bailleur ou une entité des Nations Unies et des partenaires de mise en œuvre sont impliqués, l'un des scénarios suivants peut se produire :

- Une agence des Nations Unies ou un bailleur passif ou un financement propre – le partenaire de mise en œuvre est l'entité en charge du contrôle des données ;
- Une agence des Nations Unies ou un bailleur directif qui exige des systèmes/approches/données spécifiques – le bailleur est l'entité en charge du contrôle des données, le partenaire de mise en œuvre est l'entité en charge du traitement des données.

Dans une certaine mesure, il peut s'agir d'une décision politique. Les partenaires de mise en œuvre qui estiment être davantage attachés aux principes que les bailleurs/l'agence des Nations Unies peuvent souhaiter endosser le rôle d'entité en charge du contrôle des données. Sinon, s'ils souhaitent assumer moins de responsabilités, ils peuvent vouloir que leur bailleur/l'agence des Nations Unies endosse le rôle d'entité en charge du contrôle des données.

Parmi les ONG et les ONG internationales :

La situation peut être très simple ou plus compliquée si l'ONG ou l'ONG internationale travaille en partenariat avec d'autres (par ex., programme de consortium). Divers scénarios sont possibles, notamment :

- L'ONG ou l'ONG internationale travaille principalement pour son compte avec son propre personnel de terrain et des programmes papier/numériques « en boucle fermée ». Le cas échéant, l'ONG ou l'ONG internationale en question cumule les deux rôles.
- Un consortium linéaire où les rôles sont difficiles à distinguer est plus propice à la présence d'entités conjointes en charge du contrôle des données. Or, les équipes juridiques peuvent être mal à l'aise avec cette situation en raison de la somme de responsabilités qu'elle introduit, car n'importe quel membre des entités conjointes en charge du contrôle des données peut être tenu responsable d'une violation commise par un autre membre. Les équipes en charge de la confidentialité et les équipes de terrain peuvent avoir du mal à communiquer entre elles dans une telle situation, car elles ont forcément des propensions au risque différentes.
- Lorsqu'un membre du consortium prend clairement le « lead », il peut jouer le rôle d'entité principale en charge du contrôle ou du traitement et délivrer des sous-concessions à d'autres partenaires. Le cas échéant, l'entité principale assume la plupart des responsabilités en cas de violation des données.
- Lorsque le consortium prévoit des rôles très différents (par ex., le membre A travaille sur la sécurité alimentaire et le membre B fournit des conseils juridiques), il peut y avoir des entités de contrôle distinctes (« entités de contrôle en commun ») avec de simples accords de partage des données (« pour éviter toute ambiguïté »).

Participation d'un PSF :

Lorsqu'un PSF est impliqué, deux scénarios sont probables :

- Le PSF a ses propres obligations (par ex., KYC ou vente de services aux bénéficiaires par l'intermédiaire de cartes en boucle ouverte), auquel cas il peut être une entité de contrôle distincte. Le cas échéant, à l'instar d'un consortium aux rôles différents, cela peut se faire avec un accord de partage de données pour éviter toute ambiguïté/des entités de contrôle en commun. Ici, il serait opportun de réaliser une évaluation des risques pour définir d'éventuelles responsabilités et stratégies d'atténuation des risques à introduire au moment de l'ajout ou de l'approbation d'un PSF.
- Un PSF a peu d'obligations/aucune autre obligation (rares cas ; un prestataire de services comme un vendeur de logiciel/matériel pour les transferts monétaires peut entrer dans cette catégorie). Le PSF est alors simplement une entité en charge du traitement des données. Un PSF peut également être une entité en charge du traitement des données pour certaines activités, mais une entité en charge du contrôle des données pour d'autres (par ex., les client-e-s possèdent déjà une carte de débit pour laquelle la banque est l'entité en charge du contrôle des données ; pour certaines activités le PSF fait en revanche office d'entité en charge du traitement des données pour le compte d'une ONG internationale).

DÉFINIR LA BASE LÉGALE POUR LE TRAITEMENT DES DONNÉES *AVANT* DE RECUEILLIR DES DONNÉES PERSONELLES OU SENSIBLES

Pour traiter des données personnelles ou sensibles, vous devez avoir identifié une base légale. Il peut être utile d'envisager cette base légale pour le recueil des données comme une passerelle légale et éthique clé pour l'ensemble des activités impliquant des données, pour ainsi dire comme un test d'utilité sociale qui, s'il n'est pas probant, suggère qu'une utilisation particulière des données risque de ne pas servir au mieux la communauté ou les personnes affectées. Dans les législations nationales, les bases légales ont tendance à se concentrer sur l'équilibre entre d'une part les droits des personnes et les groupes, et d'autre part le « locus du pouvoir », c'est-à-dire le lieu où résident le contrôle, le pouvoir et le mandat.

Dans certains contextes, la base légale est très simple et porte entièrement sur le choix individuel. En revanche, dans la loi européenne et dans des contextes similaires, la base légale est plus nuancée et offre différentes options qui reconnaissent qu'un choix est parfois impossible, par exemple en présence d'une nécessité publique impérieuse, d'une exigence vitale ou d'une autre raison qui impose la collecte et le traitement des données. Lorsqu'un choix est impossible, quiconque souhaite collecter et traiter des données est souvent tenu de répondre à d'autres exigences de suivi pour s'assurer qu'aucun autre droit n'est enfreint.

Pour ces raisons, une base légale opportune n'est pas seulement une protection juridique essentielle, mais aussi un principe fondateur qui reconnaît et identifie où se trouve le pouvoir et définit la base de votre activité comme étant à vocation sociale.

ENCADRÉ 12: BASES LÉGALES POUR LE TRAITEMENT DES DONNÉES

Le RGPD répertorie par exemple six bases légales pour le traitement des données, comme suit :

- **Intérêts vitaux :** le traitement est nécessaire pour protéger la vie d'une personne en cas d'urgence.
- **Mission d'intérêt public :** le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de vos fonctions officielles, et la mission ou la fonction repose sur un fondement légal clair.
- **Consentement individuel :** la personne a consenti au traitement de ses données à caractère personnel à une fin spécifique.
- **Intérêts légitimes :** le traitement est nécessaire pour vos intérêts légitimes ou ceux d'une tierce partie, à moins que ne prévale un motif valable pour protéger les données à caractère personnel de la personne concernée.
- **Exécution d'un contrat :** le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci.
- **Obligation légale :** le traitement est nécessaire au respect d'une obligation légale (en dehors des obligations contractuelles).

Le CICR utilise les mêmes bases légales pour recueillir des données personnelles, mais regroupe les obligations légales et contractuelles dans une seule catégorie. La base légale doit être déterminée en amont de la collecte de données. Par ailleurs, la base légale et la finalité de la collecte des données ne peuvent pas être modulées une fois les activités de recueil et de traitement des données commencées. Le cas échéant, les données déjà recueillies devront de nouveau être collectées et traitées conformément à la base légale révisée[21].

Les bases légales ont fait l'objet de longues discussions dans le secteur humanitaire, notamment sur la question de savoir si et quand utiliser le type « consentement » plutôt que l'une des autres bases légales. En règle générale, les discussions portent sur les difficultés réelles à obtenir un consentement véritablement éclairé, volontaire et révocable dans les contextes humanitaires à cause des rapports de force en présence (notamment avec des transferts monétaires), de l'absence de choix et de la difficulté à expliquer comment les données seront traitées et partagées, entre autres aspects. Ce débat, complété par une autre étude sur les réglementations (comme le RGPD), a incité certaines organisations à opter pour la base légale « Intérêts légitimes » ou « Mission d'intérêt public », combinée à une approche du consentement éclairé éthique et positive. Reportez-vous à l'Encadré 13 pour obtenir des explications plus détaillées sur les bases légales et des recommandations sur la base légale la mieux adaptée aux transferts monétaires. *Il convient de préciser que ces recommandations ne font pas office de conseils juridiques, mais ont pour vocation de fournir à votre équipe juridique ou à votre service de protection des données des points à prendre en compte dans le choix des bases légales.*

21 Ces bases légales sont extraites du Règlement général sur la protection des données de l'Union européenne. Vous devrez consulter la législation nationale pour identifier les bases légales d'un pays particulier. Plusieurs organisations internationales (comme les Nations Unies et le CICR) jouissent de certains privilèges et de certaines immunités et suivent leurs propres règles, processus, politiques et principes en matière de protection des données.

ENCADRÉ 13: CHOISIR UNE BASE LÉGALE POUR LE TRAITEMENT DES DONNÉES

Les limites du consentement éclairé comme base légale pour traiter les données dans des situations humanitaires font l'objet d'intenses discussions. Il semblerait que d'autres bases légales soient mieux adaptées que le consentement. Nous explorons ici ces autres options en détails.

En vertu du RGPD, certaines bases légales risquent de ne pas convenir aux transferts monétaires. Par exemple, la base légale « Intérêts vitaux » semble inadaptée, même dans un contexte humanitaire[22]. De la même manière, les activités humanitaires ou de développement ne sont généralement pas exigées par la loi, ce qui rend la base « Obligation légale » non pertinente. En général, les agences ne concluent pas de contrats avec les communautés dans lesquelles elles interviennent. Le choix de la base légale « Exécution d'un contrat » (avec des personnes) semble donc improbable.

Il reste donc trois bases légales pour une intervention humanitaire (notamment avec des transferts monétaires), réparties dans deux groupes principaux :

Groupe 1 – Consentement est la base légale qui donne le pouvoir à la personne.

Groupe 2 – Mission d'intérêt public et Intérêts légitimes – l'accent est placé sur l'équilibre entre les droits des personnes et les besoins des organisations ou de la société dans son ensemble, comme exprimé dans ses lois et usages.

Consentement

Si l'utilisation de la base légale Consentement n'affranchit pas les organisations de leurs obligations en matière de redevabilité, de sécurité et d'évaluation des risques, elle fait effectivement valoir que, dans le contexte où le consentement est obtenu, les personnes sont suffisamment à même de faire des choix délibérés et éclairés. D'après le RGPD, pour que les personnes puissent donner leur consentement, les organisations doivent être en mesure de proposer un choix éclairé, révocable (réversible) dans des circonstances où le consentement peut être reporté ou refusé sans répercussions négatives.

Le recours à la base légale Consentement dans des contextes humanitaires et de développement s'accompagne de plusieurs défis, notamment :

- Au vu de la place centrale des données dans les programmes, le refus d'une personne de communiquer des données aura vraisemblablement des conséquences, par exemple si l'aide est conditionnée à une inscription ou un enregistrement.
- Il est difficile d'offrir un choix authentique ou libre au vu des rapports de force déséquilibrés en présence, surtout dans un contexte humanitaire.
- Il est rare qu'un retrait de consentement ou qu'un « droit à l'oubli » authentique puisse être proposé, notamment en présence d'autres exigences de type KYC, lutte contre le détournement de l'aide, audit, lutte contre la fraude ou MEAL qui peuvent exiger la conservation de données personnelles ou sensibles et donc empêcher tout « oubli » de la personne concernée.

Mission d'intérêt public et Intérêts légitimes

En l'absence de choix, mais lorsque l'activité est toujours souhaitable pour honorer la mission d'une agence ou défendre un bien social reconnu d'intérêt public, la base légale Intérêts légitimes (IL) ou Mission d'intérêt public (MIP) peut être indiquée.

Les bases légales IL et MIP peuvent sembler ne pas aller de pair, mais elles représentent toutes deux un « intérêt » ou un impératif, comme expliqué ci-dessous :

- L'organisation (IL) peut avoir un intérêt à défendre un impératif humanitaire ou des objectifs de programme inscrits dans sa charte, ses documents fondateurs, sa mission ou ses objectifs philanthropiques. Par exemple, une organisation peut avoir un *« intérêt légitime à servir des objectifs philanthropiques en fournissant un travail vital aux communautés par l'intermédiaire d'une aide en nature dans le cadre d'un programme de transferts monétaires qui requiert le nom et le statut du bénéficiaire pour évaluer et fournir cette aide »* ;
- Droit et société (MIP) : une base « Mission d'intérêt public » peut émaner d'un financement institutionnel de la part de bailleurs nationaux avec un mandat explicite pour fournir une aide vitale.

Aucune des justifications IL ou MIP en matière de collecte des données ne supplante les autres obligations au regard de la loi ni les bonnes pratiques de protection des données. L'obligation d'informer les personnes, de limiter la finalité et de garantir sécurité et collecte minimale demeure. Le RGPD stipule clairement que s'il existe un autre moyen d'obtenir le même résultat (c'est-à-dire sans requérir de données), la base légale ne sera pas valide.

Dans la plupart des cas, le choix définitif d'une base légale alliera circonstances spécifiques d'une organisation, contexte juridique local (surtout dans une situation hors RGPD et si le contexte est plus binaire) et interprétation de la loi. **Du fait des rapports de force déséquilibrés, des besoins externes (comme KYC) et des contextes difficiles ou changeants, nous considérons que la base légale**

22 La Raison 46 stipule que la base légale « Intérêts vitaux » ne devrait s'appliquer que dans un nombre limité de cas vitaux, « lorsque le traitement ne peut manifestement pas être fondé sur une autre base juridique ». La Raison 46 fournit l'exemple des « fins humanitaires » pour illustrer un traitement pouvant servir à la fois l'intérêt public et les intérêts vitaux, y compris pour suivre des épidémies et leur propagation, ou dans des situations d'urgence humanitaire. Cela indique clairement que la base légale « Intérêts vitaux » n'est pas un choix judicieux pour les acteurs humanitaires dans la plupart des interventions non critiques.

ENCADRÉ 13: CHOISIR UNE BASE LÉGALE POUR LE TRAITEMENT DES DONNÉES (SUITE)

« Consentement » est un choix inapproprié dans la plupart, voire dans tous les cas. Alliée à une approche du consentement éclairé éthique et positive, une approche axée sur les « intérêts » (Mission d'intérêt public ou Intérêts légitimes) peut offrir le meilleur compromis :

- en permettant aux personnes de faire des choix qualitatifs d'après une représentation contextuelle pertinente et exhaustive quant à la façon dont les données seront utilisées, et à quelle(s) fin(s) ;
- en imposant aux organisations d'être et de rester redevables et réfléchies au sujet de leurs comportements, des risques qu'elles font courir aux participant-e-s et de l'évolution de ces risques au fil du temps ;
- en insistant sur la nécessité de contextualiser tout jugement et tout exercice de compréhension (planification, mise en contexte, action et réaction).

INTÉGRER LE CONCEPT DE PROTECTION DE LA VIE PRIVÉE DÈS LA CONCEPTION

Alors que la Fiche-conseil 1 soulignait l'importance d'appliquer des principes de haut niveau pour une gestion responsable des données, le RGPD (tout comme les défenseurs et défenseuses du droit à la vie privée) recommande spécifiquement d'intégrer les principes de protection de la vie privée dès la conception (*Privacy by Design*, en anglais) dès la phase de conception et de planification. Ce concept sous-tend que la protection de la vie privée ne peut pas être garantie en se contentant de suivre les cadres politiques et réglementaires. Il doit également être intégré dans la conception des processus de recueil de données de sorte que la rigueur des mesures de protection de la vie privée soit proportionnelle à la sensibilité des données recueillies et traitées[23]. La protection de la vie privée doit être l'approche par défaut dans la conception des processus relatifs aux données, et non une option vers laquelle les personnes peuvent tendre. L'Encadré 14 rappelle de manière utile comment intégrer la protection de la vie privée dans vos conceptions.

ENCADRÉ 14: 7 PRINCIPES FONDAMENTAUX DU CONCEPT DE PROTECTION DE LA VIE PRIVÉE DÈS LA CONCEPTION

1. **Prendre des mesures proactives et non réactives, des mesures préventives et non correctives.** Anticiper les risques, prévenir les dommages ou incidents d'atteinte à la vie privée avant qu'ils ne se produisent et concevoir dès le départ des stratégies d'atténuation.
2. **Assurer la protection implicite de la vie privée.** Les particuliers n'ont aucune mesure particulière à prendre pour protéger leur vie privée. Cette protection est inscrite par défaut dans tous les paramètres.
3. **Intégrer la protection de la vie privée dans la conception.** La protection de la vie privée est intégrée dans la conception et l'architecture des systèmes et des pratiques. Elle est un composant essentiel des fonctionnalités de base fournies.
4. **Assurer une fonctionnalité complète (selon un paradigme à somme positive et non à somme nulle).** Les particuliers n'ont pas à choisir entre la protection de la vie privée et l'utilisation d'une application, d'un outil, d'une plateforme ou d'un service. Il n'est donc pas nécessaire de renoncer à la protection de sa vie privée pour accéder à un produit.
5. **Assurer la sécurité de bout en bout.** Le respect de la vie privé est garanti grâce à la protection de la confidentialité des données tout au long du cycle de vie des données. Toutes les données sont collectées, utilisées, conservées, stockées puis supprimées en toute sécurité en fin de cycle, en temps opportun.
6. **Assurer la visibilité et la transparence, garder la porte ouverte.** Les technologies et les pratiques fonctionnent conformément aux objectifs et aux promesses déclarées, sous réserve d'une vérification indépendante. Les personnes concernées sont averties du type de données personnelles collectées, de l'utilisation de ces données, pour quelle(s) fin(s) et par qui.
7. **Respecter la vie privée des utilisateurs/trices, garder le regard axé sur l'utilisateur/trice.** Les architectes et les opérateurs/trices privilégient les intérêts de la personne en proposant des mesures strictes de protection de la vie privée, des avis appropriés et des fonctions conviviales. Il est également important d'écouter les utilisateurs/trices et de répondre à leur feedback.

Reportez-vous à cette vue d'ensemble pour plus d'informations sur le concept de protection de la vie privée dès la conception.

23 https://www.ryerson.ca/content/dam/pbdce/seven-foundational-principles/The-7-Foundational-Principles.pdf

CONTRÔLER PRÉALABLEMENT LES PARTENAIRES DU SECTEUR PRIVÉ, NOTAMMENT LES PSF ET LES AUTRES TIERCES PARTIES

Les données et les outils numériques intègrent de plus en plus le quotidien des organisations humanitaires. Or, les données étant plus complexes et requérant des compétences que de nombreuses organisations n'ont pas encore, les partenariats avec le secteur privé jouent un rôle croissant dans la manière dont les organisations gèrent les données. Ces partenariats s'accompagnent parfois d'un financement ou d'une expertise technique en nature. Ils peuvent également permettre une mise à l'échelle et des initiatives plus durables, ce qui les rend attractifs aux yeux du secteur humanitaire.

En outre, les transferts monétaires sont de plus en plus acheminés par des prestataires tiers. Ces entités peuvent avoir un intérêt à « bien faire », mais leur principale motivation reste de réaliser des profits. Elles peuvent également être tenues de partager des données en vertu des lois sur la lutte contre le terrorisme et le blanchiment d'argent, ce qui peut influer sur la façon dont elles traitent les données. Dans certains cas, le secteur privé prend la sécurité et la confidentialité des données très au sérieux afin d'entretenir la confiance de la clientèle. Dans d'autres, il peut avoir un intérêt à monétiser les données ou à réutiliser les données client pour développer des services et des produits commerciaux. Si vous avez réalisé une analyse de l'économie politique des données (reportez-vous à la Fiche-conseil 1), elle a probablement permis d'identifier la dynamique de pouvoir et les possibles motivations des partenaires du secteur privé dans les transferts monétaires. La phase « Partager les données » (Fiche-conseil 6) porte sur la mise en place d'accords qui protègent les données des bénéficiaires de transferts monétaires et les données organisationnelles lors des programmes de transferts monétaires.

De nombreuses organisations humanitaires ont établi des procédures de contrôle des partenaires. Concernant la gestion responsable des données, ces procédures visent à s'assurer que les partenaires du secteur privé :

- ont les ressources et la volonté de protéger les données conformément aux exigences des acteurs humanitaires ;
- suivent des pratiques et des politiques strictes et responsables qui protègent et sécurisent les données ;
- ont réagi de manière adéquate à de précédents incidents ou violations concernant les données ;
- ont des lignes et des modèles commerciaux antérieurs, actuels et futurs en phase avec les principaux objectifs humanitaires et le principe « ne pas nuire » ;
- ne mènent pas des activités préjudiciables pour les populations vulnérables auxquelles les agences humanitaires viennent en aide (par ex., utiliser des données pour identifier des réfugié-e-s et des migrant-e-s aux fins de détention ou d'expulsion, concevoir des technologies de surveillance utilisées par les gouvernements pour cibler et nuire à des populations spécifiques, ou encore construire des modèles de données utilisés pour priver des personnes vulnérables ou des groupes spécifiques d'avantages et de services) ;
- s'engagent fermement à travailler avec les programmes de transferts monétaires et les bénéficiaires sans dérive prédatrice ni exploitation.

Certains partenaires du secteur privé, comme de nombreux opérateurs de téléphonie mobile, ont des modèles commerciaux qui s'appuient sur une gestion sécurisée des données, ce qui leur confère une expertise étendue en matière de sécurité et de confidentialité des données. Dans certains cas, ils peuvent aider les organisations humanitaires à s'améliorer dans ce domaine.

Si vous prévoyez de travailler avec le secteur privé sur des projets impliquant des données ou des technologies, vous pouvez consulter cette **note d'orientation** pour vous aider à définir un partenariat axé sur une gestion responsable des données.

Cette **liste de contrôle imprimable d'Electronic Frontier Foundation** peut vous aider à évaluer la capacité d'un partenaire en matière de confidentialité et de sécurité des données.

Cette **série de 7 questions** peut vous aider à poser les bonnes questions à votre prestataire en matière de conformité avec le RGPD.

DÉFINIR UN PROCESSUS DE GOUVERNANCE DES DONNÉES POUR FACILITER LA GESTION DE LA REDEVABILITÉ ET DES RESPONSABILITÉS CONCERNANT LES DONNÉES

Selon la structure du programme de transferts monétaires et les partenaires impliqués, il est important de préciser qui est responsable de la gestion des données dans l'ensemble et pour chaque processus de recueil des données aux différentes étapes du cycle du programme de transferts monétaires. Cela inclut ce qui suit :

- Tenir une liste d'inventaire des données et suivre quels partenaires détiennent quels types de données, et s'assurer qu'ils respectent les calendriers pour la conservation et la suppression des données, les accords de partage des données ainsi que toute autre disposition dans les contrats et les accords en lien avec la maintenance, la conservation et la destruction des données ;
- Suivre qui accède à quels types de données et gérer les changements des niveaux d'accès accordés au personnel et aux partenaires ;
- S'assurer que les données sont agrégées ou anonymisées le plus vite possible après leur recueil ou leur utilisation (selon les circonstances) ;

- Gérer et répondre à toute demande des participant-e-s aux programmes de transferts monétaires concernant la correction, la suppression ou le retrait de leurs données du système.

Veillez à préciser vos besoins en termes de maintenance et de conservation des données aux premiers stades de votre planification afin de vous assurer de disposer du budget nécessaire pour une maintenance, une conservation et une destruction sûres des données. Votre rôle dans le projet déterminera si le coût est supporté par votre organisation ou par un partenaire.

SE PRÉPARER À DE POSSIBLES VIOLATIONS OU INCIDENTS CRITIQUES EN MATIÈRE DE DONNÉES

Les incidents critiques en matière de données comprennent les violations d'infrastructure, toute divulgation ou altération non autorisée des données, ou encore l'utilisation de données collectées à des fins humanitaires à d'autres fins sans avoir obtenu le consentement ou l'accord correspondant. Ils surviennent lorsque la façon dont les données sont gérées nuit aux populations affectées, aux organisations, au personnel ou à d'autres personnes ou groupes. Les incidents de données peuvent impliquer le vol ou la confiscation d'un ordinateur portable contenant des données sensibles, l'altération ou le partage d'une liste de bénéficiaires de transferts monétaires sans autorisation ou la remise forcée de données en lien avec une étude ou sur les ménages aux autorités. Des incidents en matière de données peuvent survenir sans compromettre l'infrastructure technique. On parle également d'incident critique en matière de données lorsque le recueil, l'utilisation et le partage des données donnent lieu à la diffusion de rumeurs, sensibilités culturelles et dynamiques politiques négatives, ainsi qu'à d'autres facteurs portant préjudice aux populations affectées ou aux organisations humanitaires[24].

D'après l'évaluation de votre capacité et de votre contexte général (Fiche-conseil 1), vos expériences passées et les types d'acteurs susceptibles d'avoir un intérêt à accéder à vos données, élaborez une liste des types d'incidents de données risquant de se produire lors d'un programme de transferts monétaires et déterminez comment atténuer ce risque dans votre conception et votre planification. Vous devrez évoquer ce point avec les organisations partenaires ou (si vous êtes une organisation de mise en œuvre) avec les agences qui gèrent les systèmes de données. **Lors de la vérification des partenaires (par ex., PSF, opérateurs de téléphonie mobile, etc.) qui géreront les outils de données numériques et les systèmes de données plus vastes, il est important de formaliser par écrit dans votre accord contractuel leurs responsabilités (et les vôtres !) en cas d'incidents critiques en matière de données.** Votre équipe en charge de la sécurité des informations doit participer à ce type de vérification et votre équipe juridique peut fournir des modèles ou les formulations à inclure. Vous devrez aussi sans doute impliquer votre agent de protection des données.

Enfin, il conviendra de déterminer comment organiser la réponse à un incident critique en matière de données, en documentant la conduite à tenir dans un « protocole d'incident critique en matière de données » qui précise comment les incidents de données sont signalés, examinés et communiqués. Ce protocole définit également la marche à suivre pour déterminer si et comment proposer une compensation ou un soutien à quiconque voit une violation des données lui causer du tort. La plupart des lois sur la confidentialité des données exigent que toute violation des données soit signalée dans des délais spécifiques aux autorités en charge de la protection des données et aux personnes affectées par cette violation. Bien qu'il soit rare que les acteurs humanitaires divulguent aux populations affectées les cas de violation de données ou d'incidents critiques en matière de données, ces personnes ont le droit de savoir si leurs données ont été compromises, d'être informées des préjudices potentiels et d'être indemnisées pour les dommages subis. Ce domaine est étroitement lié à la redevabilité vis-à-vis des populations affectées dans le secteur des transferts monétaires, si bien que les équipes qui travaillent sur la redevabilité vis-à-vis des populations affectées peuvent être de bons alliés dans ce travail. Les équipes de prévention et protection sont également d'excellents alliés, car les incidents critiques en matière de données impliquent préjudice et dynamique du pouvoir. Les organisations sont tenues de prévenir les incidents en matière de données et ont un devoir de protection si de tels incidents se produisent.

Vos stratégies d'atténuation des incidents en matière de données devront englober la sécurité des données et les systèmes de données, ainsi que la formation et l'incitation à protéger ses données. Elles exigeront la contribution du personnel, des enquêteurs/trices et d'autres responsables des données « sur le terrain » qui connaissent le contexte quotidien d'une intervention.

Échangez avec vos équipes prévention et protection, cybersécurité, gestion des données, protection des données, juridique, communications/RP et conformité pour déterminer comment répondre collectivement aux incidents critiques en matière de données et si des politiques de ce type existent déjà. Vous pouvez éventuellement vous inspirer des protocoles et des expériences de votre organisation en termes de prévention et protection ou de gestion des crises de relations publiques pour anticiper et gérer les incidents critiques en matière de données.

Veillez à inclure les incidents critiques en matière de données dans votre évaluation des risques-avantages-dommages ou de l'impact sur la confidentialité des données (reportez-vous à la section suivante dans cette Fiche-conseil), ainsi que des exemples sur la façon de limiter les préjudices potentiels.

24 Centre for Humanitarian Data de l'OCHA, Note #2: Data Incident Management. Guidance Note Series: Responsible Data in Action. 2019.

UNE FOIS LE CYCLE DE VIE DES DONNÉES COMPLET PLANIFIÉ (FICHES-CONSEILS 1–7), RÉALISER UNE ÉVALUATION DE L'IMPACT SUR LA CONFIDENTIALITÉ DES DONNÉES

Une évaluation de l'impact sur la confidentialité des données (DPIA) (également appelée Évaluation de l'impact sur la confidentialité ou PIA ou encore Évaluation des risques et des avantages ou RBA) est une évaluation systématique des risques potentiels pour la confidentialité auxquels les personnes sont exposées suite au recueil et à l'utilisation de leurs données lors de la mise en œuvre du programme.

L'évaluation DPIA doit être réalisée lors de la phase de planification, à condition que vous ayez planifié le cycle de vie complet des données (étapes 1–7) pour disposer des informations requises à cette fin.

Une évaluation DPIA permet de mettre en lumière les préjudices potentiels *pour les personnes dont des données sont collectées et traitées*. Il ne s'agit pas d'un outil pour évaluer les risques et la responsabilité d'une organisation. Toutefois, en cas de risque important de préjudices aux personnes et aux groupes ayant participé à un programme, une organisation cumule risque et responsabilité. Une évaluation DPIA vous permet d'analyser les menaces et les risques en liens avec l'impact des données et d'élaborer des stratégies d'atténuation. Les évaluations DPIA aident les acteurs humanitaires à protéger la vie privée des participant-e-s et à renforcer la confiance du public dans le programme. Le Règlement général sur la protection des données (RGPD) et d'autres cadres légaux imposent qu'une évaluation DPIA ou PIA soit menée chaque fois qu'un risque élevé est probable pour la population cible. Une évaluation DPIA aide les organisations à déterminer si les avantages potentiels d'un recueil de données l'emportent sur les dommages potentiels et permet de documenter les conclusions. Des évaluation DPIA doivent être menées, quelles que soient les modalités des transferts monétaires.

Si votre organisation est auditée pour ses pratiques de gestion des données, une évaluation DPIA peut vous aider à fournir les documents indiquant comment votre organisation a identifié et atténué les risques en lien avec le recueil et le traitement des données. S'il peut être démontré que votre organisation a réalisé un travail exhaustif de gestion des données et de réduction des risques, les jugements et les sanctions devraient être moins sévères. Si votre organisation est perçue comme ayant agi avec négligence, des sanctions plus lourdes peuvent être recommandées. Si aucune évaluation DPIA n'est menée, il est également important de justifier en quoi cela était impossible.

Votre évaluation DPIA doit être utilisée comme un outil de planification qui complète (ou intègre) les autres processus d'évaluation des risques de l'organisation afin d'identifier les domaines à risque d'une organisation quant à la façon dont la gestion des données pourrait nuire aux populations affectées, ainsi qu'à la réputation ou à la situation financière ou juridique de l'organisation. Dans la mesure du possible, les évaluations DPIA doivent être des activités participatives, afin que le feedback des populations affectées soit inclus dans l'identification et la qualification des risques, ainsi que dans la proposition de stratégies d'atténuation. Les questions de sélection en lien avec une évaluation DPIA (de type « Cette population est-elle vulnérable ? ») doivent être intégrées dans d'autres processus comme les listes de contrôle de planification, les guides de conception de programme, les cadres d'approbation et les processus d'approbation des offres pour systématiser le respect de la vie privée dans l'organisation au sens large.

Si une organisation identifie au cours du processus DPIA que le soutien et les ressources requises ne sont pas disponibles pour gérer les données de manière responsable, que les données ne peuvent pas être recueillies et utilisées de façon responsable en raison du contexte, ou encore que des risques disproportionnés par rapport aux avantages pèsent sur les populations affectées en raison de l'utilisation des données, l'intervention doit être interrompue et une approche programmatique différente et moins consommatrice de données doit être mise en œuvre.

Certaines organisations intègrent également l'évaluation DPIA dans leurs cadres et structures de gouvernance. Dans tous les cas, il est important de réaliser une évaluation des risques axée sur les données qui porte sur l'impact de l'utilisation des données sur les populations affectées[25].

Alors que la Fiche-conseil 1 suggère une évaluation rapide pour déterminer si une organisation doit déployer une intervention en se basant sur le contexte et la capacité (reportez-vous à l'Encadré 9), l'évaluation DPIA analyse en profondeur les activités envisagées en termes de recueil et d'utilisation des données, telles que définies dans la proposition ou dans l'exercice de recueil et d'utilisation des données au sein de la proposition (par exemple, un processus de collecte des données pour cibler les transferts monétaires, le recours à une modalité spécifique d'acheminement des transferts monétaires ou un processus MEAL ou d'étude).

Exemples de processus et de cadres DPIA, PIA et RBA :

- **Data Protection Handbook** du CICR, Annexe 1, page 299.
- **Benefit Risk Assessment Framework Workshop** de Sonjara.

25 Les évaluation DPIA peuvent être réalisées à différentes étapes du cycle d'un programme de transferts monétaires. Une évaluation DPIA globale peut être effectuée lors de la phase de conception du programme pour déterminer si les acteurs des transferts monétaires sont en mesure de réduire les risques en matière de confidentialité à un niveau acceptable. Les risques potentiels pour les populations affectées ne doivent pas l'emporter sur les avantages potentiels. Il en va de même pour les organisations : les processus de recueil des données doivent présenter plus d'avantages que de risques. Des évaluations DPIA doivent également être effectuées pour les activités de recueil de données menées tout au long du cycle du programme. Si un format DPIA normalisé est utilisé, les évaluations DPIA peuvent être réalisées périodiquement et de manière centralisée au début des nouvelles activités de recueil des données. Ces activités peuvent être consolidées et utilisées à intervalles réguliers aux fins d'apprentissage et d'amélioration progressive. Une évaluation DPIA doit être un « document vivant » révisé à intervalles réguliers, par exemple en cas de changement dans les partenaires, le contexte ou l'utilisation des données.

- **Outil Benefit Risk Assessment** de l'USAID, pages 11–13 du document Considerations for Using Data Responsibly.
- **PIA, Privacy Commissioner of New Zealand**.
- **Protéger la vie privée des bénéficiaires** du CaLP, pages 19-20.
- Cadre de travail **Évaluation des dommages pour les créateurs de technologies** de Microsoft.

Certaines organisations utilisent une Évaluation des risques et des avantages (RBA), qui peut être plus utile dans le contexte humanitaire. À condition de couvrir les questions de confidentialité des données, cette évaluation peut dans bien des cas remplacer une évaluation DPIA. Les évaluations RBA sur les données posent une question cruciale : qui s'expose à des risques et qui tire parti du recueil des données ? Cela vise à s'assurer que les risques ne pèsent pas sur les plus vulnérables tandis que les organisations récoltent les avantages. La **note d'orientation de l'OCHA sur les évaluations des impacts des données** présente les différents types d'évaluations et propose des méthodes pour déterminer le mieux adapté selon le contexte.

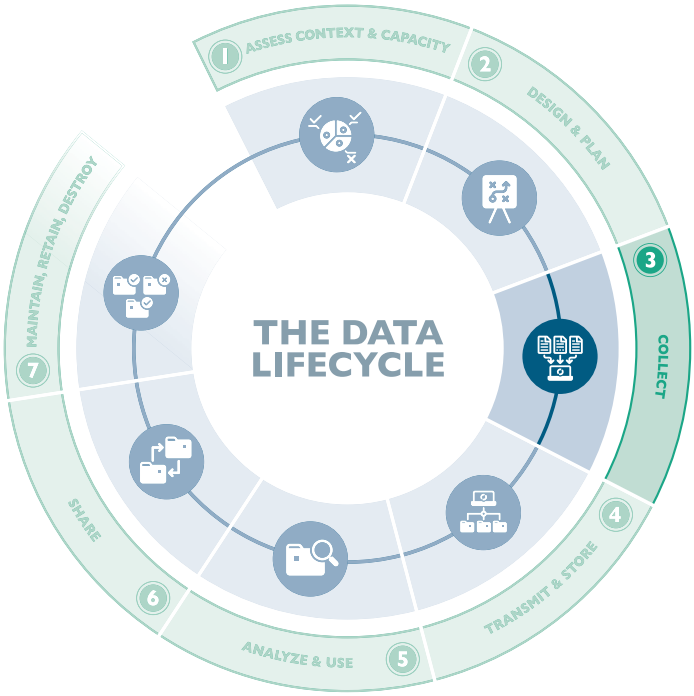
FICHE-CONSEIL 3

COLLECTER/ACCÉDER AUX DONNÉES

Les données peuvent être utilisées à bon escient, par exemple pour améliorer le ciblage des programmes et lutter contre les doublons et la fraude. Elles peuvent également être utilisées pour influer de manière opaque sur des comportements : à des fins d'extorsion, pour cibler et nuire à des personnes et des groupes, ou encore pour diffuser de fausses informations. Les données peuvent également causer du tort de manière involontaire, malgré de bonnes intentions. Pour toutes ces raisons, et parce que chacun-e a droit au respect de sa vie privée, il est essentiel de recueillir les données et d'y accéder de manière responsable.

Le recueil de données personnelles et d'autres formes de données sensibles s'effectue à toutes les étapes d'un programme de transferts monétaires, notamment :

- planification et évaluations des besoins
- ciblage
- inscription et enregistrement
- acheminement
- feedback
- suivi et évaluation



La Fiche-conseil 3 couvre les aspects qui vous aideront à recueillir des données de grande qualité, telles que requises et de manière proportionnée aux fins de la collecte. Cette note d'orientation s'applique également en cas d'accès à des données recueillies précédemment ou par d'autres organisations.

ENCADRÉ 15 : DÉFINITIONS : DONNÉES PERSONNELLES, DONNÉES PERSONNELLES SENSIBLES, DONNÉES NON PERSONNELLES SENSIBLES ET MÉTADONNÉES

Qu'entend-on par données personnelles ?

- Données en lien avec une personne identifiée ou *identifiable*, notamment les données qui identifient clairement une personne (nom, numéro, adresse IP ou identifiant cookie) ou les données qui pourraient permettre d'identifier une personne (par ex., avec un petit ensemble de données ou parce que les données incluent des informations ou une combinaison d'informations qui facilitent l'identification d'une personne dans un grand ensemble de données).
- Données qui identifient une personne lorsqu'un ensemble de données est croisé avec un autre ensemble de données.

Qu'entend-on par données sensibles ?

- Les données sensibles incluent les données personnelles sensibles qui, en cas d'accès ou de divulgation sans autorisation appropriée, pourraient entraîner une discrimination ou une répression à l'encontre d'une personne, de la source d'information ou d'autres personnes ou groupes identifiables.

ENCADRÉ 15 : DÉFINITIONS : DONNÉES PERSONNELLES, DONNÉES PERSONNELLES SENSIBLES, DONNÉES NON PERSONNELLES SENSIBLES ET MÉTADONNÉES (SUITE)

- En général, les données personnelles sensibles incluent la race, l'origine ethnique, l'affiliation politique, la religion, l'adhésion à un syndicat, des informations génétiques, des informations biométriques, ainsi que des informations sur la santé, la vie sexuelle et l'orientation sexuelle. Elles incluent également des données personnelles sur les personnes extrêmement vulnérables, comme les enfants ou les personnes déplacées.
- D'autres informations personnelles peuvent être sensibles selon le contexte ou la culture. Dans les contextes humanitaires, beaucoup de données sont très sensibles. Les données présentent différents niveaux de sensibilité selon le contexte. C'est pourquoi nous ne fournissons pas une liste exhaustive des points de données sensibles dans la présente Boîte à outils.
- Il est également important de déterminer qui décide de la nature sensible ou non des données. Les communautés affectées peuvent déterminer qu'un champ de données spécifique est sensible même si la réglementation sur la confidentialité des données ou si les organisations de mise en œuvre ne les identifient pas comme telles.

Qu'entend-on par données non personnelles sensibles ?

- Données sur le contexte dans lequel une crise survient (par ex., informations sur les communautés bénéficiaires de transferts monétaires).
- Données sur la réponse apportée par les organisations et les personnes cherchant à aider (par ex., emplacements des distributions d'espèces ou plans des exercices de collecte des données[26].

Qu'entend-on par métadonnées ?

- Les métadonnées sont des « données sur des données ».
- Elles résultent des dispositions pratiques des transferts monétaires et différentes obligations juridiques et réglementaires s'appliquent au recueil, au partage et à la conservation des métadonnées.
- Concernant l'argent mobile, par exemple, les métadonnées incluent le numéro de téléphone de l'émetteur/trice et celui du/de la destinataire, la date et l'heure de la transaction financière, l'identifiant de la transaction, le lieu et le montant de la transaction, la boutique où elle a été effectuée et tous les agents impliqués à chaque extrémité.
- Ces données peuvent être utilisées pour déduire d'autres informations et renseignements susceptibles d'être utilisés pour dresser le profil, cibler et suivre des utilisateurs/trices. Elles peuvent être exploitées pour déduire des informations sur les comportements, les déplacements, les affiliations ou d'autres caractéristiques des populations affectées. L'aptitude à tirer des déductions sur les bénéficiaires demeure longtemps après la fin d'un programme[27,28].

DÉTERMINER COMMENT PROTÉGER LES DONNÉES EN CAS DE COLLECTE À DISTANCE OU PAR TÉLÉPHONE MOBILE

Même si le recueil de données à distance avait déjà cours dans certains pays à cause d'un conflit ou d'environnements de travail complexes, cette forme de collecte s'est généralisée avec la pandémie de COVID-19. De nombreuses organisations ont commencé à réaliser le ciblage pour les transferts monétaires par téléphone ou à déléguer l'identification et la gestion de la sélection des bénéficiaires de transferts monétaires aux membres de la communauté. Ce type de recueil des données s'accompagne de problèmes de confidentialité, ce qui peut donner lieu à du favoritisme ou à une manipulation des listes ou encore placer les membres de la communauté dans une position où ils doivent gérer des demandes d'espèces. En cas d'opération réalisée totalement à distance, il n'y aura pas de tiers externe disponible (comme une organisation de transferts monétaires) pour signaler ou proposer un soutien dans ces situations[29]. Par ailleurs, les réglementations Connaissance de la clientèle (Know your customer, ou KYC) sont parfois levées ou allégées, et lorsqu'elles sont déployées, les organisations peinent à les respecter au moment d'enregistrer des bénéficiaires par téléphone, car elles ne sont pas en mesure de vérifier l'identité en direct. Si certaines de ces données sont toujours collectées sans recourir à des mécanismes numériques distants, le recueil de données à distance connaît une évolution rapide, avec bon nombre de nouvelles interventions impliquant des méthodes de collecte des données numériques. Parmi les pratiques innovantes, on peut citer le recours à l'identification vocale ou au « selfies » comme justificatif d'identité. Le GAFI a récemment observé que la vérification à distance de l'identité pouvait être aussi efficace là où de hauts niveaux de validation de l'identité pouvaient être atteints. Les points mentionnés dans l'Encadré 14 rappellent de manière utile comment intégrer la protection de la vie privée dans la conception[30].

26 OCHA (2019), 'Data Responsibility Guidelines: Working Draft'.
27 CICR (2020), Data Protection Handbook.
28 CICR et Privacy International (2018), 'The Humanitarian Metadata Problem: Doing No Harm in the Digital Era'.
29 Save the Children, Tip-sheet: Adaptations in how we identify, register, and verify CVA beneficiaries in the time of COVID-19 (non publié).
30 Groupe d'action financière (GAFI) (2020), 'Digital Identity'.

Reportez-vous au document **CVA in COVID-19 contexts** du CaLP pour obtenir un aperçu de la façon dont les agences s'adaptent au recueil de données à distance et aux autres activités à distance.

Consultez **cette discussion** sur les avantages, les inconvénients et les bonnes pratiques de suivi à distance.

Reportez-vous à **cette liste de contrôles** pour savoir comment collecter des données à distance en toute sécurité. Elle peut être adaptée pour le recueil de données mobiles aux fins de transferts monétaires.

La boîte à outils **Vulnerability Analysis & Mapping (VAM)** du PAM indique comment mener des enquêtes mobiles de façon responsable.

UTILISER DES MÉTHODES, DES APPROCHES ET DES OUTILS DE COLLECTE DES DONNÉES INCLUSIFS

Lors de la conception de la phase de recueil des données, notamment si des outils numériques sont utilisés, il est essentiel d'intégrer à dessein l'inclusivité afin d'éviter de laisser les populations les plus vulnérables à l'écart. Les femmes sont moins susceptibles que les hommes de posséder un téléphone portable, particulièrement dans des contextes humanitaires. Le document The Mobile Gender Gap Report 2020 de GSMA démontrait par exemple que les femmes sont 8 % moins susceptibles que les hommes de posséder un téléphone portable, et que cet écart atteint 20 % concernant l'Internet mobile[31]. Ces écarts peuvent être encore plus prononcés dans les contextes humanitaires[32]. Les personnes les plus pauvres sont également davantage exclues de l'accès mobile. De la même manière, il est important que les organisations déterminent si elles incluent les personnes en situations de handicap et d'autres groupes faisant l'objet de discriminations. Vous devrez intégrer dès le départ ces cas « limites » dans la conception de votre processus de recueil des données et prévoir un budget correspondant. Il s'agira de prendre des mesures pour concevoir d'autres types d'accès et de rechercher activement ces cas « limites » pour s'assurer que vous testez les approches et les méthodes de recueil des données sur ces groupes qui sont plus susceptibles d'être exclus.

Le portail **IASC Accountability and Inclusion Portal** propose des ressources et des guides pour garantir l'inclusion dans les processus humanitaires.

Reportez-vous à cette **boîte à outils** pour l'inclusion numérique des personnes handicapées.

La boîte à outils **Gender and Information Communication Technology (ICT) Survey Toolkit** de l'USAID propose différents modules et réflexions pour mieux cerner l'accès des femmes aux TIC.

Vous devrez proposer plusieurs options ou modalités de recueil des données pour garantir l'inclusion des plus vulnérables (par exemple, les personnes isolées, les femmes, les personnes ne parlant que des dialectes) et des personnes handicapées.

TENIR COMPTE DE L'IMPACT DES EXIGENCES DE CONNAISSANCE DE LA CLIENTÈLE, DE L'ENREGISTREMENT DE LA CARTE SIM ET DES MESURES ANTI-TERRORISTES

Lorsque les organisations humanitaires collaborent avec des opérateurs de téléphonie mobile et d'autres PSF, elles sont tenues de respecter les exigences de Connaissance de la clientèle (KYC), les règlementations sur la lutte contre le blanchiment d'argent (AML), les mesures anti-terroristes (CTM) et d'autres réglementations et lois destinées à lutter contre la corruption et le blanchiment d'argent. Autrement dit, votre organisation ou les bénéficiaires des transferts monétaires doivent partager des données sensibles et personnelles avec des tiers, notamment des régulateurs, aux fins de contrôle de l'identité des bénéficiaires de transferts monétaires. Certains bailleurs exigent une vérification supplémentaire dans le cadre des mesures anti-terroristes. En outre, plus de 155 gouvernements dans le monde ont mis en place des politiques d'enregistrement obligatoire de la carte SIM qui imposent aux personnes de fournir une pièce d'identité pour obtenir une carte SIM[33].

Le Groupe d'action financière (GAFI), l'autorité mondiale de surveillance des activités de blanchiment d'argent et de financement du terrorisme, peut également formuler d'autres recommandations, transposées ensuite dans la législation nationale. Les nouveaux/nouvelles bénéficiaires de transferts monétaires doivent alors être soumis-es aux critères de ces listes. Les informations KYC doivent être vérifiées au regard de listes établies par les autorités locales, notamment concernant les personnes et les entités potentiellement impliquées dans un conflit ou un contexte violent. Les bénéficiaires de transferts monétaires peuvent être exclu-e-s de l'aide si ils ou elles figurent sur l'une de ces listes, même si cela découle d'une erreur sur la personne. En cas de conflit, des familles ayant besoin de transferts monétaires peuvent être issues de communautés figurant sur ces listes de surveillance, qui sont souvent classées par zone géographique.

Ce processus peut être supervisé par les autorités publiques et inclure des obligations de signalement. La lutte contre le blanchiment d'argent et les mesures anti-terroristes sont souvent mises en œuvre avec l'aide de logiciels tiers. Toutefois, ce qu'il advient des données saisies dans ces bases reste parfois obscur. Les données collectées pourraient être utilisées à d'autres fins par les gouvernements ou les PSF/opérateurs de téléphonie mobile, comme la promotion d'autres services financiers (ou d'autres services si les données sont ensuite cédées ou partagées) ou la détermination de la solvabilité.

31 GSMA (2020) 'The Mobile Gender Gap 2020'.
32 GSMA (2020) 'Bridging the mobile gender gap for refugees'.
33 GSMA (2020) 'GSMA Digital Identity Programme: Insights and Achievements (2016–2020)'.

Lors de la négociation de la portée d'une intervention ou du processus d'approvisionnement avec un PSF, il est essentiel que ces éléments importants soient évalués et que les organisations disposent de procédures claires pour réviser les documents sur la portée d'une intervention. Ce processus doit être coordonné entre les équipes qui gèrent directement les processus de transferts monétaires, les équipes techniques qui évaluent des aspects comme la sécurité, le stockage des données et les éléments de serveur, les responsables des données et du respect de la vie privée, et l'approvisionnement. Cela peut aider les organisations à éviter les failles, les lacunes ou les surprises, comme des clauses sur le partage des données qui ne protègent pas totalement les données sur les transferts monétaires.

Certains bailleurs ou gouvernements n'imposent pas ce type de sélection. Toutefois, lorsque cela est exigé, vous devez expliquer la situation aux personnes affectées dans le cadre du processus de recueil des données et ces personnes doivent avoir le choix entre fournir leurs données, opter pour un autre type de processus et recevoir une aide sous une autre forme (en nature, paiement direct, coupons uniques ou cartes à puce anonymisées). Toutefois, certaines agences ne sont pas en mesure de proposer ce choix du fait de leur structure, de leur taille et de leur dépendance vis-à-vis d'autres agences pour les systèmes et le financement.

Il est possible de négocier avec les bailleurs concernant les implications opérationnelles de leurs critères de sélection. Les bailleurs sont de plus en plus sensibilisés à la nécessité de gérer les données de manière responsable et d'atténuer les risques en lien avec les données. Ils comprennent souvent les compromis nécessaires, par exemple que la sélection nuit aux principes humanitaires d'impartialité. Cela vous laisse une marge de négociation.

Une liste des pays qui exigent l'enregistrement de la carte SIM (en date de 2020) est disponible **ici**.

Les exigences KYC et certains exemples de réglementations ajustées sont discutés dans cette **Fiche-conseil** de 2016.

BIEN TENIR COMPTE DES COÛTS ET DES AVANTAGES DE LA COLLECTE DE DONNÉES BIOMÉTRIQUES OU DE L'INTRODUCTION DE SYSTÈMES NUMÉRIQUES D'IDENTIFICATION

L'utilisation de données biométriques pour gérer et suivre l'inscription et l'acheminement de l'aide humanitaire, notamment les transferts monétaires, présente plusieurs avantages. Les données biométriques (empreintes digitales, reconnaissance de l'iris, reconnaissance faciale et reconnaissance vocale) sont toutes utilisées dans le cadre de programmes de transferts monétaires déployés dans différentes régions du monde. Elles offrent une forme d'identification unique pour une personne, même en l'absence d'autres moyens de prouver leur identité car les autres documents d'identification ont été perdus ou sont inaccessibles (ce qui est souvent le cas pour les personnes déplacées). Si les données biométriques sont louées pour leur capacité à réduire les fraudes individuelles, des critiques pointent en revanche le fait qu'elles ne luttent pas contre la corruption et les abus au sens large au niveau systémique, où l'on considère que la fraude est la plus répandue[34]. Par ailleurs, les données biométriques sont régulièrement remises en question car elles permettraient aux agences de gagner en efficacité sans apporter d'autres avantages aux populations affectées[35], ainsi que pour d'autres raisons (inexactitudes, risque d'utilisation détournée et risque de voir les données biométriques partagées avec les gouvernements, par ex.). Certaines organisations explorent l'utilisation de technologies qui respectent la vie privée, la cryptologie et des systèmes de registres distribués comme la technologie « blockchain » afin de conserver les données biométriques d'une manière plus sécurisée, même si ce domaine doit encore être approfondi.

Si des données biométriques sont utilisées, leur utilisation doit être proportionnelle aux fins pour lesquelles elles ont été collectées. Les organisations doivent pouvoir démontrer que les avantages présentés par les données biométriques l'emportent sur les risques associés à leur utilisation. En raison de la nature très sensible des données biométriques, vous devrez toujours réaliser une évaluation DPIA, PIA ou RBA avant de confirmer leur utilisation. Si, en tant qu'agence de mise en œuvre, il vous est demandé d'utiliser des données biométriques car le système dans lequel vous saisissez des données l'exige, vous devrez étudier soigneusement votre capacité à collecter et à gérer les données biométriques de façon sécurisée. Les agences qui demandent à leurs partenaires d'utiliser des données biométriques doivent s'assurer que ces partenaires sont à même de protéger les données biométriques. À cause du degré d'inconfort lié aux données biométriques dans certaines communautés affectées, il est indispensable que les personnes choisissent de manière délibérée et rationnelle si elles souhaitent fournir des données biométriques pour s'inscrire ou recevoir des transferts monétaires, ainsi que de proposer une alternative qui ne représente pas une charge pour ces personnes. Des organisations comme Mercy Corps explorent actuellement d'autres formes d'identification unique qui n'impliquent pas de données biométriques. Si vous envisagez d'utiliser des données biométriques, assurez-vous de bien comprendre le fonctionnement de bout en bout d'une solution donnée. Si la solution est trop difficile à comprendre, cela peut être une raison suffisante pour revenir à des formes d'identification ne recourant pas à des données biométriques. Le CICR a mené une enquête approfondie pour déterminer où et quand il pourrait être approprié d'utiliser des données biométriques et identifié plusieurs cas où leur utilisation est pertinente et d'autres où elle ne l'est pas.

34 Oxfam et The Engine Room (2018) 'Biometrics in the Humanitarian Sector'.
35 Voir la lettre ouverte d'Access Now « 'Why ID' » pour plus d'informations sur les défis relatifs aux données biométriques dans une intervention humanitaire et dans d'autres situations.

Le document **Internal Primer on Biometrics** de Mercy Corps fournit des orientations détaillées.

Reportez-vous au Chapitre 8 sur les données biométriques du document **Data Protection Handbook** du CICR pour plus de détails sur les données biométriques, sur la façon de gérer ce type de données sensibles et pour déterminer sur quelle base légale les données biométriques peuvent être collectées dans différentes circonstances.

Reportez-vous à **ce document** pour plus de détails sur l'utilisation des données biométriques et de systèmes d'identification et d'inscription dans le contexte de crises longues et récurrentes.

Lisez la lettre ouverte « **Open letter to to the leaders of international development banks, the United Nations, international aid organisations, funding agencies, and national governments** pour explorer plus en détails certaines des questions et problématiques clés en lien avec les systèmes d'identification biométrique.

COMMUNIQUER DE FAÇON TRANSPARENTE AVEC LES POPULATIONS AFFECTÉES SUR LE RECUEIL ET LE TRAITEMENT DES DONNÉES

Une communication claire et transparente avec les populations affectées sur le recueil et le traitement des données est une composante importante de tout processus impliquant des données et doit faire partie intégrante de la façon dont vous concevez et budgétisez la gestion responsable des données. Comme indiqué dans la Fiche-conseil 2 dans la section dédiée aux bases légales (reportez-vous aux Encadrés 12 et 13, pages 20 et 21), le recours au consentement comme base légale pour le recueil et le traitement des données est contesté. Néanmoins, quelle que soit la base légale utilisée, vous devrez être à même d'expliquer clairement aux communautés affectées (d'une manière culturellement pertinente) qui demande le recueil des données, comment contacter ce donneur d'ordre, pourquoi les données sont collectées et traitées, qui contacter en cas de questions sur le traitement des données et avec qui les données seront partagées, surtout en cas de partage avec les autorités, avec des instances gouvernementales (comme celles chargées de faire respecter la loi) ou avec des entités dans d'autres territoires ou juridictions.

ENCADRÉ 16 : QUE DOIVENT SAVOIR LES PERSONNES AFFECTÉES AVANT DE FOURNIR LEURS DONNÉES ?

D'après la politique du CICR, les informations suivantes doivent être communiquées aux personnes affectées lorsque la base légale choisie est « Consentement » :

- l'identité et les coordonnées de l'organisation qui a demandé et qui contrôle le recueil et le traitement des données (« entité en charge du contrôle des données ») ;
- l'objectif spécifique du traitement des données personnelles ;
- une explication des risques et avantages potentiels liés au traitement des données ;
- le fait que l'entité en charge du contrôle des données peut traiter les données personnelles pour d'autres fins similaires (avec des exemples) ;
- le fait que le consentement peut être retiré à tout moment ;
- les circonstances dans lesquelles il peut être impossible de traiter les données de manière confidentielle ;
- leurs droits de s'opposer au traitement de leurs données et leurs droits d'accéder, de corriger et de supprimer leurs données personnelles ;
- comment exercer leurs droits en lien avec les données et quelles sont les restrictions possibles quant à l'exercice de leurs droits ;
- auprès de quel-le-s pays tiers ou organisations internationales leurs données peuvent être transférées pour atteindre l'objectif de la collecte initiale et du traitement complémentaire ;
- combien de temps les données personnelles seront conservées (ou les critères qui seront utilisés pour déterminer la durée de conservation) et toute mesure prise pour s'assurer que les registres sont précis et à jour ;
- auprès de quelles autres organisations (par ex., les autorités du pays où les données sont collectées) leurs données seront partagées ;
- une indication des mesures de sécurité mises en œuvre par l'entité en charge du contrôle des données concernant le traitement des données[36].

36 CICR (2020), Data Protection Handbook (2020).

Vous devrez reformuler toute communication sur la façon dont les données seront traitées et enregistrées dans un langage clair et accessible que les communautés et les personnes affectées comprennent. Des illustrations, des vidéos et des processus de consentement audio peuvent aider. N'oubliez pas que les concepts de consentement individuel et de respect de la vie privée sont perçus de manière différente selon la culture. Certains membres du personnel travaillant sur les transferts monétaires émettent des critiques concernant les approches juridiques de l'Europe vis-à-vis du consentement et du respect de la vie privée, les jugeant trop centrées sur l'hémisphère Nord et condescendantes, et souvent non pertinentes ni valorisées. Concernant la transparence sur le recueil et le traitement des données, la priorité absolue est de s'assurer que les populations affectées assimilent parfaitement le processus, plutôt que de se contenter de suivre une liste de contrôle.

Veillez à inclure des informations sur la collecte des données, les droits en lien avec les données et les mécanismes de réclamation dans vos processus globaux de feedback et de redevabilité pour tout programme de transferts monétaires. Cela concerne notamment les métadonnées (voir la définition page 26) qui seront recueillies lors des programmes de transferts monétaires numériques ou de la collecte de données.

Cette boîte à outils peut vous aider à concevoir un plan de communication et de sensibilisation sur la gestion responsable des données pour votre intervention.

Si vous proposez un mécanisme de réclamations (comme il se doit !), assurez-vous d'avoir prévu les ressources adéquates (personnel, capacité des systèmes, budget) pour sa mise en œuvre. Par exemple, si une personne demande à ce que ses données soient supprimées de votre système, savez-vous localiser ces informations dans votre système, vérifier l'identité et accéder à cette demande ?

Pour plus d'informations sur le consentement, voir la **fiche de consentement éclairée** de World Vision.

Reportez-vous au document **Data Protection Handbook** du CICR pour plus de suggestions sur la façon de gérer le consentement éclairé et d'autres bases légales, avec des modèles et des formulations à adapter à votre situation. Le Chapitre 9 de ce manuel fournit des orientations détaillées sur les transferts monétaires et sur la protection des données.

Retrouvez de plus amples informations sur les **mécanismes communautaires de plainte interorganisations**.

FICHE-CONSEIL 4

ENVOYER/STOCKER LES DONNÉES

On parle de transmission de données chaque fois que des données sont envoyées d'un lieu vers un autre, par exemple lorsque des employé-e-s de votre organisation s'envoient des données ou des fichiers entre eux/elles ou les envoient à une autre organisation, à un gouvernement ou à une autre entité. Dans certains cas, la transmission de données est un processus actif, par exemple lorsqu'un agent recenseur appuie sur « Envoyer » afin que les données de l'enquête soient transférées via le réseau mobile d'un téléphone portable vers le serveur d'une organisation ou vers le cloud. Dans d'autres, la transmission s'effectue en arrière-plan car un appareil mobile, une application, un site Web ou un logiciel back-end transmet automatiquement des données pendant son utilisation. C'est par exemple le cas quand des données de localisation sont transmises à un opérateur de téléphonie mobile lorsqu'un téléphone portable capte une antenne-relais à proximité. Les données sont généralement stockées sur un appareil (téléphone portable, ordinateur portable), sur un serveur ou dans le cloud.

Les données collectées au cours des différentes étapes d'un programme de transferts monétaires (évaluation des besoins, ciblage, inscription enregistrement, acheminement, feedback et MEAL) seront transmises et stockées de différentes manières selon la conception de votre processus de recueil des données. Les données peuvent être exposées à des risques lors de la transmission et du stockage pour diverses raisons. C'est pourquoi il est important de transmettre et de stocker les données d'une façon sécurisée qui limite le nombre de personnes pouvant y accéder. Les professionnel-le-s du secteur des transferts monétaires travaillent souvent avec des partenaires et des applications tierces. Vous devrez donc vous assurer que les données collectées auprès des populations affectées ne sont pas vulnérables à un accès, une altération, une suppression ou un partage non autorisé(e) et potentiellement nuisible. Des accords sur les transferts de données peuvent contribuer à formaliser le transfert des données entre les acteurs des transferts monétaires.

Dans la Fiche-conseil 4, nous explorons comment limiter les risques associés à la transmission et au stockage des données.

SUIVRE LES RECOMMANDATIONS DE BASE SUR LA SÉCURITÉ DES DONNÉES POUR LA TRANSMISSION ET LE STOCKAGE DES DONNÉES

Quiconque collecte, transmet ou stocke des données doit suivre plusieurs protocoles de base pour la sécurité des données. Les professionnel-le-s du secteur des transferts monétaires doivent avant tout se référer et se conformer à leurs politiques institutionnelles et aux directives sur la sécurité des données, parallèlement aux meilleures pratiques et autres normes juridiques et réglementaires.

ENCADRÉ 17 : MOYENS DE PROTÉGER LES DONNÉES LORS DE L'UTILISATION D'APPLICATIONS ET D'OUTILS NUMÉRIQUES

- Évitez de concevoir de nouveaux outils ou des applications personnalisées, car cela pourrait nécessiter des ressources intensives pour garantir, gérer et maintenir la sécurité, ainsi qu'une phase de test pour détecter d'éventuels défauts.
- N'utilisez pas un système ou un outil simplement parce qu'un partenaire, une organisation homologue ou un bailleur vous le demande : rapprochez-vous d'abord de votre équipe de sécurité informatique et de votre agent en charge du respect de la vie privée pour vous assurer que son utilisation est sûre.
- Prévoyez suffisamment de temps et de ressources pour réaliser des évaluations de sécurité sur les outils et les plateformes.
- Utilisez uniquement des réseaux Wi-Fi privés et sécurisés ou connectez-vous via un réseau privé virtuel (VPN).
- Cryptez les appareils et la transmission des données et utilisez des applications de messagerie cryptées comme Signal.
- Recourez à une authentification à deux facteurs.
- Consultez uniquement des sites Web sécurisés (avec « https » dans l'URL, et non « http »).
- Utilisez des mots de passe complexes, ne partagez pas vos mots de passe et n'utilisez pas une seule combinaison nom d'utilisateur-mot de passe pour plusieurs personnes.
- Utilisez des systèmes institutionnels approuvés pour le transfert et le stockage de données cryptées (par exemple, Microsoft SharePoint pour le transfert de fichiers au lieu de programmes de partage de fichiers tiers).
- Utilisez des moteurs de recherche et des navigateurs qui privilégient la confidentialité (Firefox et DuckDuckGo).
- Installez les dernières versions de vos logiciels et actualisez votre protection antivirus.

Votre équipe de sécurité informatique saura vous guider pour identifier les moyens les plus sûrs de transmettre et de stocker des données. Vous pouvez être amené-e à travailler avec vos équipes informatiques au siège social pour identifier certains des défis contextuels afin qu'il soit possible de faire des compromis éclairés si la sécurité des données nuit à la facilité des opérations, ce qui augmente la probabilité que les utilisateurs/trices contournent la sécurité pour fluidifier les méthodes de travail. Il s'agit là d'un point clé à souligner dans votre évaluation DPIA ou RBA (voir la Fiche-conseil 2). La sécurité des données n'est peut-être pas une priorité dans l'esprit du personnel et des enquêteurs/trices, surtout dans des situations stressantes et conflictuelles. Des mesures de sécurité technique renforcées ont tendance à ralentir les systèmes et les processus, si bien que le personnel peut être contraint de les contourner pour gagner du temps. Il est essentiel que votre organisation souligne l'importance de suivre les mesures de sécurité imposées et ouvre le dialogue avec le personnel et les enquêteurs/trices pour concevoir des mesures de sécurité qui sont susceptibles d'être suivies et qui n'alourdissent pas inutilement leur charge de travail.

En situation de conflit, même les meilleures mesures de sécurité peuvent être inefficaces, car le personnel ou les enquêteurs/trices peuvent être physiquement menacés par des personnes voulant accéder aux données sur les bénéficiaires de transferts monétaires ou à d'autres informations. L'identification de solutions leur permettant de stocker des volumes de données limités sur leurs appareils et de minimiser le recueil de données sensibles peut contribuer à réduire les risques pour le personnel et les populations affectées. De nombreux outils mobiles de recueil des données permettent de transmettre immédiatement les données dans le cloud par simple pression sur la touche « Envoyer », si bien que les données ne sont pas stockées sur un appareil. Cela peut contribuer à protéger les enquêteurs/trices et le personnel en première ligne. Dans certains contextes volatiles, les organisations ont choisi comme autre mécanisme de protection de ne pas communiquer les besoins et les critères de vulnérabilité aux enquêteurs/trices. Le fait de décider de l'éligibilité en dehors du pays protégerait le personnel de première ligne de la coercition et des menaces proférées par des groupes cherchant à interférer dans les programmes de transferts monétaires ou à accéder aux données des populations affectées.

En plus des avantages susmentionnés, le stockage sur le cloud permet de bénéficier d'une puissance informatique de haut niveau, d'une grande flexibilité en termes de localisation et de flux de données, et de coûts réduits pour les organisations. Il a toutefois ses inconvénients dans les domaines de la sécurité et de la confidentialité. Le CICR identifie deux défauts majeurs des services cloud : l'absence de contrôle sur les données et le manque de transparence sur la façon dont les services cloud traitent les données. Il recommande que les acteurs humanitaires soient particulièrement attentifs aux risques présentés par des services cloud, à savoir : accès depuis des lieux non sécurisés/protégés ; interception des informations sensibles ; authentification faible ; violations des données de la part du prestataire de services cloud ; risque d'accès aux données par le gouvernement et les forces de l'ordre. Ces risques devront être évalués et corrigés par vos équipes en charge de la sécurité et du respect de la vie privée afin d'optimiser la gestion responsable des données. Par ailleurs, certains pays interdisent la transmission des données de leurs citoyen-ne-s en dehors de leur territoire, notamment sur des serveurs cloud hébergés à l'étranger.

Des ressources plus détaillées sur les applications de protection de la confidentialité des données organisationnelles sont fournies dans **cette liste de contrôle de sécurité** et dans la **Fiche-conseil sur le cryptage** d'ELAN.

The Centre for Humanitarian Data fournit des **directives sur les transferts de données** et la **sécurité des opérations organisationnelles**.

Le CICR donne un **aperçu des types de données collectées automatiquement** lors de l'utilisation d'un logiciel ou d'une application numérique. Ces éléments doivent être pris en compte lors de votre évaluation DPIA, PIA ou RBA.

Si vous envisagez de stocker des données dans le cloud, pensez à vous renseigner sur les lois nationales sur les données et assurez-vous que les données dans le cloud sont protégées par des accords de partage des données avec les hébergeurs cloud. Conseil : reportez-vous au Chapitre 10 du document **Data Protection Handbook** du CICR pour une vue d'ensemble complète de l'utilisation d'un stockage sur le cloud.

UTILISER ET MAINTENIR LES NIVEAUX D'ACCÈS BASÉS SUR LES RÔLES

Pour gérer les données de façon responsable, il est également important de s'assurer que seules les personnes autorisées peuvent y accéder. Par exemple, une organisation peut ne pas autoriser des responsables au niveau du district à accéder à des données au niveau mondial. Les enquêteurs/trices peuvent ne pas être autorisés à accéder aux données d'un système, mais seulement à alimenter ce système en données. Les partenaires d'un grand programme de transferts monétaires peuvent être uniquement autorisés à accéder aux données qu'ils ont chargées, mais pas aux données que d'autres organisations ont chargées. Ces autorisations basées sur les rôles doivent refléter l'autorité et les responsabilités en lien avec les données concernées. Autrement dit, elles doivent permettre d'accéder uniquement aux données dont les différentes personnes ont réellement besoin pour remplir leur mission, ni plus ni moins. Des examens réguliers doivent être réalisés pour suivre les niveaux d'accès aux données lorsque des personnes changent de poste au sein de l'organisation ou quittent celle-ci, ainsi que pour les consultant-e-s et les tiers.

Des autorisations intégrées peuvent être définies dans les systèmes de gestion des données (il faut alors formuler une demande pour accéder à certaines données dont l'accès est restreint). De tels mécanismes de sécurité incluent des horodatages, des demandes de téléchargement, le suivi des consultations et d'autres types de suivi concernant les personnes qui interviennent sur une base de données et la nature des opérations réalisées. Ces mécanismes aident l'équipe informatique et le/la responsable des systèmes à suivre en continu la sécurité de la base de données et l'accès aux données. Ils peuvent également vous aider à déterminer si l'intégrité des données a été compromise ou à identifier toute fraude ou violation. L'hébergement des données dans le cloud peut être plus sécurisé dans certains cas. En effet, les ordinateurs portables et les autres appareils exposés au vol et au piratage sont ainsi délestés de toutes les données personnelles et sensibles.

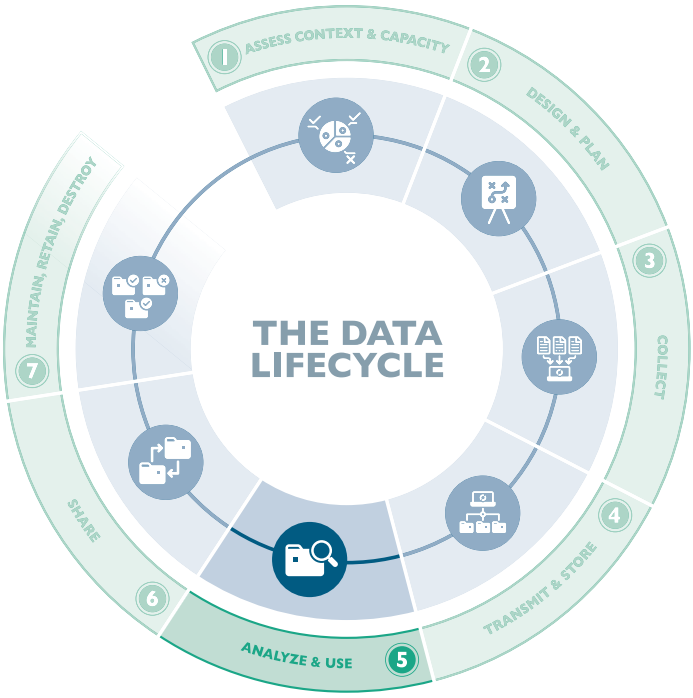
Les niveaux d'accès autorisés réduisent le risque d'altération non autorisée des données, de fuite et de violations des données. Cela peut toutefois être frustrant pour les organisations qui transfèrent des données dans un système plus vaste si elles ne peuvent pas avoir une vision d'ensemble de toutes les données. Cela pourrait donner l'impression que les agences de plus grande envergure contrôlent les données et régissent l'intervention, car elles ont accès à toutes les données des autres partenaires et disposent donc de plus d'informations sur les tendances, ce qui pourrait les aider dans leurs demandes de financement et la recherche d'autres partenariats. Il peut être judicieux de discuter des situations de ce type au sein des consortiums ou du groupe de travail sur les transferts monétaires pour trouver une solution adaptée.

En interne, les organisations doivent demander à leurs équipes RH d'établir des contrats sur la confidentialité et la protection des données à faire signer aux personnes qui ont accès aux données, afin qu'elles soient tenues responsables en cas de partage non autorisé, de destruction ou de mauvaise utilisation des données.

FICHE-CONSEIL 5

ANALYSER/EXPLOITER LES DONNÉES

Une fois les données disponibles, qu'il s'agisse de nouvelles données collectées pour le programme de transferts monétaires ou de données de sources existantes, il convient d'en déterminer la qualité et le caractère exploitable. Révisez votre processus d'analyse des données pour vous assurer que les données sont inclusives, que cette analyse des données n'entraîne pas l'exclusion de certains groupes ou de certaines personnes des prestations auxquelles ils/elles sont éligibles. Si vous utilisez des données pour prendre des décisions automatisées, il est important que les critères et les processus décisionnels soient clairs et transparents afin que des tiers puissent en confirmer l'impartialité en cas de soupçons ou d'allégations d'allocation inéquitable des prestations. Par ailleurs, les données doivent être utilisées uniquement aux fins prévues au moment de la collecte et qui font l'objet d'un consentement ou reposent sur une autre base légale.



La Fiche-conseil 5 couvre les aspects à prendre en compte pour analyser et exploiter de manière responsable les données dans les programmes de transferts monétaires.

UTILISER LES DONNÉES UNIQUEMENT AUX FINS POUR LESQUELLES ELLES ONT ÉTÉ COLLECTÉES, SAUF SI DE NOUVELLES AUTORISATIONS ONT ÉTÉ OBTENUES

Comme indiqué dans la Fiche-conseil 2 (reportez-vous aux Encadrés 12 et 13 sur les bases légales), le traitement des données doit reposer sur une base légale et des finalités légitimes. Avant toute analyse ou exploitation des données, réexaminez la base légale selon laquelle les données ont été initialement recueillies, puis déterminez (avec votre équipe juridique et votre agent de protection des données) si vous êtes légalement en droit de les traiter.

Les organisations humanitaires reçoivent souvent des listes de participant-e-s à un programme de transferts monétaires ou des recommandations d'autres groupes (par ex., partenaires locaux, agences homologues, organismes des Nations Unies ou gouvernements). Si les données ont été recueillies en vertu de la base légale « Intérêts légitimes » ou « Mission d'intérêt public », il peut être acceptable de les traiter si le traitement secondaire s'inscrit dans le même esprit que ce qui a été initialement annoncé aux personnes concernant l'utilisation qui serait faite de leurs données. Si les données ont été collectées en vertu de la base légale « Consentement », vous devrez probablement obtenir un nouveau consentement avant de pouvoir exploiter ces données à une autre fin. Il est important d'impliquer votre équipe juridique ou votre agent en charge du respect de la vie privée pour vous assurer de ne pas être en infraction en réutilisant les données.

Les prestataires de services financiers (PSF), les opérateurs de téléphonie mobile ou d'autres entités du secteur privé peuvent

souhaiter recouper les listes de bénéficiaires ou conserver les métadonnées à des fins légales, ce qui peut être admis en vertu des exigences légales en matière de conformité. Ils peuvent également souhaiter dresser le profil des bénéficiaires pour déterminer leur solvabilité, ce qui serait incompatible avec la finalité initiale du recueil de données (acheminement des transferts monétaires) et requiert une nouvelle base légale pour le traitement des données, et potentiellement une nouvelle relation avec les bénéficiaires, avec un nouveau consentement ou d'autres autorisations. Poursuivre ce type de traitement serait illégal d'après les termes du RGPD, par exemple. Les organisations humanitaires doivent analyser tout traitement supplémentaire des données par les PSF ou les opérateurs de téléphonie mobile afin d'identifier tout risque de préjudice à court et à long terme pour les populations affectées (par exemple, incapacité future à accéder au crédit ou promotion de produits financiers aux fins d'exploitation). Une telle utilisation des données peut aller à l'encontre des principes humanitaires de neutralité, d'impartialité et d'indépendance.

ÉPURER LES DONNÉES ET CONTRÔLER LEUR QUALITÉ

Des données désordonnées produiront des résultats biaisés ou non valides. Que les données soient recueillies directement par votre organisation ou que vous réutilisiez des ensembles de données ou des listes partagées par d'autres, vous devrez épurer les données pour les rendre exploitables. Cela peut inclure de supprimer les doublons, de contrôler les critères d'éligibilité des participant-e-s et de vérifier une partie de la liste, mais sans doute aussi de supprimer les données susceptibles d'être utilisées pour identifier des personnes dans un ensemble de données, sauf si ces données sont requises dans la mise en œuvre du programme. Veillez à documenter l'ensemble des lacunes, restrictions et défauts identifiés dans les jeux de données.

Remarque : veillez à ne pas exposer par inadvertance des informations ou des données humanitaires sensibles pendant ou après l'analyse et/ou la visualisation. L'analyse de données humanitaires sensibles doit uniquement être réalisée dans un environnement sécurisé et par des personnes autorisées à accéder aux données.

Conseil : IMPACT Initiatives propose une **procédure opérationnelle normalisée** pour le nettoyage des données que vous pouvez appliquer à vos propres processus.

SUPPRIMER OU ANONYMISER LES DONNÉES PERSONNELLES ET SENSIBLES DES JEUX DE DONNÉES LORSQUE LA SITUATION LE PERMET

Comme indiqué dans la Fiche-conseil 3, la minimisation des données est un principe fondamental de la gestion responsable des données. L'un des moyens de minimiser la somme de données personnelles ou sensibles en votre possession est de les anonymiser, c'est-à-dire de retirer les informations d'identification pour que les données deviennent « anonymes ». Lorsque les données sont anonymisées, l'association entre les données et les personnes auxquelles elles font référence est supprimée, si bien que les données ne permettent plus d'identifier ces personnes. Pour cela, il faut supprimer les « identifiants directs » et les « identifiants indirects », par exemple en retirant un numéro de carte d'identité nationale ou une date de naissance. Ce processus rend les données plus privées et réduit le risque pour les personnes car il a supprimé les données d'identification ou les a agrégées à un niveau tel qu'il ne permet plus l'identification des personnes.

Il convient de rappeler que même des données anonymisées ou agrégées peuvent exposer des groupes entiers de personnes à un risque. Par exemple, la localisation de groupes religieux ou ethniques particuliers peut être utilisée pour attaquer ces groupes. Si des informations sont communiquées quant au lieu d'une distribution de transferts monétaires, des groupes indésirables pourraient interférer ou menacer les personnes qui reçoivent des transferts monétaires ou les organisations qui les distribuent. En plus de commencer par planifier l'anonymisation des données personnelles, vous devrez également envisager comment protéger les données non personnelles. Certaines données doivent uniquement être partagées avec/diffusées à celles et ceux qui en ont besoin aux fins d'approbation et dans des environnements de données convenablement protégés, avec les contrôles techniques et organisationnels appropriés.

Les technologies et l'analyse des données devenant de plus en plus sophistiquées, vous aurez probablement besoin du soutien de votre équipe informatique ou en charge des données pour anonymiser les données.

Les données anonymisées sont plus sûres, mais si elles deviennent trop générales, elles ne sont plus exploitables pour l'acheminement des transferts monétaires. Vous devrez trouver des solutions qui minimisent les données tout en remplissant les objectifs en matière de transferts monétaires.

Même si les données individuelles ont été anonymisées, les personnes concernées peuvent être de nouveau identifiées par recoupement (statistique) avec d'autres jeux de données ou dans les résultats des enquêtes au niveau individuel. Les listes de transferts monétaires sont souvent combinées et fusionnées, à la fois au sein de chaque organisation et après le partage des jeux de

données. Le cas échéant, il devient plus simple d'identifier les personnes au sein de jeux de données. Le contrôle de la divulgation des données statistiques est une méthode qui permet d'évaluer le risque de ré-identification et qui réduit ce risque avant de partager des données. OCHA fournit des **directives** sur cette méthode.

En cas de collaboration avec des partenaires commerciaux dans des lieux où la confidentialité des données est préoccupante, il peut être intéressant de conclure un accord avec un PSF pour utiliser des sous-comptes, de sorte que la diligence raisonnable ou les exigences KYC s'appliquent uniquement à l'agence de mise en œuvre en tant que titulaire principal du compte, et non aux personnes accédant aux sous-comptes. L'accès aux sous-comptes peut s'effectuer au moyen de cartes à puce (comme des cartes prépayées ou des cartes de retrait) uniquement associées à des numéros de référence, sans aucun détail personnel. Les bénéficiaires de transferts monétaires peuvent alors retirer des espèces sans que leurs données personnelles soient partagées avec le PSF. Seule l'agence de mise en œuvre dispose des informations qui relient la carte ou le compte au/à la bénéficiaire des transferts monétaires.

PROCESSUS DÉCISIONNELS AUTOMATISÉS

Le Rapporteur spécial des Nations Unies sur les droits de l'homme et l'extrême pauvreté a averti en 2019 que les réformes de protection sociale facilitées, justifiées et protégées par les nouvelles technologies numériques pouvaient refléter des valeurs et des hypothèses non conformes aux principes des droits humains[37]. Par exemple, des personnes peuvent être exclues par erreur des prestations lorsque des décisions sont prises par des logiciels automatisés. Par ailleurs, des personnes peuvent être définitivement étiquetées ou catégorisées d'une manière susceptible d'engendrer une future discrimination. Par exemple, une personne qui reçoit une prestation découlant de son statut de réfugié-e au cours d'une phase spécifique de sa vie peut être définitivement désignée comme présentant un risque de crédit par des algorithmes décisionnels. Les programmes de transferts monétaires deviennent de plus en plus numériques. Il est donc important que les valeurs humanitaires demeurent des priorités et que les technologies et les outils numériques que les acteurs des transferts monétaires intègrent dans leurs programmes n'exacerbent pas l'exclusion et les préjudices inhérents aux données. Les processus décisionnels automatisés reposant sur des données permettent certes de prendre des décisions plus rapides et à plus grande échelle, mais ils sont encore balbutiants et pourraient entraîner une exclusion ou des préjudices par la suite.

Le RGPD prévoit également des dispositions spécifiques pour protéger les personnes dont les données font l'objet de processus décisionnels automatisés ayant des répercussions juridiques ou des effets significatifs similaires sur elles. Si ce type de processus décisionnel est impliqué, le RGPD impose par exemple que les personnes concernées reçoivent des informations sur le traitement. Ces personnes doivent par ailleurs disposer de moyens simples pour demander une intervention humaine ou contester une décision. Vous devez enfin réaliser des contrôles réguliers pour vérifier que vos systèmes fonctionnent comme prévu.

Bien que la plupart des organisations n'utilisent pas de processus décisionnels automatisés dans leurs programmes, ces processus sont de plus en plus courants dans le secteur commercial pour les transactions financières comme les approbations de crédit. Dans le domaine des transferts monétaires, certaines organisations analysent comment utiliser les enregistrements des détails des appels pour cibler de potentiel-le-s bénéficiaires de transferts monétaires.

Lorsqu'ils sont utilisés, les processus décisionnels automatisés doivent étayer les décisions humaines, et non s'y substituer. Les organisations effectuant des transferts monétaires doivent s'assurer que tout processus décisionnel automatisé utilisé aux fins de ciblage ou d'inscription/enregistrement repose sur des algorithmes ouverts et transparents et fait l'objet d'une supervision humaine, d'une recherche comparative et de tests pour identifier tout biais potentiel, et qu'il existe des mécanismes clairs pour les réclamations et les recours si des décisions sont erronées ou risquent d'entraîner des préjudices à l'avenir.

Reportez-vous à **l'étude de cas sur le ciblage à distance à l'aide de données non traditionnelles** du CaLP pour plus d'informations à ce sujet.

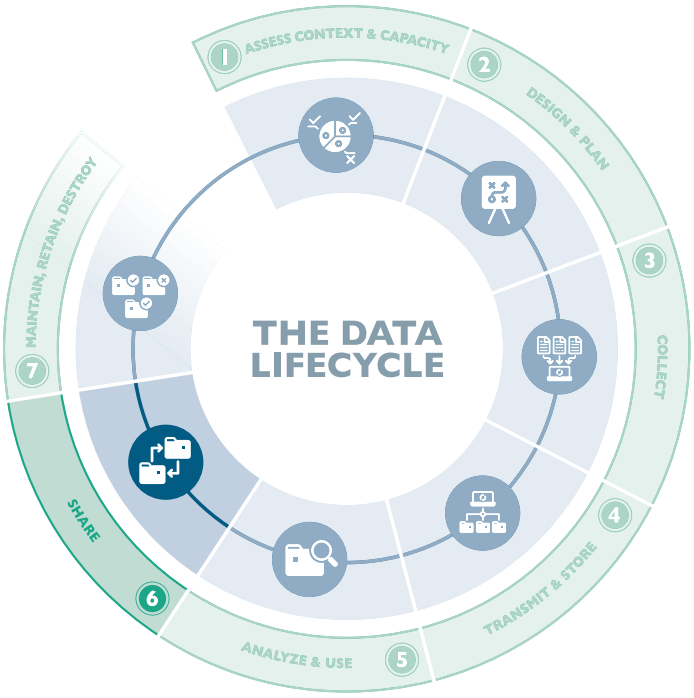
37 P. Alston (2019), Rapport du Rapporteur spécial sur les droits de l'homme et l'extrême pauvreté. Assemblée générale des Nations Unies.

FICHE-CONSEIL 6

PARTAGER LES DONNÉES

Les acteurs des transferts monétaires interviennent dans les contextes les plus variés, notamment dans des zones de conflits actifs, en situation de crise des réfugié-e-s, avec des personnes déplacées internes et lors de blocus. Le partage des données est nécessaire dans les programmes de transferts monétaires. À mesure que les groupes de travail sur les transferts monétaires et les consortiums s'alignent et collaborent, que des partenariats sont créés avec les PSF et les opérateurs de téléphonie mobile, et que des liens avec la protection sociale sont établis, le partage des données est de plus en plus fréquent aux fins de coordination et pour d'autres raisons.

Les bailleurs et les acteurs humanitaires sont de plus en plus favorables au développement de registres uniques ou sociaux pour les programmes d'assistance sociale et promeuvent une plus grande interopérabilité et un partage étendu des informations, délaissant les systèmes de gestion des informations distincts et déconnectés. Certaines agences des Nations Unies, comme le PAM, le HCR, l'UNICEF et OCHA, réclament des approches communes sur les transferts monétaires humanitaires et une collaboration accrue entre les agences[38]. Or, les avantages du partage des données sont souvent définis en termes de gains d'efficacité, reléguant au second plan les avantages en matière de protection et dans d'autres domaines, ainsi que les compromis[39].



La Fiche-conseil 6 donne des directives pour partager les données de façon responsable tout en reconnaissant qu'il s'agit d'un domaine litigieux qui devra être arbitré au cas par cas selon le contexte et les acteurs impliqués.

DÉTERMINER QUELLES INFORMATIONS DOIVENT ÊTRE PARTAGÉES, AVEC QUI ET POURQUOI

Comme souligné dans la Fiche-conseil 2, Encadré 10 sur les entités de contrôle et de traitement des données, les entités en charge du contrôle des données prennent des décisions sur la façon dont les données sont recueillies et traitées. Elles prennent également des décisions sur le partage des données. Les entités en charge du traitement des données ne doivent pas décider pourquoi ni avec qui partager des données, car cela relève des attributions de l'entité en charge du contrôle des données[40].

Avant de partager des données, vous devez définir les paramètres suivants :

- **Objectif :** pourquoi partagez-vous des données ? Quelles données partagez-vous ? Devez-vous partager l'intégralité des données pour atteindre votre but ou pouvez-vous en partager seulement une partie ou dans des domaines spécifiques ?
- **Licéité :** la législation vous autorise-t-elle à partager ces données ou à décider de leur partage ? Disposez-vous des autorisations

38 Voir cette annonce sur le système commun de transferts monétaires.
39 R. Goodman et al. (2020), Review and Analysis of Identification and Registration Systems in Protracted and Recurrent Crises.
40 Information Commissioner's Office du Royaume-Uni (2018), Controllers and Processors.

nécessaires et/ou les populations affectées ont-elles été informées du partage des données ?

- **Fonctionnement :** comment allez-vous les partager ? Comment seront-elles stockées ? Avez-vous vérifié l'organisation avec laquelle vous partagerez des données pour vous assurer qu'elle les conservera de façon sécurisée et confidentielle ? (Reportez-vous à la Fiche-conseil 4 sur la transmission et le stockage des données)
- **Description :** avez-vous fourni une description suffisante des données et du contexte dans lequel elles ont été recueillies, du moment où elles ont été recueillies et d'autres informations clés afin que les données ne soient pas utilisées hors contexte[41] ?

Vous devrez probablement créer plusieurs versions de jeux de données pour différents partenaires et différentes utilisations. Les données personnelles et sensibles doivent uniquement être partagées en cas d'absolue nécessité et après avoir obtenu un accord de partage de données.

Avant de partager des informations de quelque type que ce soit, il est essentiel de s'assurer que les personnes concernées par les données comprennent ce qu'il adviendra de leurs données et qu'elles aient donné leur consentement éclairé pour leur exploitation ou qu'une autre base légale pour le partage et le traitement des données ait été établie. Autrement dit, les participant-e-s ont autorisé le partage des données, en toute connaissance des répercussions potentielles (reportez-vous à la Fiche-conseil 2 et aux Encadrés 12 et 13).

L'accès aux données personnelles et sensibles ne doit pas s'effectuer par défaut, mais selon le principe du « besoin de savoir ».

Déterminez le type d'accès dont les partenaires ont besoin et définissez si possible des autorisations d'accès et des paramètres de suivi des bases de données pour contrôler qui peut consulter, ajouter, modifier, télécharger ou supprimer des données.

ÉVALUER LES RISQUES ET LES AVANTAGES AVANT DE PARTAGER DES DONNÉES AVEC DES GOUVERNEMENTS

Un postulat fréquent est que les systèmes de transferts monétaires humanitaires centralisés constitueront la base de systèmes de protection sociale gouvernementaux à plus long terme. Une telle hypothèse est à mettre en balance avec les aspects de la protection des données et de la confidentialité, en raison des effets potentiels sur les droits fondamentaux des bénéficiaires[42]. Dans certains cas, un système unique peut convenir, tandis que dans d'autres, il ne sera pas idéal au vu du contexte national et de l'intervention. Quel que soit le contexte, les organisations doivent chercher à évaluer ce point conjointement pour identifier la meilleure solution pour les populations touchées par une crise.

Selon le contexte, le partage des données avec les gouvernements peut présenter des risques importants pour les populations vulnérables, par exemple si des données sur des migrant-e-s en situation irrégulière sont partagées avec des gouvernements hostiles envers les migrant-e-s ou si des données sur des réfugié-e-s ou des populations déplacées internes sont partagées avec des groupes armés locaux déterminés à leur causer du tort. Outre un partage des données légal (bien que potentiellement préjudiciable), un partage forcé des données peut survenir à différents stades d'une intervention, notamment au niveau local lorsque les enquêteurs/trices font l'objet de menaces et de harcèlement, ainsi qu'à plus haut niveau lorsque les agences sont contraintes de partager des données pour obtenir l'autorisation d'intervenir dans un pays ou dans une région spécifique d'un pays. Il convient également de garder à l'esprit que les données partagées avec un service spécifique du gouvernement peuvent ensuite être transmises à d'autres services du gouvernement. De même, les entités tenues au partage avec les gouvernements peuvent être contraintes de partager les données que vous collectez.

N'oubliez pas que la composition des gouvernements évolue, si bien qu'un partage des données a priori sans risque aujourd'hui peut poser problème l'année suivante. C'est pourquoi les bonnes pratiques préconisent de minimiser les données et de limiter leur partage, comme indiqué dans la Fiche-conseil 2 sur la gouvernance des données. Un changement de gouvernement doit servir d'événement déclencheur pour réviser et éventuellement actualiser votre évaluation DPIA.

Reportez-vous à **l'étude de cas sur le partage de données avec des gouvernements** du CaLP.

ÉVALUER LES RISQUES ET LES AVANTAGES DU PARTAGE DES DONNÉES ET DE LA COLLABORATION AU SEIN D'UN CONSORTIUM OU D'UN GROUPE DE TRAVAIL SUR LES TRANSFERTS MONÉTAIRES

S'ils sont réalisés correctement, avec une attention suffisante à la protection des données, le partage des données et l'utilisation de systèmes communs et interopérables peuvent faciliter le processus de mise en œuvre des transferts monétaires et réduire le risque de doublon et la fraude. Les Orientations opérationnelles de l'IASC sur la gestion responsable des données recommandent par exemple de créer des protocoles de partage des informations au niveau de l'intervention (via les équipes ICCM ou HCT). Il est également conseillé de créer des protocoles de partage des informations spécifiques aux groupes de travail sur les transferts monétaires dans les contextes où cela s'avère utile. Parallèlement, comme les données confèrent un certain pouvoir, le choix du système à utiliser et des personnes autorisées à accéder et à gérer les données dans

41 A. Doornbos (2020), Data Sharing with Partners.
42 R. Goodman et al. (2020), Review and Analysis of Identification and Registration Systems in Protracted and Recurrent Crises.

ce système est souvent source de conflits au sein des consortiums ou des groupes de travail sur les transferts monétaires. En outre, les systèmes uniques et le partage accru des données peuvent exposer les données des bénéficiaires des transferts monétaires à des violations de la vie privée et se révéler directement préjudiciables en cas de violations des données ou de partage avec des acteurs qui en font un usage abusif.

Les consortiums et/ou les membres des groupes de travail sur les transferts monétaires ont souvent des difficultés à collaborer et à partager des données les uns avec les autres. Comme indiqué dans la Fiche-conseil 1 sur le contexte et la capacité, le processus d'identification des personnes/entités qui supervisent l'intervention et de qui partage des données avec qui est source de tensions en matière de pouvoir et de contrôle sur une intervention, d'accès actuel et futur au financement des bailleurs et d'approches sur le respect de la vie privée des bénéficiaires de transferts monétaires, et suscite différentes préoccupations à cet égard. Certaines organisations émettent des réserves quant à la quantité de données collectées auprès des bénéficiaires de transferts monétaires, à l'inclusion (ou non) de données biométriques et à l'adéquation du niveau de sécurité des systèmes de données gérés par les autres acteurs. De plus, les partenaires de mise en œuvre financés par les Nations Unies peuvent voir leur participation à une intervention conditionnée au partage des données avec les agences des Nations Unies. Des tensions sont indiscutablement à l'œuvre lorsqu'un financement est conditionné à des modalités de partage des données, car la fourniture, l'accès et le contrôle des données est politique et implique une dynamique de pouvoir.

Bien que chaque organisation dispose de ses propres systèmes, si le partage des données fait partie d'un programme de transferts monétaires, les données devront être interopérables afin de pouvoir alimenter un système commun de gestion des informations. S'accorder sur les données à recueillir et sur la façon de les structurer pour rendre leur utilisation efficace est un autre aspect problématique du partage des données.

Certains acteurs des transferts monétaires, consortiums et groupes de travail sur les transferts monétaires inventent de nouvelles façons de partager les données dans le cadre d'accords de partage des données établis. Par exemple, si les organisations n'ont pas conclu d'accord de partage de données entre elles, mais si chacune a un accord de partage de données avec une agence tierce, elles peuvent décider de partager les données avec cette agence tierce qui pourra alors faire office de passerelle sans contrevenir aux accords juridiques et de partage de données. D'autres membres du groupe de travail sur les transferts monétaires expérimentent différentes façons de partager les données de manière anonyme, par exemple par l'intermédiaire d'un « hash » sécurisé ou en recourant à la technologie « blockchain ». En Turquie, le programme de filet social de sécurité d'urgence repose sur une architecture d'informations partagée pour les données des différents partenaires, harmonisant les systèmes d'informations sans pour autant partager les données avec l'ensemble des acteurs. Les acteurs des transferts monétaires peuvent également établir des protocoles de partage des informations ou des procédures opérationnelles standard régissant la manière dont les données sont partagées entre et parmi les agences.

Il est possible de se référer à la législation sur la protection des données pour éclairer les décisions sur la gestion des données. Les entités en charge du contrôle des données sont responsables en cas de violations des données ou d'autres violations de la vie privée. Elles gèrent également toute demande de redevabilité formulée par les populations affectées. En désignant l'entité en charge du contrôle des données et l'entité en charge du traitement des données, ou éventuellement les entités de contrôle conjointes, les organisations peuvent trouver un terrain neutre sur lequel débattre ouvertement des thématiques du pouvoir et de la redevabilité (reportez-vous à la Fiche-conseil 2 et aux Encadrés 10 et 11 sur les entités de contrôle et de traitement des données).

EXAMINER LES POLITIQUES DES PSF ET DES AUTRES PARTIES AVANT D'ACCEPTER DE PARTAGER DES DONNÉES

Les modalités des transferts monétaires ayant évolué pour inclure davantage de PSF et d'opérateurs de téléphonie mobile, les acteurs des transferts monétaires partagent régulièrement les données personnelles des participant-e-s au programme avec les PSF et les gouvernements des pays hôtes pour répondre aux exigences KYC, entre autres. Ces données peuvent inclure des noms, des numéros de téléphone ou des numéros d'identification, ainsi que des données biométriques, comme cela est de plus en plus fréquent. Les PSF conservent souvent des registres sur les transactions, en plus des données personnelles. De tels registres consignent où et quand les achats ont été réalisés, ainsi que des informations sur l'épargne et les dépenses. Ces données transactionnelles doivent être protégées contre toute utilisation abusive. Il est important que les acteurs des transferts monétaires aient une vision claire des données que les PSF recueilleront sur les participant-e-s au programme dans le cadre de leurs services et qu'ils évaluent au cours du processus DPIA ou RBA les risques potentiels que cela pourrait représenter pour les populations affectées. Les conditions de partage des données doivent être explicites dans tout contrat, tout comme les dispositions en matière de responsabilité en cas de violation ou de fuite des données.

Lors de l'instauration d'accords de partage de données avec des partenaires du secteur privé (notamment des PSF et des opérateurs de téléphonie mobile), veillez à examiner leurs conditions générales et leurs politiques de partage des données et à inclure des conditions strictes dans votre propre accord afin que la protection et la gestion responsable des données au sens large suivent des normes adéquates, avec par exemple des restrictions sur le partage, l'utilisation, la conservation et la destruction des données par la suite. Les contrats de certains prestataires peuvent inclure une clause par défaut autorisant « le partage avec une tierce partie », si bien qu'ils pourront à l'avenir partager les données avec quiconque. Ces prestataires sont également susceptibles d'avoir une clause stipulant qu'en cas de vente ou d'acquisition de l'entreprise, toutes les données en leur possession feront partie intégrante des actifs concernés par cette vente ou cette acquisition.

Si vous n'êtes pas à l'aise avec ce scénario, clarifiez ce point en amont de tout partage de données ou de tout accord de partenariat. Il peut être tout à fait raisonnable de s'opposer à une politique de partage des données par défaut et de rendre l'accès aux données d'un programme de transferts monétaires plus réfléchi et adapté aux besoins spécifiques de la tierce partie.

Les partenaires du secteur privé doivent faire l'objet d'évaluations de diligence raisonnable en amont de tout partage de données.

Les PSF et autres tierces parties peuvent s'opposer aux restrictions concernant le partage et l'utilisation ultérieure des données. Ils peuvent dans certains cas invoquer des motifs légitimes (par exemple, s'ils sont légalement tenus de partager des données KYC ou autres avec le gouvernement). Dans d'autres cas, leur modèle commercial peut reposer sur les profits issus des données, ce qui pourrait être incompatible avec la mission humanitaire. Si les exigences légales (comme les exigences KYC) ne sont pas négociables, il est en revanche possible d'ajouter des clauses qui interdisent l'utilisation des données sur les bénéficiaires de transferts monétaires à des fins de marketing ou de stipuler que les PSF doivent faire preuve de transparence et notifier les organisations en cas de demande de partage de données avec les autorités gouvernementales.

Les agences partenaires n'ont peut-être pas conscience des risques associés au partage des données. Il est donc important d'en discuter avant toute signature d'un accord de partage de données.

METTRE EN PLACE DES ACCORDS DE PARTAGE DE DONNÉES AVANT DE PARTAGER DES DONNÉES

Avant de partager des données, il est important de spécifier explicitement ce qu'il est autorisé ou non de faire avec les données. Ces précisions font généralement l'objet d'un accord de partage de données. Les accords de partage de données ne contiennent pas nécessairement d'informations spécifiques aux données de programme que vous collectez. Ils indiquent plutôt de manière explicite ce qu'il faut faire et ce qu'il ne faut pas faire lors d'un partage de données. Ils doivent inclure des normes minimales en matière de confidentialité et de sécurité des données et définir les responsabilités en cas de violation de la confidentialité des données, de violation de la sécurité des données, de mauvaise utilisation des données ou de partage sans autorisation.

L'élaboration d'un accord de partage de données peut nécessiter plusieurs mois, même en présence de conditions générales antérieures régissant la coopération entre les organisations et les agences. Cela tient notamment au caractère chronophage de la définition de normes interopérables. Par ailleurs, les organisations et les agences doivent généralement faire appel à leurs équipes juridiques, à leurs équipes de protection des données et à leurs équipes informatiques, ce qui peut nécessiter une implication à la fois au niveau national et mondial dans le cas d'organisations internationales. Bien que l'on observe une tendance à partager des données sans qu'aucun accord ne soit en place, il convient de préciser que le RGPD et d'autres réglementations sur la confidentialité des données imposent que soient établis des accords de partage de données et des accords de transfert de données. Dans certains cas, négocier des accords de partage des données est devenu un exercice de pouvoir des grandes organisations sur les plus petites.

Les informations sur le partage des données doivent être incluses dans les demandes de consentement ou dans les autres informations fournies aux populations affectées afin que ces dernières assimilent parfaitement ce à quoi elles consentent et ce qu'il adviendra de leurs données. Même si vous optez pour une base légale autre que « Consentement » pour le recueil des données, vous devez informer les bénéficiaires en toute transparence concernant toutes les parties avec lesquelles vous pourrez partager leurs données.

Lorsqu'une intervention d'urgence doit être déployée avant qu'un accord de partage de données ait pu être finalisé, vous pouvez être amené-e à partager un volume limité de données dans le cadre d'un protocole d'accord ciblé et limité dans le temps pour vous permettre de lancer l'intervention. Il s'agit là d'un compromis à étudier : est-il préférable de partager les données pour que l'intervention puisse être mise en place, ou le risque est-il trop élevé ? Dans de telles situations, vous pouvez opter pour une conception de programme de transferts monétaires la plus sobre possible en données.

Les accords de partage de données sont un outil essentiel de la gestion responsable des données. Dans la pratique, les mécanismes de redevabilité de ces accords peuvent toutefois être difficiles à mettre en œuvre, si bien qu'il y a peu de contrôle sur la façon dont les données sont utilisées ou partagées. C'est pourquoi il est important d'appliquer les principes de minimisation des données lorsque vous identifiez précisément les données à partager et avec qui les partager.

Le partage des données parmi les membres des groupes de travail sur les transferts monétaires, les consortiums, les gouvernements et les PSF doit être un élément clé de l'évaluation DPIA, PIA ou RBA menée lors des évaluations initiales du contexte et de la capacité et lors de la conception et de la planification des programmes. Vous devez également mener une étude de fond pour déterminer les niveaux de protection des données en vigueur lors des précédentes interventions et dans les systèmes de données envisagés pour une intervention conjointe.

Le HCR et le PAM ont élaboré un protocole d'accord sur le partage des données, disponible **ici**.

La question du partage des données est abordée dans le document **Data Responsibility Guide** d'OCHA.

ÉLABORER DES STRATÉGIES ET RÉPETER LES MESURES DE PRÉVENTION ET LA RÉPONSE AU « PARTAGE FORCÉ DES DONNÉES » ET À D'AUTRES INCIDENTS CRITIQUES EN MATIÈRE DE DONNÉES

Parallèlement au partage de données convenu, le « partage de données forcé » est une réalité dans de nombreux contextes de programmes de transferts monétaires. Votre personnel et vos partenaires locaux peuvent être contraints par divers moyens de partager leurs données avec des groupes cherchant à obtenir l'accès et le contrôle sur ces données. Il est également à craindre que certaines entités partagent des données qui ne devraient pas l'être, comme lorsque certaines organisations refusent de partager des données avec les gouvernements, qui parviennent toutefois à se les procurer par l'intermédiaire des PSF ou d'une autre agence partenaire. Il est essentiel d'identifier les domaines où le risque de partage forcé des données est avéré et de répéter comment vous-même et votre personnel devrez réagir.

Reportez-vous à la Fiche-conseil 2 (Concevoir et planifier) pour plus d'informations sur les incidents critiques en matière de données.

Le CaLP encourage les consortiums et les groupes de travail sur les transferts monétaires à collaborer et à définir conjointement des stratégies sur la conduite à tenir face aux incidents courants en matière de données dans leur contexte, mais aussi à consigner ces incidents dans un registre pour permettre d'intensifier les recherches et les apprentissages sur les bonnes pratiques. Reportez-vous à **l'initiative de gestion des incidents critiques en matière de données du CaLP** pour plus d'informations.

OPÉRATIONNALISER VOS ACCORDS DE PARTAGE DE DONNÉES

Rédiger des accords de partage de données est une chose, mais veiller à leur mise en œuvre en est une autre. Les organisations doivent s'assurer que leur personnel et leurs partenaires connaissent la teneur des accords de partage de données et autres accords conclus avec les bailleurs, les gouvernements et les PSF concernant les données, de sorte que les organisations ne partagent pas ni ne gèrent les données en dehors du cadre de ces accords et de sorte que les partenaires respectent les termes convenus.

Les accords de partage de données demandent beaucoup de temps et d'efforts et peuvent être difficiles à mettre en place. Ils devront être validés par les équipes juridiques et les bureaux en charge de la protection des données, ce qui peut impliquer de nombreuses phases de révision. Il est important d'inscrire les accords de partage de données dans les premières étapes de votre intervention et d'affecter les ressources correspondantes afin de disposer dès le départ du personnel et du temps nécessaires.

Prévoyez un moment dès le début du processus pour examiner les accords avec les partenaires et discuter des attentes en matière de gestion des données et des restrictions sur le partage des données. Dispensez une formation, au besoin. Vous devrez peut-être renforcer les capacités les partenaires ou mettre d'autres ressources à leur disposition s'ils ont besoin d'améliorer leurs compétences, leurs connaissances ou leurs systèmes pour mettre en œuvre et respecter les exigences en matière de partage sûr et responsable des données.

FICHE-CONSEIL 7

ACTUALISER/CONSERVER/SUPPRIMER LES DONNÉES

Tout au long du cycle du programme, les données collectées devront être enregistrées et conservées en toute sécurité, comme indiqué dans la Fiche-conseil 4. Au terme d'une intervention, les données devront être conservées ou détruites, selon la situation. Votre organisation doit conserver les données personnelles et sensibles uniquement pendant la durée nécessaire. Il est en général préférable que les données personnelles soient anonymisées ou agrégées le plus tôt possible. Lorsque les données ne sont plus requises sur le plan légal ou pour d'autres motifs légitimes, vous devez les détruire en toute sécurité.

PLANIFIER ET BUDGÉTISER LA MAINTENANCE, LA CONSERVATION ET LA DESTRUCTION DES DONNÉES DÈS LE DÉPART

Même si la conservation et la destruction des données ne surviennent qu'à la fin du programme ou à la fin du cycle de vie des données, vous devez planifier ces opérations dès les premiers stades de la conception et de la planification afin d'affecter les budgets adéquats. Tout défaut de planification expose les participant-e-s à des risques ou peut vous contraindre à conserver les données plus longtemps que nécessaire. Pour une planification adéquate, vous devez comprendre les besoins de toutes les parties prenantes. Même au sein d'un même programme, les différentes équipes peuvent avoir des besoins différents en matière de conservation des données. Par exemple, les services en charge des finances et de la conformité peuvent avoir besoin d'accéder aux données du programme en cas d'audit d'un bailleur des années après la fin d'un programme. Le personnel du programme, quant à lui, peut ne plus avoir besoin des données dès le programme terminé.

Pour répondre aux besoins de toutes les équipes en matière de données, il est important de parvenir à une compréhension commune des besoins de chaque équipe concernant la conservation des données avant la fin du programme et de s'assurer de la bonne coordination des systèmes utilisés pour recueillir et enregistrer les données du programme de bout en bout.

CONSERVER UNIQUEMENT LES DONNÉES DONT VOUS AVEZ BESOIN, AU DEGRÉ DE GRANULARITÉ REQUIS, ET DÉTRUIRE LE RESTE

Les programmes de transferts monétaires impliquent de recueillir un volume conséquent de données. Selon le type de votre programme et votre structure de financement, vous pouvez être amené-e à conserver certaines données pour justifier les décisions, aux fins

La Fiche-conseil 7 fournit des directives pour une conservation et une destruction responsables des données.

(La Fiche-conseil 4 sur la transmission et le stockage donne plus d'informations sur la sécurisation des données lors d'une intervention en cours.)

d'audit, ainsi que pour le suivi, l'évaluation et l'apprentissage. Les responsables de programme peuvent hésiter à supprimer des données par crainte de supprimer des informations importantes. Si cela peut être un risque, conserver les données trop longtemps n'est pas non plus sans risque. Plus elle détient de données personnelles et sensibles, plus une organisation assume de risques et de responsabilités, et plus le risque de fuite ou d'utilisation abusive ou malintentionnée des données des bénéficiaires de transferts monétaires est grand. En outre, avec le temps et les mouvements de personnel, il devient de plus en plus difficile de s'assurer que les données sont exactes, que les nouveaux membres du personnel connaissent les limites placées sur certains jeux de données et que la source des données et les autorisations correspondantes puissent faire l'objet d'un suivi précis. De plus, une organisation qui détient des données en est responsable et doit être en mesure de répondre aux demandes d'accès des participant-e-s à leurs données personnelles. Plus une organisation détient de données, plus cette responsabilité est lourde à assumer.

Votre organisation a peut-être déjà une politique générale de conservation des données, qui doit inclure les données sur les transferts monétaires. Si vous travaillez au sein d'un consortium plus large, il faudra convenir d'une politique de conservation des données avec l'ensemble des membres. Le Groupe de travail sur les transferts monétaires peut être tout indiqué pour déterminer à quel stade du cycle du programme certaines données doivent être agrégées et discuter des délais convenables pour détruire certains types de données. Il vous faudra définir des conditions claires pour la conservation et la destruction des données dans vos différents documents d'orientations, protocoles d'accord, accords de partage et de transfert de données, etc.

S'il peut être tentant de conserver les listes de bénéficiaires de transferts monétaires sur de longues périodes, ces listes perdent de leur pertinence au fil du temps et ne seront plus utiles pour cibler et distribuer des espèces si elles ne sont pas mises à jour.

On parle de Plan de conservation des données, ou encore de Plan de conservation, d'archivage et de destruction. Reportez-vous à la fiche-conseil **Data Starter Kit** d'ELAN pour plus de conseils à cet égard et pour voir des exemples de tels plans.

www.calpnetwork.org

Mars 2021