PROTÉGER LA VIE PRIVÉE DES BÉNÉFICIAIRES

Principes et normes operationnelles pour une utilisation securisee des donnees personnelles dans les programmes de transfert monetaire et electronique

CaLP
The Cash Learning Partnership

CONTEXTE DES PRINCIPES

Photo: Geoff Sayer/Oxfam

L'utilisation des transferts électroniques dans les programmes de transfert monétaire (PTM) s'est accrue dans la sphère humanitaire ; ces transferts sont de plus en plus reconnus comme un type d'intervention rentable et efficace dans certains contextes d'urgence. En 2011, le Cash Learning Partnership (CaLP) a émis des recommandations dans ses recherches sur le thème des transferts électroniques, dans le rapport Les nouvelles technologies dans les programmes de transfert monétaire et l'aide humanitaire1 (Smith, G. et al, 2011). En suivant ces recommandations et l'intérêt qu'a manifesté la communauté de pratique à l'égard du document, le CaLP a entrepris trois autres études sur cette thématique en 2013, dont le présent rapport fait partie. Les deux autres documents abordent le développement de directives sur les transferts électroniques et une étude des facteurs qui affectent l'efficacité par rapport aux coûts de ce type de transfert par rapport à des méthodes plus manuelles.

Les transferts électroniques sont porteurs de risques inhérents relatifs à la collecte et au traitement des données personnelles des bénéficiaires. Toutefois, à ce jour, ces risques sont largement méconnus et ils font l'objet de peu de solutions. Les pratiques des organisations sont rarement codifiées et souvent laissées à la gestion des équipes, avec pour mot d'ordre de « ne pas nuire » et néanmoins, peu de directives pratiques. Les publications récentes telles que *Humanitarianism in a Network Age* (OCHA, 2013) et *Standards professionnels pour les activités de protection* (CICR, 2013) mettent en évidence cette appréhension.

Avisé par ce contexte, le CaLP s'est lancé dans l'élaboration d'une série de principes et normes opérationnelles, qui visent à contribuer à des transferts électroniques et monétaires éthiques ainsi qu'à garantir que le recours aux données des bénéficiaires respecte certains principes.

[1] Voir le site web du CaLP : http://www.cashlearning.org/resources/library/272-new-technologies-in-cash-transfer-programming-and-humanitarian-assistance?keywords=new+technologies&country=all&sector=all&modality=all&language=all&payment_method=all&document_type=all&searched=1&x=0&y=0

La mise au point des principes et des normes opérationnelles a été menée par Kokoévi Sossouvi (consultante indépendante) qui s'est aidée de contributions de nombreuses parties prenantes, dont un groupe de travail technique. Le processus a intégré une revue documentaire qui portait, entre autres, sur : les normes essentielles humanitaires et du secteur privé ; les codes et les directives opérationnelles, ainsi que les outils liés à la lutte contre le blanchiment d'argent et le financement du terrorisme. Cette revue traitait également : d'un sondage en ligne sur les politiques générales et pratiques actuelles de gestion des données utilisées par les praticiens ; d'une cartographie des parties prenantes ; et d'un processus d'ébauche qui a bénéficié de conseils juridiques de la part d'Oxfam GB, de Save the Children UK et d'ACF France. Suite à l'intégration de commentaires et recommandations émis par de nombreuses parties prenantes, une table ronde a été organisée en vue de traiter et débattre du contenu de l'avant-dernière ébauche de document, ainsi que des prochaines étapes pour la finalisation et l'adoption du document. Le présent rapport s'appuie sur les résultats de la table ronde.

Remerciements

Le CaLP souhaite remercier Kokoévi Sossouvi (consultante indépendante), Mike Parkinson (Oxfam GB), Carly Nyst (Privacy International), Alexander Beck (UNHCR) et Kate Lauer (consultante indépendante), entre autres collaborateurs pour leur contributions et recommandations lors de l'élaboration de ce document.

Étant donné qu'un processus fondé tout particulièrement sur la consultation a été appliqué pour élaborer ce rapport, le CaLP a considérablement bénéficié de l'expérience juridique et technique de nombreuses personnes et des organisations pour lesquelles elles œuvrent, notamment : l'IRC, ACF, C-Gap, Smart Campaign, Vodafone, GSMA, OpenRevolution, la FISCR, le CNR et le PAM. Le CaLP souhaite remercier toutes ces personnes (qui se reconnaîtront) ainsi que l'ensemble de la communauté de pratique, pour avoir répondu aux questions liées à ce travail posées sur les D-Groups.

Membres du groupe de travail technique qui ont apporté une vue d'ensemble et leur soutien, et qui ont consacré du temps ainsi que de l'énergie :

Ruth Aggiss et Jessica Saulle, Save the Children UK

Jenny Aker, Tufts University

Simon Clements, Programme alimentaire mondial

Olivia Collins, Fonds des Nations unies pour l'enfance (anciennement au sein du Somalia Cash Consortium)

Hanna Mattinen, Agence des Nations unies pour les réfugiés

Hamilton McNutt, NetHope

Julien Morel, Action Contre la Faim

Sasha Muench, Mercy Corps

Gabrielle Smith, Concern Worldwide

En plus des personnes ci-dessus, l'élaboration de ce document n'aurait pas été possible sans l'aide financière de Visa Inc. et du DFID..

Prochaines étapes

Le CaLP souhaite recevoir des commentaires liés à l'utilisation des principes définis dans ce document. Il invite gracieusement les organisations à faire part de leur point de vue et de leur expérience de programme à l'adresse info@cashlearning.org, ainsi qu'à rejoindre le groupe de discussion CaLP (via le lien sur le site web www.cashlearning.org/francais/accueil).

En outre, nous rappelons aux lecteurs que d'importantes ressources sont disponibles sur le site web du CaLP : des études de cas et des rapports sur l'utilisation des nouvelles technologies, des directives sur les programmes de transfert monétaire (PTM), en passant par des recherches sur le recours aux PTM et sur les analyses de marché.

PROTEGER LA VIE PRIVEE DES BENEFICIAIRES : PRINCIPES ET NORMES OPERATIONNELLES POUR UNE UTILISATION SECURISEE DES DONNEES PERSONNELLES DANS LES PROGRAMMES DE TRANSFERT MONETAIRE ET ELECTRONIQUE

A OBJECTIF

Le droit à la vie privée par le biais de la protection des données personnelles n'est pas uniquement un droit important en soi mais aussi un élément clé de l'autonomie et de la dignité de chacun. La protection et le respect de la vie privée représentent un facteur habilitant considérable pour les libertés politiques, spirituelles, religieuses et même sexuelles. Plusieurs instruments internationaux renferment des principes de protection des données, comme par exemple la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales par le biais de son Article 8[2], ainsi que de nombreux corps législatifs nationaux ont intégré de tels principes aux lois nationales.

Les principes et les normes opérationnelles présentées dans ce document ont été mis au point par le Cash Learning Partnership afin de permettre aux organisations de répondre à ces normes internationales et de les respecter. Cela leur permettra, en particulier, de lutter contre les risques inhérents à l'utilisation des données des bénéficiaires par les organisations engagées dans la distribution d'argent avec une attention particulière sur les programmes de transfert électronique.

Ces risques sont associés à la collecte, au stockage, à l'utilisation et à la divulgation des données des bénéficiaires à l'occasion de la réception de transferts monétaires et électroniques. Ces données personnelles sont souvent plus volumineuses que celles rassemblées lors de distributions d'aide conventionnelles ; elles sont systématiquement partagées avec des partenaires commerciaux (ou générées par ces derniers) qui contribuent à la distribution de l'argent à l'aide de nouvelles technologies.

De manière générale, à ce jour, ces risques sont largement méconnus et ils font l'objet de peu de solutions. Néanmoins, à mesure que les initiatives humanitaires adoptent de plus en plus les nouvelles technologies en vue d'améliorer l'efficacité de la distribution d'aide, il est essentiel de mettre en place des normes. Celles-ci permettront de garantir que les bénéficiaires (ceux que les organisations cherchent à aider) ne sont pas exploités, mis en danger ou désavantagés par leur implication dans des programmes de transfert monétaire.

Ces principes et normes opérationnelles sont une tentative d'établir de bonnes pratiques au sein du secteur, pour la collecte et le traitement des données des bénéficiaires. Pour les raisons citées ci-dessus, ces principes et normes sont spécialement adressés aux responsables de programmes de transfert monétaire et électronique mais ils peuvent avoir une plus vaste application. Leur but n'est pas de détrôner ou remplacer les principes directeurs organisationnels existants en matière de vie privée ou de protection des données, mais de les renforcer ou de les compléter lorsqu'elles n'abordent pas la protection des données des bénéficiaires ou qu'elles manquent de précision. Lorsqu'il n'existe pas de principes directeurs organisationnels sur la vie privée ou la protection des données, les normes et principes énoncés dans ce document constituent un cadre permettant de protéger les données des bénéficiaires.

Étant donné la variété de juridictions potentielles dans le cadre desquelles ces principes et normes opérationnelles pourraient être appliqués, ces derniers peuvent uniquement faire office de conseils sans constituer des recommandations juridiques. En cas de doute au sujet des normes juridiques qui pourraient s'appliquer, il est suggéré de faire appel à un avis juridique indépendant. Le CaLP s'est efforcé de garantir que ces principes et normes répondent aux exigences de certains cadres légaux majeurs mails il ne peut assurer la satisfaction des exigences de certains pays en matière de divulgation, cryptage ou transfert de données par l'intermédiaire d'une série unique de principes consultatifs.

[2] Voir la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (N°108), 1981 ; les Lignes directrices de l'Organisation de Coopération et de Développement Économiques régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel (1980) ; et les Lignes directrices des Nations unies relatives au traitement électronique des données à caractère personnel (E/CN.4/1990/72, résolution 45/95 de l'Assemblée générale)

B METTRE LES PRINCIPES EN PRATIQUE

L'une des principales difficultés rencontrées lors de l'élaboration de ce document consistait à savoir comment produire des directives utiles et applicables que les praticiens trouveraient nécessaires et pertinentes vis-à-vis de leurs façons de travailler, tout en décrivant une activité réglementée.

Les praticiens consultés au cours du développement de ce rapport ont confié qu'ils souhaitaient des directives pratiques, qui répondaient à la réalité quotidienne du travail de programme, souvent entrepris en temps de crise et d'insécurité opérationnelle ainsi qu'avec des bénéficiaires qui ont grandement besoin d'aide. Tout le long du document, et notamment en lien avec les principes, il était nécessaire d'établir un équilibre quant à l'utilisation des cadres légaux et d'un langage réglementaire organisationnel (une demande faite par les chargés du respect des principes), ainsi que de garder ce document pratique et approchable par un groupe large (demandes des praticiens). Le CaLP s'est efforcé d'exprimer les principes fondamentaux d'une façon qui se rapporte à la manière de penser des praticiens afin de les rendre accessibles tout en gardant à l'esprit que le traitement des données personnelles est une activité réglementée dans de nombreux pays. On peut espérer que les références indiquées dans la partie « Normes opérationnelles » et dans les encadrés informeront les praticiens des détails du cadre légal et répondront aux besoins des personnes en charge du respect des principes. Les commentaires[3] des praticiens et des personnes en charge du respect des principes sont les bienvenus. En effet, nous reconnaissons qu'il s'agit d'une appréciation personnelle qui appelle à une vigilance constante.

En plus de lier les besoins des programmes aux cadres réglementaires, nous sommes également conscients du fait que, dans certaines circonstances, des frais supplémentaires peuvent être imputés ou de nouvelles compétences peuvent être requises en vue d'atteindre les normes fixées dans ce document. Le fait de respecter les normes n'entraîne pas toujours un coût nul, même si l'on s'attend à réussir beaucoup de choses simplement en améliorant l'organisation, la planification et la conception des programmes. Ainsi, certaines personnes interrogées lors de notre processus de consultation ont affirmé qu'elles collectaient trop de données des bénéficiaires. D'autres souhaitaient s'assurer que lorsque l'on se réfèrerait, dans le présent rapport, aux normes opérationnelles sur la sécurité, on intègrerait celles-ci aux ressources institutionnelles existantes, telles que des systèmes informatiques organisationnels de sécurité, plutôt que d'encourager les équipes de programmes monétaires à créer leurs propres systèmes de sécurité.

C DEFINITIONS

Pour les besoins de ce document, les données personnelles ont été définies de manière générale comme étant toute donnée qui identifie ou peut être utilisée pour identifier une personne vivante. Cette désignation est dérivée de cadres réglementaires et de législations sur la protection des clients, et elle peut inclure les données personnelles financières. Si l'on établit que l'un des principes consiste à s'assurer de la qualité et de la précision des informations, on permet d'appliquer l'ensemble des principes à d'autres formes de données : données financières et de transaction (dont les soldes de compte), schémas et calendrier des dépenses, reçus, taux d'activité, etc. Ces données peuvent ne pas toujours être personnelles mais elles sont relatives à l'efficacité opérationnelle.

D FLUX DES DONNEES ET TRANSFERTS INTER-ORGANISATIONNELS

En parallèle de la collecte et de l'utilisation sécurisées des données personnelles au sein des organisations, la problématique de la protection des données est particulièrement pertinente, étant donné la complexité du flux d'informations entre les organisations, que ce soient des partenaires qui rassemblent les données pour des organisations de mise en œuvre ou des organisations commerciales engagées dans l'optique d'aider à appliquer des programmes (voir schéma 1). La mise au point et l'analyse des flux de données, en plus de l'utilisation des évaluations d'impact sur la vie privée (voir encadré 2 et annexe 1) contribueront à analyser les risques liés aux programmes de transfert monétaire. Nous recommandons fortement d'y avoir recours.

[3] Merci de contacter le CaLP à l'adresse : info@cashlearning.org, avec pour titre de message : « Principles and Operational Standards » (principes et normes opérationelles)

E STATUT DU DOCUMENT, RECOMMANDATIONS SUR SON UTILISATION ET SON APPLICATION

Ces principes et normes opérationnelles ont été élaborés par le Cash Learning Partnership avec le soutien financier du DFID et de Visa Inc. Veuillez noter que le contenu est sous la responsabilité du CaLP et ne reflète pas nécessairement le point de vue du DFID ni de Visa Inc.

On suppose une adoption des principes et normes par les organisations non gouvernementales et inter-gouvernementales qui mettent en œuvre des programmes de transfert monétaire et électronique. Toutefois, ils peuvent être utilisés dans presque tous les programmes humanitaires.

Les principes et normes opérationnelles ne sont pas soumis à un suivi ou au respect externes par le CaLP. Nous suggérons aux organisations qui adoptent ces normes d'y recourir pour les audits internes et/ou externes, les évaluations et les études de programme, ainsi que pour faire la promotion de leur application par le biais de documents publics tels que les rapports annuels ou de sites web. Ces publications servent de preuves des conditions d'utilisation et des tentatives de respect des normes.

Il est recommandé, avant l'adoption de ces principes et normes opérationnelles par une organisation, que son conseil d'administration ou de direction le décide formellement et qu'il établisse un mécanisme d'étude et de reporting en matière de respect des principes. De plus, on suggère de nommer des points focaux organisationnels pour les problèmes qui relèvent de la gestion des données au niveau national, régional et du siège. Un modèle de résolution sur cette question est proposé ci-dessous.

Modèle de résolution à utiliser par les conseils des organisations qui souhaitent adopter les principes.

« *Il est décidé que [nom de l'organisation] :*

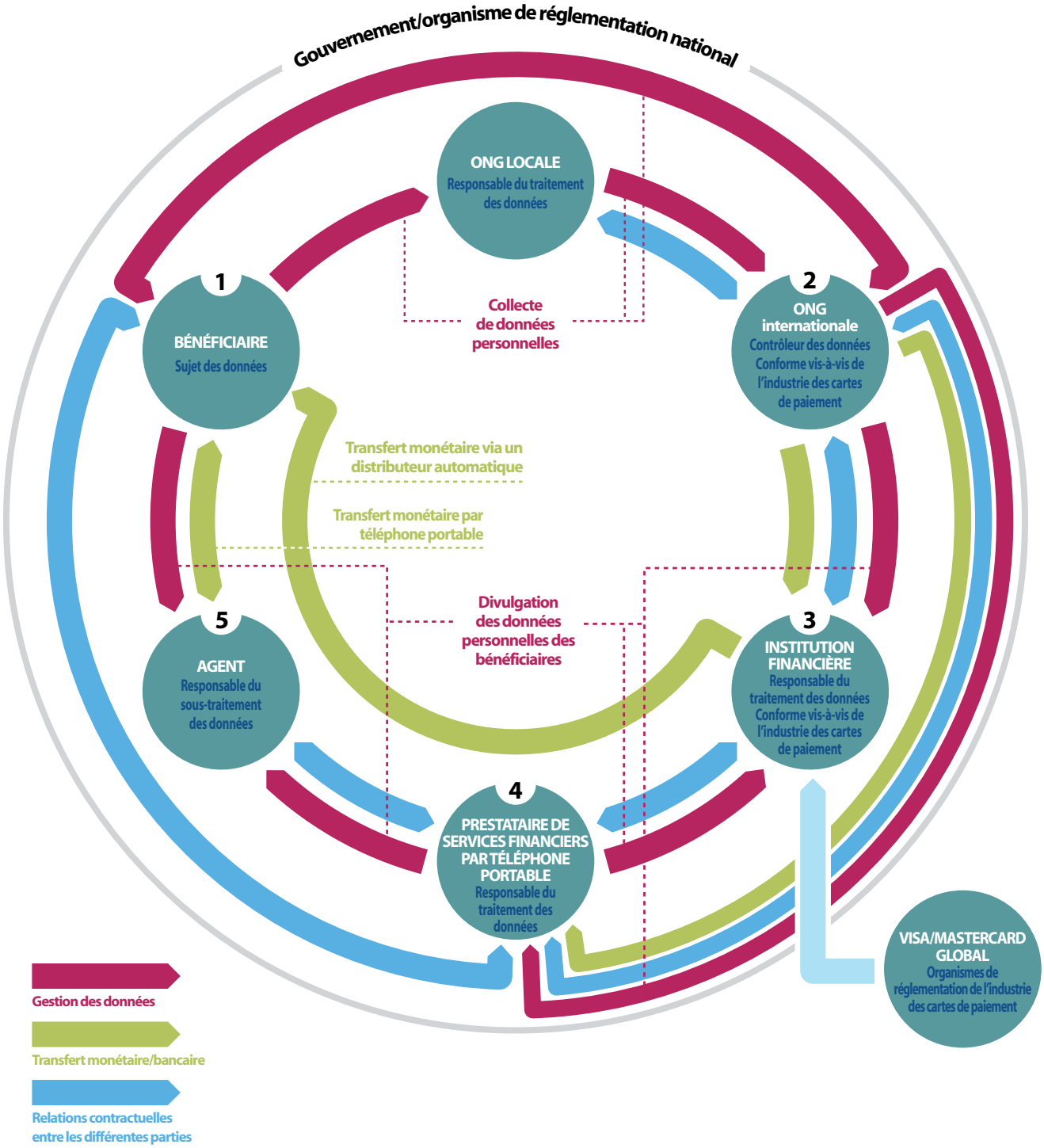
- adoptera et mettra en œuvre les principes et normes opérationnelles définis par le Cash Learning Partnership pour l'utilisation sécurisée des données des bénéficiaires dans les programmes de transfert monétaire et électronique ;
- chargera [nom de l'équipe ou service responsable de la mise en œuvre des principes] de s'assurer que [nom de l'organisation] établit des procédures internes fiables et de garantir ainsi que [nom de l'organisation] respecte les principes ;
- inclura l'adoption des principes et leur respect dans son rapport annuel ;
- informera le [conseil d'administration ou de direction, etc.] de toute violation des principes ;
- soumettra l'adoption des principes et leur respect à l'examen périodique du [conseil d'administration ou de direction, etc].

G MAINTENIR LES NORMES ET L'EMISSION DE COMMENTAIRES

Les organisations qui adhèrent à ces principes sont priées d'en informer le CaLP. Cela permettra au consortium de conserver une base de données des organisations qui les ont adoptés, puisque ce document est soumis à un réexamen. Il serait également utile au CaLP que les organisations qui adhèrent à ces mesures fassent un compte rendu de leur expérience en termes d'adoption des principes et de mise en pratique des normes opérationnelles. Voici l'adresse de contact pour ces comptes-rendus : info@cashlearning.org. Merci d'indiquer comme titre : « Principles and Operational Standards » (principes et normes opérationelles).

À mesure que les pratiques évoluent et que l'on gagne en expérience, on peut modifier les principes, les renforcer pour en faire un code de pratiques indépendant ou l'intégrer à d'autres normes existantes. Le CaLP apprécierait de recevoir tout commentaire sur l'application ou utilisation future de ce document.

Schéma 1 : approximation des flux de données donnant un aperçu combiné des transferts par carte (distributeur automatique) et par téléphone portable réalisés avec un partenaire local



Sujet des données : les bénéficiaires de transferts monétaires électroniques mis en œuvre par l'organisation et les personnes auxquelles se rapportent les données.

Contrôleur des données : la personne, au sein de l'organisation, qui détermine les objectifs et les con-ditions du traitement actuel ou futur des données personnelles.

Responsable du traitement des données : l'affilié ou prestataire de services ; personne qui réalise le traitement des données personnelles pour le contrôleur des données, au cours de la prestation des ser-vices

Responsable du sous-traitement des données : l'entité à laquelle le responsable du traitement des don-nées délègue tout ou partie du traitement des données requis par le contrôleur des données.

PRINCIPES POUR UNE UTILISATION SECURISEE DES DONNEES PERSONNELLES DANS LES PROGRAMMES DE TRANSFERT MONETAIRE ET ELECTRONIQUE

1 RESPECTER LA VIE PRIVEE

Principe : les organisations doivent respecter la vie privée des bénéficiaires et reconnaître que l'obtention et le traitement de leurs données personnelles représentent une menace potentielle à cette vie privée.

2 PROTEGER LES DONNEES DE FAÇON ANTICIPEE

Principe : les organisations doivent protéger de façon anticipée les données personnelles qu'elles obtiennent des bénéficiaires, que ce soit pour leur propre utilisation ou celle de tierces parties, pour chaque programme de transfert monétaire ou électronique qu'elles lancent ou mettent en œuvre.

3 COMPRENDRE LES FLUX ET LES RISQUES LIES AUX DONNEES

Principe : les organisations doivent analyser, documenter et comprendre le flux de données des bénéficiaires pour chaque programme de transfert monétaire ou électronique qu'elles lancent ou mettent en œuvre en leur sein, ainsi qu'entre elles-mêmes et d'autres organisations. Elles doivent également élaborer des stratégies d'atténuation des risques qui peuvent s'avérer nécessaires pour pallier tout risque créé à partir de ces flux.

4 GARANTIR LA QUALITE ET LA PRECISION DES DONNEES

Principe : les organisations doivent garantir la précision des données personnelles qu'elles rassemblent, stockent et utilisent. À cette fin, elles doivent entre autres garder les informations à jour, pertinentes et avec un volume raisonnable par rapport à l'objectif fixé, et ne pas les conserver plus longtemps que nécessaire.

5 OBTENIR LE CONSENTEMENT OU INFORMER LES BENEFICIAIRES DE L'UTILISATION DE LEURS DONNEES

Principe : au moment de la collecte de données, les bénéficiaires doivent être informés de la nature des informations recueillies, des acteurs avec lesquels elles seront partagées, et du responsable de la sécurité de leur utilisation. Ils doivent avoir la possibilité de contester l'utilisation des données et de se retirer du programme s'ils ne souhaitent pas que l'on ait recours à leurs données personnelles pour les fins décrites.

6 GARANTIR LA SECURITE DES DONNEES

Principe : les organisations doivent instaurer des normes de sécurité techniques et opérationnelles adaptées pour chaque étape de la collecte, de l'utilisation et du transfert des données des bénéficiaires. Le but est d'empêcher l'accès non autorisé aux informations, leur divulgation ou leur perte. Il convient notamment d'identifier toute menace extérieure et de prendre des mesures pour atténuer tout risque qui viendrait à apparaître.

7 PREVOIR LA SUPPRESSION DES DONNEES

Principe : les organisations ne doivent pas conserver les données des bénéficiaires plus longtemps que nécessaire, à moins qu'elles ne présentent des raisons claires, justifiables et documentées. Autrement, les données détenues par les organisations et les tierces parties concernées doivent être détruites.

8 GARANTIR LA REDEVABILITE

Principe : les organisations doivent établir un mécanisme par lequel un bénéficiaire peut demander des informations concernant les données personnelles que détient une organisation à son sujet, de même que des mécanismes pour recevoir et répondre à toute plainte ou inquiétude que les bénéficiaires pourraient formuler à l'égard de l'utilisation de leurs données personnelles.

NORMES OPERATIONNELLES POUR UNE UTILISATION SECURISEE DES DONNEES PERSONNELLES DANS LES PROGRAMMES DE TRANSFERT MONETAIRE ET ELECTRONIQUE

1 RESPECTER LA VIE PRIVEE

Principe : les organisations doivent respecter la vie privée des bénéficiaires et reconnaître que l'obtention et le traitement de leurs données personnelles représentent une menace potentielle à cette vie privée.

Norme opérationnelle : note interprétative

Les organisations doivent :

- garantir que la responsabilité de la protection des données des bénéficiaires et le respect des normes définies dans ce document sont attribués à un poste ou rôle spécifique au sein du programme ;
- garantir que des ressources suffisantes sont allouées pour permettre le fonctionnement efficace de ce poste ;
- inclure les mesures prises pour protéger les données des bénéficiaires dans tout suivi et évaluation du programme ;
- établir des mécanismes pour informer les bénéficiaires potentiels des acteurs qui collectent leurs données et de ceux responsables de protéger celles-ci (voir principe 5) ;
- recueillir les données personnelles uniquement par des moyens justes et légaux en faisant appel, si nécessaire, à des conseils juridiques dans le pays concerné afin de savoir si des normes nationales pourraient s'appliquer.

ENCADRE 1 : « DE MANIERE JUSTE ET LEGALE »

Certaines réglementations sur la protection des données ont le pré-requis suivant. Une tierce partie, à savoir le « contrôleur des données », la personne qui collecte les données pour un autre acteur, doit réaliser cela avec le consentement de la personne dont il recueille les informations (le « sujet des données »), mais aussi « de manière juste et légale ». Le test sur cette « manière juste et légale » est souvent réussi lorsque le sujet et le contrôleur des données passent un contrat pour l'approvisionnement en biens ou services requis par le sujet, ou lorsque le traitement des données est nécessaire à la protection des intérêts vitaux du sujet. L'application de ce concept aux programmes d'aide humanitaire n'a pas été mise à l'épreuve. On peut, toutefois, soutenir que l'apport d'une aide est à la fois dans l'intérêt vital du sujet des données et un engagement de la part de l'organisation à fournir un soutien financier au bénéficiaire, même si cela ne prend pas la forme d'un contrat obligatoire. Pourvu que les bénéficiaires soient informés du programme et de l'aide qu'ils peuvent recevoir, et que les mesures définies dans le principe 5 soient respectées, alors, en l'absence de directives formelles de la part des organismes de réglementation, il est probable que lorsque les réglementations imposent de recueillir les données personnelles « de manière juste et légale », cette condition soit remplie.

2 PROTEGER LES DONNEES DE FAÇON ANTICIPEE

Principe : les organisations doivent protéger de façon anticipée les données personnelles qu'elles obtiennent des bénéficiaires, que ce soit pour leur propre utilisation ou celle de tierces parties, pour chaque programme de transfert monétaire ou électronique qu'elles lancent ou mettent en œuvre.

Norme opérationnelle : note interprétative

Les organisations doivent prendre les mesures suivantes.

- S'assurer que les problèmes relatifs à la vie privée et à la protection des données des bénéficiaires sont abordés dès le début dans les programmes de transfert monétaire et électronique, plutôt que d'être « ajoutés » plus tard dans le processus, ceci afin de garantir que l'on peut remédier à tout risque potentiel dans le processus de conception.
- Déterminer, dans la conception du programme, qui est responsable du respect des règles sur la vie privée et la protection des données créées dans le cadre du programme, ainsi que du reporting et de la réaction à toute violation des règles concernées.
- Convenir de l'utilisation des données des bénéficiaires avec les tierces parties avant le début du programme et garantir que des dispositions contractuelles et des contrôles portant sur l'utilisation convenue sont intégrés aux contrats avec ces acteurs.
- Prendre les mesures nécessaires lorsque cela est possible, pour les bénéficiaires qui ne souhaitent pas fournir leurs données personnelles requises pour participer aux programmes de transfert électronique, de façon à ce qu'ils n'en soient pas exclus.
- Garantir que tous les membres du personnel reçoivent une formation sur le traitement des données.
- Entreprendre toutes les actions raisonnables pour valider l'exactitude des informations avec le bénéficiaire, lorsque les données sont reçues depuis des sources autres que les bénéficiaires concernés.
- Interdire aux tierces parties d'utiliser les données personnelles à des fins autres que celles requises pour mettre en œuvre le programme ou que celles auxquelles les bénéficiaires ont préalablement consenti.
- Empêcher la divulgation des données des bénéficiaires au-delà de ce qui est strictement requis par une tierce partie. Par ex., certains systèmes en circuit fermé derrière un compte principal détenu par une ONG peuvent être mis en place à l'aide de sous-comptes anonymes grâce auxquels les prestataires de services n'ont pas besoin de recevoir le nom des utilisateurs de ces sous-comptes (comme pour une carte cadeau).
- Prendre en compte les contextes politiques, juridiques et sociaux dans lesquels le programme est mis en œuvre. Par ex., il faut prêter attention aux réglementations ou pratiques potentiellement existantes concernant la lutte contre le blanchiment d'argent ou le financement du terrorisme, qui peuvent nécessiter la collecte d'informations personnelles supplémentaires. Cela peut être le cas en particulier si les données des bénéficiaires sont susceptibles d'être utilisées afin : de contrôler si ces derniers ne sont pas sur des listes de terroristes ; d'être divulguées aux gouvernements ou à d'autres organisations (telles que des institutions financières) ; ou d'être divulguées aux autorités afin qu'elles vérifient l'identité des bénéficiaires sur certaines listes (voir principe de sécurité 6).

ENCADRE 2 : EVALUATIONS D'IMPACT SUR LA VIE PRIVEE

Les organisations doivent prendre en compte les avantages de la réalisation d'une évaluation d'impact sur la vie privée avant de débuter un programme de transfert monétaire ou électronique. Cela aidera l'organisation à :

- déterminer les risques pour la vie privée des individus ;
- déterminer les responsabilités de l'organisation en matière de respect de la vie privée et de la protection des données ;
- protéger la réputation de l'organisation et instiller une confiance publique envers le programme ;
- s'assurer qu'elle promeut les droits humains dans le cadre de ses activités humanitaires.

L'annexe 1 contient un modèle d'évaluation d'impact sur la vie privée.

3 COMPRENDRE LES FLUX ET LES RISQUES LIES AUX DONNEES

Principe : les organisations doivent analyser, documenter et comprendre le flux de données des bénéficiaires pour chaque programme de transfert monétaire ou électronique qu'elles lancent ou mettent en œuvre en leur sein, ainsi qu'entre elles-mêmes et d'autres organisations. Elles doivent également élaborer des stratégies d'atténuation des risques qui peuvent s'avérer nécessaires pour pallier tout risque créé à partir de ces flux.

Norme opérationnelle : note interprétative

Les organisations doivent prendre les mesures suivantes.

- Analyser les flux de données créés par le programme au sein et entre les organisations, et reconnaître quand ils compromettent la vie privée des bénéficiaires.
- Garantir que les transferts entre organisations sont sécurisés et soumis à un accord écrit ou à un contrat.
- Connaître les besoins en termes d'information que présentent les partenaires ou tierces parties avec lesquels elles collaborent. Par ex., les organisations doivent évaluer chez toute tierce partie engagée dans la mise en œuvre du programme ses besoins en termes d'information ainsi que ses attentes à l'égard de la propriété et de l'utilisation des données pendant et à la fin du programme.
- Comprendre quand elles sont susceptibles de travailler sous contrat pour une tierce partie avec pour objectif de recueillir des données pour cette dernière. Par ex., une organisation peut être amenée à recueillir des données pour un réseau de téléphonie mobile.
- S'assurer que lorsque les organisations opèrent ensemble, dans le cadre d'un consortium, ce dernier a défini (en documentant cette décision) l'organisation responsable de prendre l'initiative en matière de protection des données bénéficiaires. Cette organisation devra, par ailleurs, garantir que des protections adéquates sont intégrées à la conception du programme du consortium, de sorte que chaque organisation opère selon des normes communes pour s'assurer de l'intégrité, de la protection et de l'utilisation des données des bénéficiaires.

ENCADRE 3 : CLAUSES DES MODELES

Tout au long de ce document, nous faisons référence à des accords avec des tierces parties définis par un contrat ou une convention écrite. Dans l'annexe 2, nous avons présenté des modèles de clauses que l'on peut inclure dans des contrats avec des tierces parties. Ils restent uniquement des modèles et peuvent être utilisés de diverses façons : en tant que liste de vérification des éléments qu'un contrat de prestataire de services devrait aborder, en tant que base de négociation avec les prestataires, ou en tant que telles. Il convient de reconnaître que certains prestataires sont susceptibles de ne pas pouvoir satisfaire toutes les conditions des modèles de clauses, étant donné que leurs pratiques et systèmes internes peuvent les empêcher d'accepter tous les aspects des clauses.

Photo: Andy Hall/Oxfam

4 GARANTIR LA QUALITE ET LA PRECISION DES DONNEES

Principe : les organisations doivent garantir la précision des données personnelles qu'elles rassemblent, stockent et utilisent. À cette fin, elles doivent entre autres garder les informations à jour, pertinentes et avec un volume raisonnable par rapport à l'objectif fixé, et ne pas les conserver plus longtemps que nécessaire.

Norme opérationnelle : note interprétative

Les organisations doivent prendre les mesures suivantes.

- Instaurer des processus visant à vérifier l'exactitude de l'ensemble des mécanismes et données, afin de garder les informations à jour, ainsi qu'à supprimer les données qui ne sont plus nécessaires. Par ex. :
  - il convient de mettre en place un processus permettant de s'assurer que les données des bénéficiaires qui ont quitté le programme sont supprimées à la fois par l'organisation et par toute tierce partie qui y avait accès, à moins qu'elle n'ait l'autorisation de les conserver.
- Garantir que les données des bénéficiaires qui ont quitté le programme sont supprimées à la fois par l'organisation et par toute tierce partie qui y avait accès.
- Déterminer quelles informations elles doivent garder (le cas échéant) à la fin d'un programme. Les organisations doivent seulement conserver les données dans un but légitime et dans le format minimal nécessaire. Ainsi les buts légitimes peuvent inclure les programmes potentiels futurs, le suivi et l'évaluation, tandis qu'il peut être pertinent de rendre les données anonymes ou ventilées à des fins de recherche.
- Valider toute série de données existante sur le plan de l'exactitude et des consentements avant de débuter tout programme futur.
- S'assurer que tous les membres du personnel concernés reçoivent une formation sur le traitement des données.
- Valider la précision des données reçues de sources autres que les bénéficiaires eux-mêmes.

Photo: Anna Ridout/ Oxfam

5 OBTENIR LE CONSENTEMENT OU INFORMER LES BENEFICIAIRES DE L'USAGE DE LEURS DONNEES

Principe : au moment de la collecte de données, les bénéficiaires doivent être informés de la nature des informations recueillies, des acteurs avec lesquels elles seront partagées, et du responsable de la sécurité de leur utilisation. Ils doivent avoir la possibilité de remettre en question l'utilisation des données et se retirer du programme s'ils ne souhaitent pas que l'on ait recours à leurs données personnelles pour les fins décrites.

Norme opérationnelle : note interprétative

Les organisations doivent prendre les mesures suivantes.

- Faire preuve de transparence quant à la manière dont elles souhaitent utiliser les données et donner une déclaration de confidentialité aux bénéficiaires au moment de recueillir leurs données personnelles.
- Chercher à obtenir des bénéficiaires leur consentement éclairé au sujet de l'utilisation de leurs données personnelles dans les programmes de transfert monétaire et électronique.
- Seulement recourir à des alternatives au consentement actif éclairé lorsqu'il est impossible d'obtenir ce dernier. Par exemple, les raisons légitimes pour lesquelles on peut se passer du consentement actif éclairé pourraient être les suivantes :
  - des problèmes d'alphabétisation pourraient rendre difficile l'obtention du consentement des individus ;
  - l'urgence, dans la mesure où le calendrier peut empêcher d'obtenir le consentement lors des entretiens individuels ;
  - le contexte de la distribution peut rendre le « consentement actif éclairé »inutile si la vie ou la sécurité des individus ou des familles sont en danger ;
- Garantir que les données sont uniquement utilisées dans le(s) but(s) pour le(s)quel(s) elles ont été recueillies. Si ce(s) but(s) change(nt), il faut de nouveau en informer le bénéficiaire afin d'obtenir son accord.

ENCADRE 4 : CONSENTEMENT ECLAIRE

Comme indiqué dans le principe 1 et expliqué dans l'encadré 1, certaines juridictions exigent que les données personnelles soient traitées de manière « juste et légale ». Le consentement du sujet des données, à savoir, le bénéficiaire, est l'une des formes que prend une collecte des données « juste et légale ». Celle-ci s'applique aussi lorsque l'on a rédigé un contrat ou que le contrôleur des données présente un « intérêt légitime ». On peut uniquement recourir à ce dernier si les intérêts du sujet des données ne sont pas influencés par le traitement de leurs données, d'où des inquiétudes formulées en vertu du principe 6, sur la sécurité des données personnelles.

Les praticiens ont fait part de leurs appréhensions quant à la faisabilité de l'obtention du consentement éclairé des bénéficiaires, dans les programmes de transfert monétaire ou électronique. S'il est impossible d'obtenir cet accord, on considère alors que les bénéficiaires doivent au moins être informés individuellement, collectivement ou des deux façons, au sujet de la nature du programme mis en œuvre, des informations collectées, des acteurs qui le feront et dans quel but. Voici quelques possibilités :

- informer les individus/groupes de bénéficiaires par oral avec la possibilité de poser des questions ;
- en plus d'une introduction de groupe, lire une courte déclaration aux bénéficiaires sur le lieu de l'entretien ou de la collecte de données ;
- fournir des brochures ou d'autres documents de communication qui apportent aux bénéficiaires des informations sur le programme et sur leurs droits ;
- informer les bénéficiaires sur les tierces parties qui pourraient accéder à leurs données et sur la manière dont ils peuvent empêcher toute communication future non voulue avec ces tierces parties.

Gardez toujours à l'esprit la capacité des bénéficiaires à comprendre et à donner leur consentement ; dans le cas d'enfants, ou d'individus ou communautés vulnérables, adaptez vos méthodologies comme il se doit.

L'annexe 2 propose un modèle basique de formulaire de consentement.

6 GARANTIR LA SECURITE DES DONNEES

Principe : les organisations doivent instaurer des normes de sécurité techniques et opérationnelles adaptées pour chaque étape de la collecte, de l'utilisation et du transfert des données des bénéficiaires. Le but est d'empêcher l'accès non autorisé, la divulgation ou perte des informations. Il convient notamment d'identifier toute menace extérieure et de prendre des mesures pour atténuer tout risque qui viendrait à apparaître.

Norme opérationnelle : note interprétative

Les organisations doivent prendre les mesures suivantes.

- S'assurer que des systèmes organisationnels et de programme sont en place afin de garantir le stockage sécurisé des données des bénéficiaires. Ainsi, par ex., le personnel de programme doit se mettre en relation avec le personnel informatique interne pour les questions d'information sur la sécurité.
- Établir clairement qui, dans leur équipe de gestion de programme, est responsable de la sécurité des données et de la mise en place de processus de protection des données personnelles des bénéficiaires. Ces processus doivent protéger de la perte, du vol, des dommages et de la destruction et ils comprennent les systèmes de sauvegarde ainsi que des moyens efficaces de lutter contre les violations de la sécurité.
- Instaurer des processus visant à contrôler les personnes qui ont accès aux données personnelles des bénéficiaires et garantir que seuls les utilisateurs autorisés peuvent accéder aux données.
- S'assurer que les systèmes de stockage numériques sont cryptés et protégés par un mot de passe. Garantir que si des copies physiques des archives contenant des données des bénéficiaires sont conservées, elles sont gardées en un lieu sécurisé.
- S'assurer que les transferts de données personnelles au sein des organisations et entre elles sont uniquement entrepris lorsqu'imposés par un programme ; qu'ils sont réalisés par des moyens sécurisés ; et que les destinataires des données reconnaîtront à leur tour la nature confidentielle de celles-ci. Par ex.,
  - les destinataires doivent vérifier les antécédents des partenaires du secteur privé afin de protéger le caractère privé des données.
- Évaluer les risques associés à la nature et au type de données recueillies, par ex., lors de la collecte de données parmi des groupes ou communautés vulnérables.
- Avoir conscience des facteurs locaux qui pourraient accroître les risques de sécurité relatifs aux transferts électroniques. Ces facteurs peuvent comprendre :
  - un contrôle gouvernemental étendu des communications mobiles, ainsi qu'une surveillance répandue des échanges téléphoniques et web ;
  - les faiblesses en termes de sécurité, au niveau des technologies mobiles utilisées pour recueillir, stocker ou transférer des données ;
  - les contextes politiques, religieux, techniques ou sociaux du pays, qui peuvent créer des risques particuliers au moment de la collecte et de l'utilisation de données personnelles.

7 PREVOIR LA SUPPRESSION DES DONNEES

Principe : les organisations ne doivent pas conserver les données des bénéficiaires plus longtemps que nécessaire, à moins qu'elles ne présentent des raisons claires, justifiables et documentées. Autrement, les données détenues par les organisations et les tierces parties concernées doivent être détruites.

Norme opérationnelle : note interprétative

Les organisations doivent prendre les mesures suivantes.

- Indiquer dans la stratégie de sortie de leur programme les données personnelles qu'elles souhaitent conserver et la raison.
- Définir toute raison juridique ou contractuelle pour laquelle elles doivent ou non conserver des données des bénéficiaires.
- Lorsque les données ne sont pas requises, garantir que la suppression ou destruction et/ou l'archivage sécurisés des données personnelles par toutes les parties qui y ont accédé. À cette fin, les organisations doivent par ex. :
  - chercher conseil auprès du personnel informatique interne quant à la manière de détruire des données en toute sécurité ;
  - intégrer aux systèmes de traitement des données la capacité à détruire des données en toute sécurité ;
  - intégrer des procédures particulières de suppression de données dans les contrats de services passés avec les parties avec lesquelles ils ont l'intention de partager les données des bénéficiaires ;
  - au moment de fournir du matériel informatique de programme tel que des cartes SIM, intégrer des clauses dérogatoires automatiques dans le contrat, au cas où les bénéficiaires ne souhaiteraient pas maintenir de relation commerciale avec le prestataire de services à la fin du programme humanitaire.
- Lorsque les données doivent être conservées au-delà du délai préalablement communiqué au bénéficiaire, ou lorsqu'elles sont conservées dans un but différent de celui communiqué à l'origine au bénéficiaire, garantir alors que le bénéficiaire en est informé. En outre, si nécessaire, il convient d'obtenir le consentement des bénéficiaires ; ainsi, si le but a changé de manière significative, il faut obtenir le consentement à l'utilisation future des données.

Photo: Simon Rawles

8 GARANTIR LA REDEVABILITE

Principe : les organisations doivent établir un mécanisme par lequel un bénéficiaire peut demander des informations concernant les données personnelles que détient une organisation à son sujet, de même que des mécanismes pour recevoir et répondre à toute plainte ou inquiétude que les bénéficiaires pourraient formuler à l'égard de l'utilisation de leurs données personnelles.

Norme opérationnelle : note interprétative

Les organisations doivent les mesures suivantes.

- Être au courant de toute obligation qui s'applique dans le pays hôte quant à la redevabilité envers les bénéficiaires et leurs droits en matière d'accès à leurs données personnelles.
- Instaurer un mécanisme par lequel un bénéficiaire peut demander des informations au sujet des données que détient une organisation à son sujet, des tierces parties avec lesquelles les informations ont été partagées et du but dans le quel elles sont utilisées.
- Reconnaître que de tels systèmes peuvent entraîner un certain coût et prévoir ces systèmes dans les budgets des programmes.
- En accord avec le principe 2, déterminer qui est responsable de la gestion de toute violation rapportée, de la lutte contre celle-ci, ainsi que du signalement de ces violations à leur siège et, si besoin, à des organismes de réglementation externes.
- Informer le personnel et les partenaires au sujet de l'exigence consistant à signaler les violations et toute perte de données dont l'organisation est responsable.
- Permettre aux bénéficiaires d'accéder à leurs données et de les modifier, pourvu que la demande soit légitime et faite soit directement par la personne concernée ou avec son autorisation expresse. Par ex., les données personnelles ne doivent pas être divulguées à une personne non autorisée qui prétend représenter l'individu, notamment en cas de données particulièrement sensibles.
- Établir une politique générale et une procédure en matière de plaintes, et réagir promptement à toute plainte ou inquiétude émanant des bénéficiaires quant à l'utilisation de leurs données personnelles.

Photo: Simon Rawles

[4] http://www.piafproject.eu/ref/A_step-by-step_guide_to_privacy_impact_assessment-19Apr2012.pdf
Pour de plus amples informations, veuillez vous référer au document : http://piafproject.eu/ref/PIAF_D3_final.pdf

ANNEXES : RESUME

ANNEXE 1 : MODELE D'EVALUATION D'IMPACT SUR LA VIE PRIVEE

Le document ci-dessous apporte les précisions suivantes. « L'objectif d'une évaluation d'impact sur la vie privée est de prouver que les responsables de programmes et les propriétaires de systèmes ont sciemment intégré des protections de la vie privée tout au long du cycle de vie du développement d'un système ou d'un programme. Cela implique de s'assurer que des protections de la vie privée sont intégrées au système depuis le début du développement et non pas après coup, lorsqu'elles peuvent s'avérer plus onéreuses ou qu'elles peuvent affecter la viabilité du projet. »

Il existe d'autres approches à l'égard de la définition, gestion et documentation des risques pour la vie privée. L'une d'entre elles est le « Privacy Impact Assessment Framework » (PIAF). Le PIAF est un projet co-financé par la Commission européenne. Il vise à encourager l'Union européenne et ses États-membres à adopter une politique progressive d'évaluation d'impact sur la vie privée en tant que moyen de satisfaire les besoins et remédier aux problèmes liés à la vie privée et au traitement des données personnelles.

Le PIAF apporte : « *…un processus qui se concentre sur la définition des impacts sur la vie privée de tout nouveau projet, technologie, service ou programme et, en consultation avec les parties prenantes, sur la prise de mesures dans le but d'éviter tout risque ou de l'atténuer. Le processus doit commencer lorsqu'un projet en est aux premiers stades de planification, lorsqu'il y a encore une possibilité d'influencer la structure ou l'issue du programme. Ce processus doit se prolonger tout au long de la vie du projet. De nouveaux risques peuvent émerger à mesure que le projet progresse et il faut les évaluer dès qu'ils deviennent apparents.* »

Wright, D. et Wadhwa, K. A step by step guide to privacy impact assessment. 2012[4.]

ANNEXE 2 : MODELE DE CLAUSES POUR LES CONTRATS AVEC DES TIERCES PARTIES

A : INFORMATION ET CONSENTEMENT DES BÉNÉFICIAIRES (MODÈLE EN LANGAGE SIMPLE)

B : ORGANISATION HUMANITAIRE ET PRESTATAIRE DE SERVICES DE TRANSFERT ÉLECTRONIQUE

Veuillez noter que les clauses représentent une norme recommandée mais qu'elles devront être modifiées par l'organisation concernée, dans plusieurs buts : (i) pour les concilier aux variations terminologiques et aux conventions de dénomination présentes dans les lois de protection des données applicables aux pays concernés ; (ii) pour adopter des normes supérieures de protection des données ; ou (iii) pour les concilier aux particularités de l'accord entre l'organisation concernée (le contrôleur des données) et le responsable du traitement des données.

Le CaLP s'efforce ici de proposer au praticien un point de départ dans l'élaboration des clauses qui sont en phase avec les principes et normes opérationnelles définis dans ce document.

Des clauses supplémentaires seront publiées sur le site web du CaLP : www.cashlearning.org.

ANNEXE 1 : MODELE D'EVALUATION D'IMPACT SUR LA VIE PRIVEE

À propos de ce modèle d'évaluation d'impact sur la vie privée

Une évaluation d'impact sur la vie privée examine les procédures et technologies d'une organisation en vue d'analyser la façon dont les informations personnelles sont recueillies, utilisées, diffusées et conservées. Cette évaluation est conçue pour garantir qu'une organisation intègre les problématiques liées à la vie privée dans l'élaboration, la conception et l'application d'une technologie ou ligne directrice.

Il existe plusieurs méthodologies et approches pour l'évaluation d'impact sur la vie privée. Ce modèle d'évaluation a été adapté de celle mise au point par le département de la Sécurité intérieure des États-Unis (DHS). Pendant de nombreuses années, le DHS a mené des évaluations d'impact sur la vie privée pour toutes les nouvelles règles et technologies. En effet, ce processus est considéré comme étant nécessaire par nature pour tous les programmes du gouvernement fédéral des États-Unis depuis 2002, comme l'exige la loi « E-Government Act » de la même année. Selon le DHS,

« Le but d'une évaluation d'impact sur la vie privée est de prouver que les responsables de programme et les propriétaires de systèmes ont sciemment intégré des mesures de protection de la vie privée tout au long du cycle de vie du développement d'un système ou d'un programme. Cela implique de s'assurer que des mesures de protection de la vie privée sont intégrées au système depuis le début du développement et non pas après coup, lorsqu'elles peuvent s'avérer plus onéreuses ou qu'elles peuvent affecter la viabilité du projet. »

Plutôt que d'être simplement une évaluation et un rapport qui établissent si une organisation a adhéré aux principes définis, l'évaluation d'impact sur la vie privée fait elle-même partie d'un processus qui permet aux organisations de prendre en considération les conséquences des nouvelles technologies, techniques et lignes directrices, de manière à ce que l'on puisse prévoir les risques, déterminer les problèmes potentiels et lancer le processus de négociation des solutions avant qu'ils ne deviennent trop complexes.

En conséquence, l'évaluation d'impact sur la vie privée vise en premier lieu à déterminer les risques liés aux systèmes, puis à étudier des stratégies d'atténuation des risques, que l'on peut alors intégrer aux processus d'élaboration des technologies et lignes directrices en question. À l'aide d'une méthodologie qui comprend une interaction avec les parties prenantes, une évaluation d'impact sur la vie privée devient en elle-même une méthode pour : anticiper les risques et y remédier ; pour communiquer les problèmes aux parties prenantes et dans l'ensemble de l'organisation ; et pour renforcer la confiance. C'est pourquoi le département de la Sécurité intérieure américain voit l'évaluation d'impact sur la vie privée comme « un document vivant que l'on doit mettre à jour régulièrement à mesure que le programme et le système sont modifiés et mis à jour, et non pas uniquement lorsque ces derniers sont mis en pratique ».

Quand réaliser une évaluation d'impact sur la vie privée

Le DHS suggère un processus d'examen de la vie privée suivant des seuils dont l'objectif est de déterminer à quel moment il faut mener une évaluation d'impact sur la vie privée. Avant cette évaluation, il faudra déterminer si le programme implique la collecte, la création ou la conservation d'informations personnelles et de quelle manière. Dans le cadre de ce modèle d'évaluation, on suppose que l'ensemble des programmes du secteur humanitaire impliquent, d'une manière ou d'une autre, le traitement d'informations personnelles et qu'a priori, il y a donc un besoin pour ce type d'évaluation.

MODELE D'EVALUATION D'IMPACT SUR LA VIE PRIVEE POUR LES ACTEURS HUMANITAIRES

1 Informations

Quelles informations sont recueillies, utilisées, diffusées ou conservées dans le système ?

Quelles sont les sources d'information ?

Pourquoi les informations sont-elles recueillies, utilisées, diffusées ou conservées ?

Comment les informations sont-elles recueillies ?

Comment vérifiera-t-on l'exactitude des informations ?

Quelles autorités juridiques, conventions et/ou accords ont défini la collecte des informations ?

Analyse de l'impact sur la vie privée : en tenant compte de la quantité et du type de données recueillies, débattez des risques pour la vie privée qui ont été déterminés et de la manière dont ils ont été atténués.

2 Utilisations

Décrivez toutes les utilisations des informations.

À quels types d'instruments a-t-on recours afin d'analyser les données et quel type de données peut-on produire ?

Si le système utilise des données commerciales ou publiquement disponibles, expliquez en la raison et la manière dont elles sont utilisées.

Analyse de l'impact sur la vie privée : décrivez tout type de contrôle qui peut être en place en vue d'assurer que les informations sont traitées dans le respect des utilisations décrites ci-dessus.

3 Conservation

Combien de temps les informations sont-elles conservées ?

La période de conservation a-t-elle été approuvée ?

Analyse de l'impact sur la vie privée : débattez des risques associés à la durée de conservation des données et de la manière dont ces risques ont été atténués.

4 Partage et divulgation internes

Avec quelle(s) organisation(s) interne(s) les informations sont-elles partagées ? Quelles informations sont partagées et dans quel but ?

Comment les informations sont-elles transmises ou divulguées ?

Analyse de l'impact sur la vie privée : en tenant compte du degré de partage d'informations en interne, débattez des risques pour la vie privée associés au partage, ainsi que de la manière dont ils ont été atténués.

5 Partage et divulgation externes

Avec quelle(s) organisation(s) externe(s) les informations sont-elles partagées ? Quelles informations sont partagées et dans quel but ?

Le partage des données nominatives en dehors de l'organisation est-il compatible avec la collecte effectuée à l'origine ?

Si oui, le processus est-il couvert par un principe directeur adéquat et par une notification ?

Comment les informations sont-elles partagées en dehors de l'organisation et quelles mesures de sécurité protègent leur transmission ?

Analyse de l'impact sur la vie privée : en tenant compte du partage externe, expliquez les risques pour la vie privée qui ont été déterminés et décrivez comment ils ont été atténués.

6 Notification

L'individu a-t-il été informé avant la collecte d'information ?

Les individus ont-ils la possibilité et/ou le droit de refuser de fournir des informations ?

Les individus ont-ils le droit de consentir à des utilisations particulières des informations ? Si oui, comment un individu peut-il exercer ce droit ?

Analyse de l'impact sur la vie privée : décrivez comment les individus sont informés et comment les risques associés aux individus qui ne sont pas au courant de la collecte d'informations sont atténués.

7 Accès, réparation et correction

Quelles sont les procédures qui permettent aux individus d'accéder à leurs propres informations ?

Quelles sont les procédures permettant de corriger les informations inexactes ou erronées ?

Comment les individus sont-ils informés des procédures de correction de leurs informations ?

Si aucune réparation n'est effectuée, quelles solutions alternatives sont disponibles pour l'individu concerné ?

Analyse de l'impact sur la vie privée : débattez des risques pour la vie privée associés aux possibilités de réparation disponible pour les individus, ainsi que de la manière dont ces risques sont atténués.

8 Accès technique et sécurité

Quelles sont les procédures en place pour déterminer quels utilisateurs peuvent accéder au système ? Sont-elles documentées ?

Quels sous-traitants de l'organisation ont accès au système ?

Quelle formation en matière de vie privée est dispensée aux utilisateurs, que ce soit de manière générale ou spécifiquement vis-à-vis du programme ou système ?

Quelles mesures d'audit et quelles protections techniques sont instaurées en vue d'empêcher une mauvaise utilisation des données ?

Analyse de l'impact sur la vie privée : en tenant compte de la sensibilité et de la portée des informations recueillies, ainsi que de tout partage d'information réalisé sur le système, quels risques pour la vie privée ont été identifiés et comment les contrôles de sécurité les atténuent-ils ?

9 Technologies

À quel type de projet le programme ou système correspond-il ?

À quel stade du développement le système en est-il et quel cycle de vie pour le développement de projets a été utilisé ?

Le projet a-t-il recours à des technologies qui peuvent soulever des inquiétudes liées à la vie privée ? Si oui, débattez de sa mise en œuvre.

ANNEXE 2 : MODELE DE CLAUSES POUR LES CONTRATS AVEC DES TIERCES PARTIES

A : INFORMATION DU BÉNÉFICIAIRE ET CONSENTEMENT (MODÈLE EN LANGAGE SIMPLE)

Accord sur les données personnelles

Numéro de dossier/d'identité	
Nom du bénéficiaire	
Date	
Lieu	

Manière dont le formulaire sera expliqué

Nom de la personne qui explique le formulaire	
Rôle de la personne qui explique le formulaire *(ex. chargé de dossier/bénévole)*	
L'explication de la personne qui remplit le formulaire sera en *(langue de la personne qui remplit le formulaire)*	
et elle sera traduite en *(langue dans laquelle l'explication sera fournie au bénéficiaire)*	

Les personnes suivantes contribueront à l'explication

1. Traduction par un interprète de formation ou
2. traduction informelle par

(Inscrire le nom de l'interprète et sa relation vis-à-vis du bénéficiaire : sœur, prêtre, etc.)

3. Aide d'une personne de confiance

(Inscrire le nom de l'interprète et sa relation vis-à-vis du bénéficiaire : sœur, prêtre, etc.)

Si vous souhaitez intégrer le [insérer le nom du programme], nous devons vous poser quelques questions. Nous utilisons ce que vous dites à propos de vous-même dans le but de gérer la modalité selon laquelle vous recevrez [insérer l'avantage conféré par le programme ou le paiement d'argent]. Il existe des règles qui contrôlent ce que nous pouvons faire avec les informations que vous nous fournissez. Les informations que vous nous fournissez sont appelées données personnelles. Voici les règles.

1. Nous pouvons seulement utiliser vos données personnelles pour réaliser des actions auxquelles vous consentirez aujourd'hui. Nous souhaitons utiliser vos données afin de mettre en œuvre [insérer le nom du programme]. Nous utilisons vos données personnelles pour :
   - vous fournir [nom de l'avantage conféré par le programme ou du paiement d'argent] ;
   - empêcher le vol de l'argent ;
   - apprendre comment mieux mettre en œuvre [insérer le nom du programme] ;
   - [optionnel : inclure d'autres avantages conférés par (insérer le nom de l'organisation)].

Nous pouvons uniquement conserver vos données personnelles aussi longtemps que nous en aurons besoin pour effectuer ces actions. Si nous souhaitons entreprendre d'autres actions avec vos données personnelles, nous devons vous contacter à nouveau.

2. Les données personnelles que nous vous demandons de nous communiquer aujourd'hui sont [insérer les catégories de données, comme par ex. le nom, le numéro de téléphone portable ; les données elles-mêmes peuvent être enregistrées sur un formulaire séparé mais il doit être rempli seulement après l'obtention de ce consentement].

3. Nous partageons vos données personnelles avec d'autres de sorte que vous puissiez recevoir [nom de l'avantage conféré par le programme ou le paiement d'argent]. Nous les partagerons avec [insérer le nom du prestataire, tel qu'une banque ou un réseau mobile] ou bien [insérer les coordonnées des prestataires] afin de vous fournir [nom de l'avantage conféré par le programme ou du paiement d'argent]. Lorsque nous partageons vos données personnelles avec ces acteurs, ils doivent eux aussi respecter ces règles. Ils n'ont pas le droit d'utiliser vos données personnelles pour vous vendre quoi que ce soit mais seulement pour vous fournir [nom de l'avantage conféré par le programme ou du paiement d'argent]. Vous pouvez toujours nous demander avec qui nous avons partagé vos informations.
4. Nous faisons de notre mieux pour veiller sur vos données personnelles afin que personne d'autre ne puisse les utiliser, à part ceux avec qui nous les partageons. Toutes les personnes qui obtiennent vos données personnelles doivent s'efforcer de veiller sur celles-ci le mieux possible.
5. Il y a un risque qu'une personne non autorisée obtienne vos données depuis notre organisation en agissant malhonnêtement. Il peut exister un risque important qu'un organisme gouvernemental ou autre obtienne les données, avec des effets négatifs allant au-delà de la violation du caractère privé des données à l'égard du bénéficiaire. Si tel est le cas, alors la personne qui remplit le formulaire doit expliquer ce risque à ce moment de l'entretien. Il est recommandé de ne pas inscrire la nature du risque afin de faciliter le paiement. En effet, cela pourrait entraîner des représailles contre l'organisation qui recueille les données.
6. Nous pourrions avoir l'obligation de remettre vos données personnelles à un gouvernement selon certaines lois.
7. Si vous pensez que nous ou quelqu'un avec qui nous avons partagé vos données personnelles a tort, vous pouvez nous demander d'y remédier.
8. Si certaines de vos données personnelles changent, vous pouvez nous demander de faire les modifications qui en découlent au niveau des informations dont nous disposons.
9. Si vous pensez que nous ou quelqu'un avec qui nous avons partagé vos données personnelles a enfreint les règles, vous pouvez déposer une plainte auprès de nous. [Insérer les coordonnées de la personne responsable du respect du code de conduite au sein du pays]

Accord d'enregistrement

Maintenant que vous connaissez les règles au sujet de ce que nous faisons de vos données personnelles, acceptez-vous de nous les communiquer ?

Oui ☐ Non ☐

Si oui, indiquez le mode de consentement du bénéficiaire.

1. En signant un exemplaire de ce formulaire.

Signature _____

2. Making a thumbprint or fingerprint on a copy of this form.

Empreinte digitale : ☐

3. En inscrivant un signe à côté de son nom. Nom et signe : _____

4. Autre manière (notez-la) : _____

Si la réponse est non, expliquez au bénéficiaire qu'il existe un autre moyen d'obtenir l'avantage concerné et décrivez-le ; s'il n'y a pas d'autre moyen, expliquez cela.

B : ORGANISATION HUMANITAIRE ET PRESTATAIRE DE SERVICES DE TRANSFERT ÉLECTRONIQUE

Présentation générale :

Les clauses modèles prévoient ce qui suit :

- l'organisation humanitaire (l'organisation) est le « contrôleur des données », à savoir l'émetteur de la demande de traitement des données ;
- le prestataire de services de transfert électronique est le « responsable du traitement des données » ;
- le bénéficiaire du transfert électronique qui divulgue ses données personnelles à l'organisation est le « sujet des données » ;
- le responsable du traitement des données peut seulement traiter les données aux fins définies dans le contrat (qui doivent être expresses) et dans le respect des instructions du contrôleur des données ;
- le responsable du traitement des données ne doit pas divulguer les données à une quelconque tierce partie ni les faire sous-traiter par une quelconque tierce partie sans le consentement du contrôleur des données. De plus, le responsable doit disposer de normes internes de sécurité adéquates liées aux données afin d'empêcher l'accès non autorisé aux données ainsi que leur traitement ou leur divulgation non autorisés.
- accord sur ce qu'il advient des données à la fin du contrat ;
- limites en termes d'utilisation des données par le responsable du traitement à des fins de marketing, de profilage et d'autres utilisations commerciales qui ne sont pas en accord avec le traitement autorisé par l'organisation ;
- limites en termes de contact avec les sujets des données (bénéficiaires), c'est-à-dire que tout contact avec les bénéficiaires se fera par le biais de l'organisation à moins qu'il n'en soit convenu autrement entre l'organisation et la tierce partie ;
    - le responsable du traitement des données s'assurera que son personnel et ses sous-traitants, qui agissent sous son contrôle direct ou indirect dans le cadre de sa prestation des services à l'égard de l'organisation, acceptent par contrat de :
    - respecter les obligations de non-divulgation en vue de garantir la confidentialité des données ;
    - respecter les politiques générales applicables au responsable du traitement des données, telles qu'une politique sur la vie privée ou une politique de sécurité, visant à préserver les fonctions du responsable du traitement et protéger ainsi les données ;
    - respecter les obligations de conservation de la qualité (dont l'exactitude) des données traitées par le personnel concerné et les sous-traitants.

Les clauses représentent une norme minimale mais elles peuvent être modifiées par l'organisation concernée pour : (i) les concilier aux variations terminologiques et les conventions de dénomination, présentes dans les lois de protection des données applicables aux pays concernés ; (ii) adopter des normes supérieures de protection des données ; ou (iii) les concilier aux particularités de l'accord entre l'organisation concernée (le contrôleur des données) et le responsable du traitement des données.

Il est important de prendre en note que, dans plusieurs pays, les lois sur la protection des données prévalent sur les exigences définies dans le présent document *Principes et normes opérationnelles pour une utilisation sécurisée des données personnelles dans les programmes de transfert monétaire et électronique*. Selon ces lois, même si un responsable du traitement des données cause une perte ou une divulgation non autorisée des données personnelles, l'organisation, c'est à dire le contrôleur des données, sera tenu responsable de cette violation. Le contrôleur des données peut donc être tenu responsable du point de vue civil ou pénal pour les violations de la protection des données occasionnées par le responsable du traitement. L'organisation détient, toutefois, un intérêt dans l'adoption de mesures supplémentaires en complément de l'accord passé. Cela permet de garantir le respect de cet accord par le responsable du traitement des données, sur le plan technologique et organisationnel. Les mesures peuvent comporter, par exemple, l'audit du respect de l'accord par le responsable du traitement ou un rapport périodique par ce dernier sur la question du respect de la vie privée, ainsi que des principes directeurs et procédures de sécurité mis en œuvre par le responsable du traitement.

MODELES DE CLAUSES

Les modèles de clauses ci-dessous ont été ébauchés afin de constituer un accord distinct. Ils **nécessiteront d'être négociés et relus**. On peut néanmoins inclure les clauses dans les accords-cadres et accords principaux qui déterminent d'autres aspects de la relation entre l'organisation et l'affilié ou le prestataire de services.

ACCORD ENTRE :

1 [Nom de l'organisation], dont le bureau est enregistré à […] (le « contrôleur des données ») ; et

2 [Nom de l'affilié/prestataire], dont le bureau est enregistré à […] (le « responsable du traitement des données »).

BUT DE CET ACCORD

A Dans le but de faciliter les transferts monétaires électroniques depuis le contrôleur des données vers les bénéficiaire des transferts, ce contrôleur recueille et traite les données personnelles de ces bénéficiaires.

B Le contrôleur des données a engagé le responsable du traitement des données afin de rendre les services qui comprennent le traitement des données des bénéficiaires de la part du contrôleur.

C Le contrôleur des données est soumis aux lois, réglementations et codes de conduite, principes et normes opérationnelles qui instaurent des obligations à son égard. Cela l'engage à respecter la vie privée et à protéger les données personnelles des bénéficiaires dans le traitement de ce type de données, que ce soit fait de manière indépendante ou par le biais des responsables du traitement des données nommés.

D En conséquence, cet accord relève de la protection des données personnelles accédées ou autrement reçues, et traitées par le responsable du traitement des données pour le contrôleur des données, dans le cadre de la prestation des services.

L'ACCORD PORTE SUR LES POINTS SUIVANTS

1 DÉFINITIONS ET INTERPRÉTATION

1.1 Dans cet accord, les termes suivants sont utilisés.

Le contrôleur des données désigne la personne, au sein de l'organisation, qui détermine les objectifs et les conditions du traitement actuel ou futur des données personnelles.

Le responsable du traitement des données désigne l'affilié ou prestataire de services ; personne qui réalise le traitement des données personnelles pour le contrôleur des données, au cours de la prestation des services.

Le sujet des données désigne les bénéficiaires de transferts monétaires électroniques mis en œuvre par l'organisation et les personnes auxquelles se rapportent les données.

Les données personnelles désignent toute information personnelle, dont les informations nominatives telles que le nom, le numéro de carte d'identité ou de passeport, le numéro de téléphone portable, l'adresse e-mail, les modalités des transactions monétaires. Ces données peuvent être de toute nature ou de tout format. Elles sont fournies au responsable du traitement des données par le contrôleur des données et le premier y accède avec l'autorisation du contrôleur ou les reçoit pour le compte du contrôleur. Elles incluent les informations de transaction ou d'autres informations associées au sujet des données, générées par le responsable du traitement lors de la prestation des services pour le contrôleur.

Le traitement comprend, vis-à-vis des données personnelles, l'obtention, l'enregistrement ou la détention de ces données. Il peut aussi s'agir de toute activité ou série d'activités portant sur ces données, y compris : l'organisation ; l'adaptation ou l'altération ; la divulgation par transmission, par dissémination ou par un autre moyen ; l'alignement ; l'association ; le blocage ; l'effacement ou la destruction.

Le calendrier désigne les emplois du temps annexés à l'accord et qui en font partie.

Les services désignent les activités particulières pour lesquelles le contrôleur des données a engagé le responsable du traitement des données comme indiqué dans le calendrier A [ou la clause (...) de l'accord-cadre/accord principal].

2 TRAITEMENT DES DONNÉES

2.1 Le responsable du traitement des données accepte de prendre en charge les données personnelles auxquelles s'applique cet accord, et il consent en particulier aux conditions ci-dessous.

a. Traiter les données personnelles en observant les conditions générales définies dans cet accord. Lorsque les normes imposées par la législation sur la protection des données qui régit ce traitement prévalent sur celles décrites dans cet accord, alors le responsable du traitement des données doit se conformer à cette législation.

b. Traiter les données personnelles en respectant strictement les objectifs correspondant aux services, de la manière précisée ponctuellement par le contrôleur des données, sans poursuivre un autre but ni recourir à une autre manière, excepté lorsque le contrôleur en donne expressément l'autorisation au préalable.

c. Appliquer des mesures techniques et organisationnelles adéquates pour protéger les données personnelles d'un traitement non autorisé ou illégal, et d'une perte, d'une destruction ou d'un dommage accidentels, eu égard à l'état du développement technologique et au coût de mise en œuvre de telles mesures. Celles-ci assureront un niveau de sécurité adapté, d'une part, au préjudice qui pourrait résulter d'un traitement non autorisé ou illégal, et d'une perte, d'une destruction ou d'un dommage accidentels, et d'autre part, à la nature des données personnelles à protéger.

d. Considérer les données personnelles comme des informations confidentielles. Ne pas les divulguer aux personnes autres que les employés, agents ou sous-traitants vis-à-vis desquels la divulgation est requise pour la prestation des services et sujette à [...] ci-dessous, exception faite des cas où l'exige toute loi ou réglementation qui affecte le responsable du traitement des données.

e. Mettre en œuvre des mesures techniques et organisationnelles qui préservent la confidentialité, le caractère privé, l'intégrité, la disponibilité, l'exactitude et la sécurité des données personnelles. Cela implique d'instaurer des principes directeurs organisationnels qui sont destinés aux employés, agents et sous-traitants, et qui visent à se conformer aux fonctions du responsable du traitement des données, ceci afin de protéger les données personnelles dans le respect de cet accord.

f. Établir des processus de sauvegarde comme convenu entre le contrôleur des données et le responsable de leur traitement. L'objectif est d'assurer la disponibilité des données personnelles à tout instant et de garantir que le contrôleur aura accès à ces sauvegardes des données personnelles, dans la limite des besoins raisonnables exprimés par le contrôleur.

g. Garantir que toute divulgation à un employé, agent ou sous-traitant est soumise à une obligation légale de se conformer aux devoirs du responsable du traitement des données dans le cadre de cet accord. Cela inclut le respect des mesures techniques et organisationnelles concernées en matière de confidentialité, de caractère privé, d'intégrité, de disponibilité, d'exactitude et de sécurité des données personnelles. Afin d'éviter toute incertitude, nul accord passé avec un employé, agent ou sous-traitant ne supprimera l'obligation de respecter le présent accord dans son intégralité, qui incombe au responsable du traitement des données. Celui-ci restera entièrement garant du respect de cet accord dans son intégralité.

h. Respecter toute demande du contrôleur des données concernant l'amendement, le transfert ou la suppression des données personnelles. Fournir une copie de toutes ou partie des données personnelles détenues dans un format ou média spécifié par le contrôleur dans un délai raisonnable, comme convenu entre les parties [il est à la discrétion de l'organisation d'insérer dans ce paragraphe les périodes de temps concernées].

i. Si le responsable du traitement des données reçoit quelque avis, plainte ou communication que ce soit, liés directement ou indirectement au traitement des données personnelles ou au respect de l'une ou l'autre partie à la loi applicable, alors le responsable du traitement doit immédiatement en informer le contrôleur des données. Il doit aussi entièrement coopérer avec ce dernier et l'aider au sujet de tout avis, plainte ou communication.

j. Informer promptement le contrôleur si des données personnelles sont perdues, détruites, endommagées, corrompues ou inutilisables. Restaurer ces données à ses frais à la demande du contrôleur.

k. Dans le cas où les sujets des données exerceraient tout droit sur leurs données personnelles, en informer le contrôleur des données aussi tôt que possible.

l. Aider le contrôleur des données pour toute demande d'information de la part des sujets des données, qui pourrait provenir de tout sujet des données relatif à toute donnée personnelle.

m. Ne pas utiliser les données personnelles des sujets des données dans le but de contacter ces sujets, de communiquer ou interagir avec eux de quelque autre manière. Cela implique de ne pas transmettre quelque communication marketing ou commerciale que ce soit aux sujets des données, excepté avec le consentement écrit du contrôleur des données ou pour respecter l'ordonnance d'un tribunal. Afin d'éviter toute incertitude, le responsable du traitement des données n'a pas l'interdiction de contacter le sujet des données, de communiquer ou interagir avec lui dans la mesure où cela n'implique pas le traitement des données personnelles, et où ce responsable garantit que la promotion ou prestation de services n'est aucunement associée au contrôleur des données ou aux services de ce dernier.

n. Informer le contrôleur des données du ou des pays dans lesquels les données personnelles seront traitées, lorsque ce ou ces pays ne sont pas ceux où est enregistré le bureau du responsable du traitement des données.

o. Ne pas traiter ou transférer les données personnelles en-dehors du pays de son bureau enregistré, excepté avec le consentement écrit préalable du contrôleur des données à la suite d'une demande par écrit émise par le responsable du traitement envers le contrôleur.

p. Permettre et faire en sorte que les infrastructures, procédures et documents liés au traitement des données soient soumis à un examen approfondi par le contrôleur des données ou ses représentants mandatés, sur demande, dans le but de réaliser un audit ou de confirmer le respect des termes de cet accord.

q. Conseiller le contrôleur des données au sujet de tout changement significatif au niveau du risque de traitement non autorisé ou illégal, ou bien de la perte, destruction ou endommagement des données personnelles et

r. en faire le rapport [dans le respect des délais raisonnables convenus] au contrôleur des données, au sujet des mesures prises en tant que responsable du traitement en vue d'assurer le respect de la clause 3.1 de cet accord.

3 GARANTIES

3.1 Le responsable du traitement des données garantit que :

a. il traitera les données personnelles dans le respect des lois, décrets, réglementations, ordres, normes et autres instruments similaires qui lui sont applicables, et dans le respect des conditions générales de cet accord ;

b. dans le but de se conformer aux droits patrimoniaux et/ou d'autres droits de propriété, dont la propriété intellectuelle, du contrôleur des données vis-à-vis des données personnelles, il ne copiera, ne conservera ni ne traitera celles-ci de quelque manière que ce soit pendant la durée de cet accord ni après expiration ou résiliation de cet accord, excepté si la loi ou cet accord l'exigent.

4 EXONÉRATION

4.1 Le responsable du traitement des données accepte d'exonérer et de continuer d'exonérer le contrôleur des données de tout coût, réclamation, dommage ou dépense entraînés par le contrôleur ou pour lesquels le contrôleur peut devenir responsable en raison de tout manquement, de la part du responsable du traitement des données ou de ses employés, aux obligations définies par cet accord.

5 NOMINATION DE SOUS-TRAITANTS ET D'AGENTS RESPONSABLES DU RESPECT DES PRINCIPES PAR LES SOUS-TRAITANTS ET LES AGENTS

5.1 Le responsable du traitement des données peut autoriser une tierce partie (sous-traitant ou agent) à traiter les données aux conditions suivantes.

a. Respect des conditions de cet accord.

b. Obtention du consentement écrit préalable du contrôleur des données. Le consentement ne sera valide que si le responsable du traitement des données fournit au contrôleur les coordonnées complètes et exactes des sous-traitants ou agents.

c. Résiliation automatique du contrat du sous-traitant ou de l'agent suivant la résiliation de cet accord, pour quelque raison que ce soit.

6 RÉSILIATION

6.1 Cet accord sera automatiquement résilié au moment de la résiliation ou expiration des obligations du responsable du traitement des données vis-à-vis des services.

6.2 Le contrôleur des données sera habilité à résilier cet accord sans délai par avis écrit au responsable du traitement des données dans les cas suivants.

a. En cas de violation grave ou persistante du responsable du traitement des données vis-à-vis de cet accord qui, si elle peut être réparée, n'aura pas été réparée dans un délai de [...] jours à compter de la date de réception, par le responsable du traitement des données, d'un avis émanant du contrôleur des données qui détermine la violation et qui en demande réparation.

b. Si le responsable du traitement des données devient insolvable ; si un séquestre, un administrateur ou un administrateur judiciaire est nommé pour tout ou partie de ses biens ; si le responsable du traitement des données conclut un quelconque concordat avec ses créanciers ; ou si un ordre a été émis ou une résolution a été adoptée pour le clôturer (autrement que pour prolonger un dispositif de fusion ou reconstruction).

6.3 Au moment de la résiliation de cet accord, le responsable du traitement des données doit, suivant les instructions du contrôleur des données :

- remettre ou détruire toutes les données personnelles fournies par le contrôleur des données dont il dispose ou qu'il contrôle ;
- donner l'ordre à tous ses employés, agents ou sous-traitants de faciliter et assurer la remise ou destruction des données personnelles, y compris les copies, selon les instructions du contrôleur des données.

7 LOI APPLICABLE

7.1 Cet accord sera régi par les lois de [...] et les parties se soumettent à la juridiction exclusive des cours de [...] pour tous les motifs relatifs à cet accord, y compris l'exécution de tout ordre émis ou jugement rendu conformément à cet accord ou en lien avec ce dernier.

8 RENONCIATION

8.1 Le non-exercice ou la non-application, par l'une ou l'autre des parties, de tout droit conféré à cette partie ou l'octroi de toute relaxe, abstention, retard ou indulgence ne seront pas interprétés comme une renonciation des droits de cette partie au titre de cet accord.

9 INVALIDITÉ

9.1 Si une quelconque condition ou clause de cet accord venait à être rendue illégale ou inexécutable, dans sa totalité ou en partie, au titre de quelque décret ou règle de droit que ce soit, alors cette condition ou clause, ou cette partie de condition ou de clause, devra être considérée dans cette mesure comme ne formant pas partie de cet accord. Toutefois, la force exécutoire du reste de cet accord ne sera pas affectée, sous réserve que, si une quelconque condition ou clause de cet accord vient à être rendue illégale ou inexécutable, les parties cherchent à modifier cet accord dans la mesure nécessaire pour le rendre légal et exécutoire, et pour qu'il reflète aussi fidèlement que possible les intentions des parties qui y sont représentées, y compris mais sans s'y limiter la condition ou clause, ou la partie de condition ou de clause illégale ou inexécutable.

CaLP
The Cash Learning Partnership

Ces principes et normes opérationnelles ont été élaborés par le CaLP, en collaboration avec un grand nombre d'organisations et de parties prenantes. Leur but est de permettre aux organisations de lutter contre les risques inhérents à l'utilisation des données des bénéficiaires par les organisations engagées dans la distribution d'argent avec une attention particulière sur les programmes de transfert électronique.

Ces risques sont associés à la collecte, au stockage, à l'utilisation et à la divulgation des données des bénéficiaires à l'occasion de la réception de transferts monétaires et électroniques. Ces données personnelles sont souvent plus volumineuses que celles rassemblées lors de distributions d'aide conventionnelles ; elles sont systématiquement partagées avec des partenaires commerciaux (ou générées par ces derniers) qui contribuent à la distribution de l'argent à l'aide de nouvelles technologies.

Ces risques sont, dans l'ensemble, largement méconnus et ils font l'objet de peu de solutions. Néanmoins, à mesure que les initiatives humanitaires adoptent de plus en plus de nouvelles technologies en vue de parvenir à une distribution plus efficace de l'aide, il est essentiel d'établir des normes. Celles-ci permettront de garantir que les bénéficiaires ne sont pas mis en danger ou désavantagés par leur implication dans des programmes de transfert monétaire.

Ces principes et normes opérationnelles sont une tentative d'établir de bonnes pratiques au sein du secteur, pour la collecte et le traitement des données des bénéficiaires. Ces principes et normes sont spécialement adressés aux responsables de programmes de transfert monétaire et électronique mais ils peuvent avoir une plus vaste application. Leur but n'est pas de détrôner ou remplacer les principes directeurs organisationnels existants en matière de protection des données ou de la vie privée, mais de les renforcer ou de les compléter lorsqu'ils n'abordent pas la protection des données des bénéficiaires ou qu'elles manquent de précision. Lorsqu'il n'existe pas de principes directeurs organisationnels sur la vie privée ou la protection des données, les normes et principes énoncés dans ce document constituent un cadre permettant de protéger les données des bénéficiaires.

Les principes et normes opérationnelles comprennent huit *principes* qui régissent la manière dont les données doivent être traitées et les mesures que doivent prendre les organisations afin d'y adhérer, sous la forme de *notes interprétatives des normes opérationnelles*. Des modèles de clauses pour les bénéficiaires sont fournis pour être adaptés par chaque organisation.

Ce document de recherche a été commissionné par le CaLP,
avec le soutien généreux de VISA Inc. et du DFID

VISA

UKaid
from the British people