Utilisation de données « sensibles »

Directives de traitement des données sensibles

Sommaire

Motivation

La majorité des programmes et autres activités de Mercy Corps recueillent des informations personnelles sur les personnes que nous servons et avec lesquelles nous travaillons, et beaucoup d'entre elles recueillent également des informations personnelles qui seraient classées comme sensibles. La collecte de données sensibles est essentielle pour nous permettre de mener à bien notre travail et de servir les participants aux programmes et les communautés dans lesquelles nous travaillons. Par conséquent, lorsque nous collectons et utilisons des données sensibles, il est essentiel que toutes les mesures nécessaires soient prises pour garantir la protection de ces données. Le fait de ne pas protéger les données sensibles peut entraîner de graves préjudices pour la personne concernée, y compris, mais sans s'y limiter, des discriminations et des menaces pour la sécurité.

Portée

Ces directives s'appliquent à tout traitement de données sensibles dans l'ensemble de l'agence. Il s'applique aux données sensibles collectées à des fins programmatiques et opérationnelles et à toute autre situation

où des données sensibles sont présentes. Ce document détaille les étapes nécessaires chaque fois qu'un traitement de données sensibles a lieu.

Qu'est-ce qu'une donnée sensible et pourquoi est-elle différente des autres types de données personnelles ?

Les données sensibles sont généralement des données telles que le profil culturel d'une personne, son orientation sexuelle, ses données de santé, ses données biométriques et génétiques. Il s'agit de données qui, si elles sont divulguées, consultées ou partagées de manière inappropriée, peuvent avoir pour conséquence :

- un préjudice (tel que des sanctions, des discriminations et des menaces pour la sécurité) pour une personne, y compris la source de l'information ou d'autres personnes ou groupes identifiables ;
- un impact négatif sur la capacité d'une organisation à mener ses activités ou sur la perception de cette organisation par le public.

Exemple 1 :

Un programme est mis en œuvre dans une communauté et, au cours du projet, plusieurs participants révèlent qu'ils sont séropositifs. Ces informations sont accidentellement partagées avec des membres haut placés de la communauté, ce qui peut entraîner un préjudice important, voire un danger physique, pour les participants au programme.

Exemple 2 :

Un bureau organise une fête et recueille les préférences alimentaires des membres de l'équipe. Plusieurs membres de l'équipe ont indiqué qu'ils avaient besoin de repas casher ou hallal. Une feuille de calcul identifiant les membres de l'équipe ayant des besoins alimentaires spécifiques est partagée avec l'ensemble de l'équipe. Certains membres de l'équipe n'ont pas partagé leur religion, car ils craignent la discrimination.

Les données sensibles doivent être traitées avec plus de précaution car leur collecte et leur utilisation sont plus susceptibles d'interférer avec les libertés et les droits fondamentaux d'une personne, ou de causer un préjudice important, notamment une discrimination ou un danger physique, en cas d'utilisation abusive.

Le règlement général sur la protection des données (RGPD) définit un certain nombre de types de données qui sont classées comme des données sensibles de catégorie spéciale et détaille les conditions de traitement spécifiques pour ces types de données. Toutefois, il est important de noter que dans certains contextes, les données qui ne font pas partie de la catégorie spéciale standard de données sensibles peuvent encore être sensibles en raison du contexte particulier. Aux fins de la présente note d'orientation, ces types de données seront appelés « données contextuellement sensibles ».

Cette note d'orientation est conçue en complément de Mercy Corps Politique relative aux données responsables ainsi que la Politique de gestion de programme (qui intègre également la Politique MEL) et s'applique à la collecte de données sensibles dans tous les contextes, y compris, mais sans s'y limiter, au siège, dans les programmes et dans les MEL.

Définitions de la terminologie clé

- **Données opérationnelles de Mercy Corps** – Tout élément d'information, composé de lettres, de chiffres, de symboles, d'images, d'enregistrements vidéo et vocaux, de coordonnées géospatiales ou d'identifiants de localisation, de cartographie ou de toute combinaison de ceux-ci, traitée par Mercy Corps. Cela peut inclure, sans s'y limiter, des données sur les membres de l'équipe de Mercy Corps, les vendeurs, les donateurs ou les partenaires. Les données existent à la fois sous forme numérique et physique.

- **Données sensibles** – Ces informations sont souvent utilisées comme base pour cibler un groupe ou un individu particulier. Des exemples courants sont la race, la religion, les opinions politiques, l'orientation sexuelle, la santé ou les informations biométriques.

  Aux fins de la présente note, les données sensibles comprennent les « données sensibles de catégorie spéciale » telles que définies dans le RGPD et les « données contextuellement sensibles »

- **Données sensibles de catégorie spéciale** – Le RGPD définit des exigences spécifiques pour le traitement de toutes les données sensibles de catégorie spéciale qui doivent être respectées. Le RGPD définit les données sensibles de catégorie spéciale comme :

  - les données personnelles révélant l'origine raciale ou ethnique ;
  - les données personnelles révélant des opinions politiques ;
  - les données personnelles révélant des convictions religieuses ou philosophiques ;
  - les données personnelles révélant l'appartenance syndicale ;
  - les données génétiques ;
  - les données biométriques (lorsqu'elles sont utilisées à des fins d'identification) ;
  - les données relatives à la santé ;
  - les données concernant la vie sexuelle d'une personne ; et
  - les données concernant l'orientation sexuelle d'une personne

- **Données contextuellement sensibles** – les données qui n'entrent pas dans les catégories de données sensibles telles que définies par le RGPD mais qui, en raison du contexte dans lequel elles sont traitées, sont sensibles par nature et qui pourraient causer un préjudice important à la personne concernée si elles étaient divulguées.

- **Violation de données personnelles** – Une violation de données à caractère personnel peut être définie de manière générale comme un incident de sécurité qui a affecté la confidentialité, l'intégrité

ou la disponibilité des données à caractère personnel. En résumé, il y a violation des données à caractère personnel lorsque des données à caractère personnel sont perdues, détruites, corrompues ou divulguées ; si quelqu'un accède aux données ou les transmet sans autorisation appropriée ; ou si les données sont rendues indisponibles, par exemple lorsqu'elles ont été cryptées par un ransomware, ou accidentellement perdues ou détruites.

- **Données de programme** – Toute unité d'information, composée de lettres, de chiffres, de symboles, d'images, d'enregistrements vidéo et vocaux, ou toute combinaison de ceux-ci, relative aux participants au programme, à sa mise en œuvre et à ses résultats. Les données existent à la fois sous forme numérique et physique.

- **Politique relative aux données responsables de Mercy Corps** – Politique de l'agence visant à établir des principes pour l'utilisation transparente, sûre et responsable des données personnelles dans l'ensemble de l'agence et l'intégration de ces principes dans notre travail quotidien.

- **Consentement éclairé** – Un processus permettant de recueillir la permission volontaire de collecter des données de toute nature, sur la base d'une appréciation et d'une compréhension claires des faits, des implications et des conséquences de tout engagement de la part des participants. Cet accord peut être donné soit par une déclaration écrite ou orale, soit par une action positive claire. L'accord doit être obtenu au moment de la collecte des données personnelles, ou dès que c'est raisonnablement possible par la suite.

- **Consentement explicite** – Le consentement explicite exige une déclaration de consentement très claire et spécifique. Il faut consigner quand et comment le consentement a été obtenu et ce qui a été dit exactement aux personnes concernées lors de l'obtention du consentement. Le consentement explicite doit spécifier la nature des données de la catégorie spéciale ; et il doit être distinct de tout autre consentement que vous recherchez.

- **Désidentification** – Toute activité ou méthode de traitement des données visant à empêcher que l'identité d'un participant ou d'une autre personne ne soit révélée directement et/ou indirectement. Exemples : l'anonymisation (c'est-à-dire la suppression de certaines quantités de données personnelles, ou l'application d'une gamme de valeurs sur certains ensembles de données personnelles) et la pseudonymisation (c'est-à-dire le traitement des données personnelles de telle sorte que les données personnelles ne puissent plus être attribuées à une personne ou à un ménage spécifique de personnes concernées sans l'utilisation d'informations supplémentaires telles que des identifiants ou des hachages uniques).

- **Informations personnellement identifiables (PII)** – Informations relatives à une personne physique identifiée ou identifiable (« personne concernée ») une personne identifiable est une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale.. Ceci est étroitement lié aux **informations démographiques identifiables (DII)** qui peuvent être utilisées pour identifier une communauté ou un groupe distinct, qu'il soit géographique, ethnique, religieux, économique ou politique.

- **Stockées en toute sécurité** – Seuls les membres nécessaires de l'équipe de Mercy Corps peuvent accéder aux données ; des mesures sont prises pour empêcher le vol et l'utilisation

abusive des données stockées en toute sécurité. Seuls les membres nécessaires de l'équipe de Mercy Corps peuvent accéder aux données ; des mesures sont prises pour empêcher le vol et l'utilisation abusive des données. Un fichier est stocké de manière sécurisée lorsque :

- Il est hébergé sur une plateforme qui respecte des normes strictes en matière de sécurité, de protection des données et de confidentialité.
- L'accès est limité aux seules parties requises.
- L'accès est régulièrement revu et ajusté si nécessaire.

> Des exigences supplémentaires sont énoncées pour les programmes de Mercy Corps dans la politique MEL nouvellement adoptée, en particulier la norme 9, qui exige que tous les programmes garantissent des pratiques de manipulation sûres, conformément à la politique de données responsables et aux exigences des donateurs.

> **Membres de l'équipe Mercy Corps nécessaires** – Membres de l'équipe qui ont besoin d'accéder aux informations identifiées afin d'accomplir des tâches spécifiques à leur travail, telles que répondre aux besoins des participants au programme et réaliser les livrables du programme.

> **Personne concernée** – Tout individu auprès duquel et sur lequel des données sont collectées directement, indirectement ou par l'intermédiaire d'un tiers, et qui peut être identifié, directement ou indirectement, notamment par référence à des données Personnelles.

> **Protection des données** – Sauvegarde et prévention de l'accès, de l'utilisation ou de la distribution non autorisés d'informations personnelles identifiables (PII), d'informations démographiques identifiables (IDI) et d'autres données sensibles concernant un individu ou un groupe tout au long du cycle de données de gestion du programme ou du projet, ou après l'achèvement du programme ou du projet. La politique de données responsable de Mercy Corps décrit les exigences en matière de protection des données, et l'agence est également soumise à d'autres cadres juridiques/réglementaires tels que le Règlement général sur la protection des données (RGPD) de l'Union européenne.

Pour plus de définitions relatives aux données responsables, voir le Document de définitions des données responsables.

Planification

- Réfléchissez aux types de données qui seront collectées et documentez-les dès la phase de planification du projet, dans l'évaluation des incidences sur la confidentialité (PIA).

- Lorsqu'un plan prévoit la collecte et/ou la documentation et/ou le stockage de tout type de données sensibles, il convient d'accorder une attention particulière à la manière dont ces données sont utilisées et aux raisons pour lesquelles elles le sont. Examinez si la collecte de ces données est nécessaire pour obtenir les résultats requis du programme ou du projet ou si un autre type de données serait suffisant. Les données sensibles ne doivent être collectées que si elles sont nécessaires. Veuillez noter que la collecte de données sensibles, si elle est bien faite, est un processus coûteux. En allégeant la charge de la collecte de données inutiles, vous permettez aux équipes d'économiser du temps et des ressources pour d'autres travaux nécessaires. Si vous

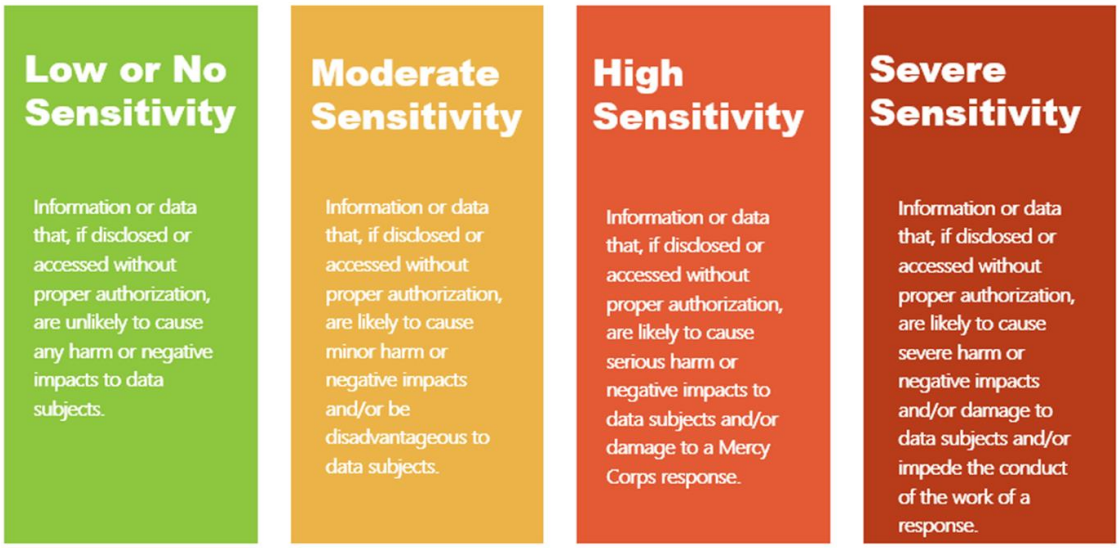
identifiez que les PII sont nécessaires, ne mettez pas en place des raccourcis. Si les ressources que vous allouez à la collecte et à la gestion des données sensibles ne sont pas suffisantes pour le faire correctement, reconsidérez l'ensemble des risques que vous pouvez faire courir aux communautés avec lesquelles vous travaillez.

- Réfléchissez aux technologies qui seront utilisées pour la collecte et le stockage. Les technologies utilisées doivent comporter des garanties appropriées pour la collecte d'informations sensibles.
- D'une manière générale, plus les données sont sensibles, plus vous devez mettre en place de mesures de protection. Les données sensibles sont généralement de sensibilité « élevée » ou « grave » (voir figure 1). En outre, plus le nombre de données collectées est élevé, plus le risque est grand et plus les garanties doivent être nombreuses. Les exemples de mesures de protection incluent, entre autres :
    - le cryptage
    - la pseudonymisation
    - la dissociation
    - le stockage de dossiers papier dans des armoires fermées à clé et à accès restreint.
    - le stockage de fichiers sur les serveurs de Mercy Corps avec des niveaux de protection
    - la restriction de l'accès aux appareils de Mercy Corps et sa réservation aux personnes qui doivent y avoir accès pour accomplir leurs tâches professionnelles.
    - la garantie que les appareils tels que les ordinateurs portables sont verrouillés lorsqu'ils ne sont pas utilisés.
    - Pour les données spatiales, randomisez ou regroupez les points GPS.

- Soyez clair quant au fondement juridique du traitement des données sensibles que vous utiliserez et planifiez en conséquence.
- Les exigences en matière de rapports dans les conventions de subvention doivent respecter les principes qui consiste à ne faire aucun tort (« Do No Harm ») (par exemple, le programme n'est pas censé collecter des informations susceptibles de compromettre la sécurité des participants) et décrire clairement les engagements et les accords pour les plateformes de partage des données, les processus avec le donateur, les partenaires et les autres parties prenantes, en intégrant les exigences de désidentification et d'anonymisation.
- Le protocole de sécurité des données au niveau du programme fait partie du plan technologique de la MEL (norme 6) et décrit les considérations relatives aux données des membres de l'équipe, y compris les niveaux de permission et les protocoles pour les membres de l'équipe MC et non MC.
- Lorsque des données sensibles sont collectées à des fins opérationnelles de Mercy Corps, planifiez et exposez les considérations relatives aux données, y compris les niveaux d'autorisation et les protocoles.

- Réfléchissez à la durée de conservation des données (période de conservation) et soyez en mesure de la justifier. Cette durée dépendra des raisons de la collecte des données, des exigences légales, des exigences des donateurs et des politiques de conservation des documents du programme MC.
- Disposer d'un processus pour la destruction des données lorsque les périodes de conservation sont respectées.

Figure 1 :



Planification de la collecte des données

- Une évaluation des incidences sur la confidentialité (PIA) est réalisée afin d'identifier et de gérer les risques de confidentialité des données associés à toute nouvelle activité, comme les nouveaux programmes, les nouvelles technologies ou les nouvelles politiques. Lorsque des données sensibles doivent être collectées, elles doivent être examinées par une personne compétente. Il s'agit de l'équipe chargée de la protection des données et de la confidentialité, de votre DPD ou de la politique de la MEL (norme minimale n° 9 - confidentialité et sécurité des données) :
    - Responsable - Directeur de pays, ou directeur des programmes et gestionnaire de programme ou chef de partie.
    - Responsable recommandé -Programme MEL/chef de la gestion des connaissances

- Effectuer une évaluation des informations sensibles (SIA) qui est liée à l'évaluation des facteurs de risque. Cela doit permettre de documenter toutes les mesures de protection supplémentaires utilisées pour les données sensibles.

- Si le consentement est la base juridique invoquée, le consentement éclairé exige que les personnes concernées soient informées des éléments suivants en langage clair :

    - Quelles sont les données collectées et pourquoi elles sont nécessaires
    - Avec qui ces informations seront partagées, y compris les partenaires externes et les donateurs
    - Si les données seront partagées au niveau international
    - Combien de temps les données seront-elles conservées ?
- Il convient de conserver une trace de la date et de la manière dont le consentement a été recueilli et de ce qui a été dit à la personne concernée. Un modèle de ce qui sera dit aux personnes concernées pour obtenir leur consentement devrait être inclus dans la phase de planification.

Collecte de données

- Un protocole de collecte de données est en place pour chaque instance de collecte de données, qui comprend :
    - les garanties supplémentaires pour les données sensibles
    - les instructions documentées pour la collecte, le nettoyage des données, la révision et la dépersonnalisation, le cas échéant
    - les instructions relatives aux violations potentielles de la sécurité des données pour toutes les données quantitatives et qualitatives collectées (par exemple, appareils perdus ou volés, identifiants compromis, etc.)
    - les instructions pour l'utilisation et la protection des formulaires papier pendant la collecte
    - les contrôles ponctuels et le suivi de la mesure dans laquelle les protocoles de sauvegarde et de protection sont respectés par la ou les personnes chargées de la collecte des données.
- Tous ces éléments doivent être liés à l'EIS

Stockage des données

- Les fichiers contenant des informations sensibles doivent être limités aux membres de l'équipe qui ont besoin d'accéder à ces informations pour mener à bien les tâches nécessaires, et la dépersonnalisation systématique des informations sensibles est effectuée avant de les relier à TolaData ou de les partager avec un tiers, le cas échéant. La norme de politique 8 de la MEL fournit des conseils supplémentaires sur les meilleures pratiques de classement et de stockage des données de la MEL.
- Les données sont stockées dans un endroit conforme à toutes les politiques pertinentes de Mercy Corps (par exemple, la politique de données responsables, l'utilisation acceptable).
- Les données sensibles ne doivent pas être conservées plus longtemps que nécessaire. Lorsque les délais de conservation sont respectés, les données doivent être détruites de manière sécurisée ou entièrement anonymisées.
- Les périodes de conservation doivent être documentées et justifiées.

- N'oubliez pas que les données peuvent également être stockées dans des systèmes mobiles de collecte de données. Toutes les considérations relatives au stockage des données mentionnées ci-dessus s'appliquent également aux systèmes mobiles de collecte de données.

Analyse des données

- Il existe un protocole pour le partage des données avec les consultants, les équipes du siège, les partenaires, les parties prenantes, y compris, mais sans s'y limiter, les accords de partage des données, les approbations par le MEL du pays, les rôles et les responsabilités, etc.

- Des accords de non-divulgation (AND) sont signés par tous les consultants avant d'accéder à tout ensemble de données appartenant à Mercy Corps.

Soumission des données au donateur, au partenaire ou à un autre tiers (le cas échéant)

- Les données brutes sont dépourvues d'identification et examinées pour vérifier qu'elles sont conformes aux principes qui consiste à ne faire aucun tort (« Do no Harm ») avant d'être soumises.

- Les données sensibles ne doivent pas être partagées avec un tiers qui n'a pas été mentionné dans le cadre du processus de consentement éclairé.

- Les données sensibles ne doivent pas être partagées avec des tiers, sauf si un accord de partage des données a été conclu.

- N'utilisez que des systèmes organisationnels autorisés tels que Google Drive ou Microsoft Sharepoint pour partager des documents, et non des plateformes de partage tierces.

Questions-réponses

Pour nous assurer que nous respectons les exigences en matière de diversité, nous demandons aux membres de l'équipe d'indiquer leur statut ethnique sur les formulaires de demande d'emploi - dois-je faire quelque chose à ce sujet ?

Oui, les données relatives à l'origine raciale ou ethnique sont considérées comme des données personnelles sensibles. Vous devrez donc suivre les directives relatives aux données sensibles et appliquer des garanties supplémentaires à ces données.

Que se passe-t-il si moi ou un membre de l'équipe avons accidentellement et involontairement partagé des données sensibles ? Quelles mesures correctives peuvent être prises ?

Lorsque l'on découvre un partage accidentel de données personnelles, le partage des données doit cesser immédiatement. Il peut s'agir de demander au destinataire accidentel de supprimer toute copie des données, d'empêcher le destinataire accidentel d'accéder aux données, de mettre les données hors ligne ou de prendre d'autres mesures si nécessaire.

Le partage accidentel ou involontaire de données personnelles est considéré comme une violation de données et vous devez en informer immédiatement **it-security@mercycorps.org** conformément au plan de réponse aux incidents. Il convient de fournir le plus d'informations possible, dès que vous le pouvez, sur la nature des données partagées.

Que dois-je faire lorsque je vois un membre de l'équipe partager intentionnellement des données sensibles avec une personne qui ne devrait pas avoir accès à ces données ?

La communication intentionnelle de données sensibles à une personne non autorisée est extrêmement grave, car elle peut entraîner un préjudice grave pour la personne concernée et pour l'agence. Si vous voyez un membre de l'équipe partager intentionnellement des informations sensibles de cette manière, vous devez le signaler immédiatement au responsable du programme, au directeur régional ou à votre directeur.

Le partage de données sensibles avec des personnes qui ne devraient pas y avoir accès constitue également une violation des données et doit être signalé immédiatement à **it-security@mercycorps.org** conformément au plan de réponse aux incidents. Il convient de fournir le plus d'informations possible sur la nature des données partagées, dès que vous le pouvez.

Comment le programme décide-t-il qui doit/ne doit pas avoir accès aux données sensibles ?

L'accès aux données sensibles ne doit être accordé qu'aux personnes qui en ont besoin pour remplir leur rôle. Les données sensibles doivent toujours être masquées avant d'être partagées, si possible. L'anonymisation ou la pseudonymisation sont des exemples courants de masquage.

Qu'est-ce qu'une donnée dissociée ?

Les données dissociées sont des données qui ont été complètement et irréversiblement détachées de la personne concernée, de sorte qu'il n'est plus possible de réassocier les données à une personne concernée. Les données dissociées sont un type d'anonymisation des données.

Dois-je activer des alertes sur les données électroniques en cas d'accès par une personne non autorisée ?

S'il est possible de déclencher des alertes en cas d'accès non autorisé, il faut toujours les activer, mais toutes les plateformes électroniques ne disposent pas de cette fonctionnalité. Vérifiez les paramètres système de votre plateforme et, si possible, activez les alertes.

Les membres de l'équipe doivent-ils utiliser des appareils personnels pour recueillir ou stocker des informations sensibles ? Si c'est le cas, quelles sont les protections à prévoir ?

Les appareils personnels ne doivent pas être utilisés pour collecter ou stocker des informations personnelles, y compris des informations sur les participants, *à moins qu'un logiciel de gestion des appareils approprié n'ait été installé* et que l'utilisation des appareils personnels ne soit consignée dans l'EFVP du projet. Les appareils personnels ne doivent jamais être utilisés pour la collecte des données des participants sans l'autorisation expresse du responsable du programme. Les appareils personnels ne doivent pas être utilisés pour collecter ou stocker des informations sensibles.

Mon donateur peut-il contrôler la façon dont je traite les données sensibles ?

Oui, de nombreux donateurs exigent des audits internes et externes de la qualité des données et des évaluations de la qualité des données. Un aspect de ces évaluations consiste à évaluer le système MEL pour les chocs, les invasions et la sécurité, en particulier si le programme collecte des informations sensibles.

Puis-je lier les listes de participants à TolaData comme preuve ?

Les listes de participants (par exemple, les listes de présence aux formations, etc.) peuvent être liées en tant que preuves puisque ces preuves doivent être hébergées et stockées en dehors de TolaData, donc seules certaines personnes auront accès à ces preuves, en fonction des permissions de ce lieu de stockage externe. Il convient d'examiner si un type de preuve lié à TolaData nécessite l'inclusion d'informations personnelles. Il est extrêmement peu probable que l'inclusion d'informations sensibles soit nécessaire.

Comment puis-je savoir si les fournisseurs ou les plateformes de technologies de collecte ou de stockage des données sont conformes aux exigences en matière de données sensibles ?

Les plateformes existantes de collecte et de stockage des données de la MEL Tech Suite sont déjà conformes aux exigences en matière de données sensibles, à condition qu'elles soient configurées de manière appropriée pour utiliser les mesures de protection et les protocoles mentionnés dans ce document. Si une plateforme extérieure à la MEL Tech Suite doit être utilisée, une évaluation des incidences sur la confidentialité (PIA) doit être réalisée pour déterminer si elle peut être considérée comme conforme aux exigences en matière de données sensibles. Pour ce qui est de l'évaluation d'un fournisseur de technologie et de sa volonté de se conformer à la politique en matière de données responsables et aux exigences en matière de données sensibles, une EFVP est encore une fois le meilleur outil pour déterminer si ses pratiques seront considérées comme conformes.

Comment puis-je savoir si des données sont des données personnelles ou sensibles ?

Si vous traitez des données qui relèvent de l'une des catégories spéciales de données sensibles définies par le GDPR (voir la section **Catégories spéciales de données sensibles** ci-dessus), il s'agira toujours de données sensibles. S'il existe une raison spécifique au contexte pour laquelle les données entrent dans la catégorie « sensibilité sévère » (voir la figure 1 ci-dessus), elles doivent également être classées comme des données sensibles.

Documents connexes :

Consentement

Outil MEL : Modèle de consentement éclairé (pour les participants aux entretiens)Guide du consentement éclairé pour le partage des donnée CARM

COVID-19 Guidage à distance de MERL

Cryptage

Utilisation de Ona.io à Mercy Corps : cryptage des formulaires et des données sensibles

Données biométriques

Biométrie @ Mercy Corps : Introduction interne

Directives d'ordre général

- Data Responsibility Toolkit – A guide for Cash and Voucher Practitioners - https://www.calpnetwork.org/wp-content/uploads/2021/03/Data-Responsibility-Toolkit_A-guide-for-Cash-and-Voucher-Practitioners.pdf
- ELAN Data Starter Kit for Humanitarian Field Staff: v https://www.calpnetwork.org/wp-content/uploads/2020/06/DataStarterKitforFieldStaffELAN.pdf
- ICRC Handbook on Data Protection in Humanitarian Action: https://www.icrc.org/en/data-protection-humanitarian-action-handbook.

Informations de désidentification

Directives de l'USDA pour l'examen des informations personnellement identifiables (PII) dans les évaluations de projets

Poverty Action Lab « Désidentification pour la publication des données »

Générer des codes uniques pour les participants au programme ou d'autres personnes concernées

Projet d'orientation du T4D

Évaluations

Évaluation des incidences sur la confidentialité (PIA)- modèle

Évaluation des incidences sur la confidentialité (PIA)- Directives

Évaluation des informations sensibles (SIA)