# 7 Pratiques responsables et protection des données

# Table des Matières du Module

# Pratiques responsables et protection des données

**La protection et l'utilisation responsable des données sont des priorités absolues à la FICR et dans l'ensemble du Mouvement. Avec ce module, nous espérons fournir des informations et des exercices qui explorent les questions auxquelles vous pourriez être confrontés et vous aider à être mieux préparés à comprendre et à résoudre ces questions dans la pratique.**

Comme pour tout contenu de nature générale, les conseils (et les exemples) contenus dans le module sont uniquement destinés à servir de point de départ. Vous devez faire preuve de vigilance, en faisant appel à un conseiller juridique le cas échéant, pour déterminer quelles sont les obligations légales spécifiques (ou autres considérations pertinentes) dans votre contexte d'exploitation.

# Questions que ce module explore :

- Que signifient l'utilisation responsable et la protection des données pour les humanitaires et pourquoi ces concepts sont-ils importants ?
- Quelles sont les différences entre les données non personnelles, les données personnelles et les données sensibles et pourquoi est-il important de connaître ces différences ?
- Que faut-il faire pour protéger et utiliser les données de manière responsable dans la pratique ?

# Objectifs d'apprentissage

- Comprendre pourquoi l'utilisation responsable des données et la protection des données sont importantes pour la mise en œuvre du travail de la FICR et comment elles sont liées aux principes humanitaires ;
- Développer la confiance et les connaissances nécessaires pour identifier et distinguer les différents types de données (par exemple les données non personnelles, personnelles, sensibles et les données de groupes sensibles) et ce que cela signifie pour la façon dont elles devraient être utilisées de manière responsable ; et
- Explorer les facteurs juridiques, éthiques, pratiques et culturels qui ont un impact sur la protection des données dans la pratique dans des situations d'urgence complexes.

# Sujets du Module

- Utiliser les données de manière responsable implique de les protéger, mais aussi de réfléchir à des responsabilités humanitaires plus larges telles que Ne pas nuire et l'Impartialité.
- Faire la distinction entre les différents types de données peut permettre de mieux comprendre quelles données doivent être protégées. Les humanitaires ont le devoir de protéger et d'utiliser de manière responsable les informations qui pourraient être utilisées pour identifier un individu ou un groupe vulnérable.

- Il est important de travailler avec les communautés locales pour identifier les risques éventuels auxquels elles sont exposées, puis de prendre des mesures pour utiliser ces données de manière responsable.
- L'utilisation responsable et la protection des données doivent être prises en compte à chaque étape du déroulement d'un projet et doivent être réfléchies avant le début de toute nouvelle activité de collecte de données.
- La manière dont les données doivent être protégées et utilisées de manière responsable dans un contexte donné dépend largement du mandat de la FICR/SN pour opérer dans ce contexte. En tant qu'humanitaires, le consentement des communautés n'est pas toujours nécessaire pour utiliser des données les concernant, mais ces données doivent toujours être utilisées de manière responsable.
- La documentation des décisions (et de la manière dont elles ont été prises) concernant la protection et l'utilisation des données est un élément clé de l'utilisation responsable des données. Les évaluations de l'impact de la protection des données, les accords de partage des données et les formulaires de consentement peuvent être utiles à cet égard.

# Recettes

## Une proposition de processus étape par étape pour atteindre les objectifs d'apprentissage

1. Comment intégrer dans notre travail les meilleures pratiques en matière de protection et d'utilisation responsable des données ? Avec vos équipes, explorez : **Les gens avant les données (polycopié) (7 - 16)**, **De quelles données avons-nous vraiment besoin ? (7 - 9)**, **Que pouvons-nous faire VS que devrions-nous faire ? (7 - 10)**
2. Les humanitaires collaborent entre organisations. Le partage des données est important pour la réponse humanitaire. Cependant, le partage des données doit se faire avec prudence et être guidé par les pratiques de protection des données et d'utilisation responsable des données. Commencez par une brève discussion. **Would you Share it? (7 - 12).** Les équipes peuvent ensuite planifier leurs projets existants en examinant ce document et la checklist associée : **Accords de partage des données (partie 1) (7 - 1)** (partie 1 et partie 2).
3. combined with the **Humanitarian Values & Data Protection (7 - 8)** Comment la protection des données s'aligne-t-elle avec nos valeurs et nos principes ? **Valeurs humanitaires et protection des données** (exercice) **(7 - 7)** combiné au document **Valeurs humanitaires et protection des données (7 - 8)** (polycopié) peut guider les équipes dans ces conversations.
4. Le **Suivi de la campagne contre la polio en Syrie (7 - 17)**, la **Simulation de données PMER (7 - 15)** " simulent " les flux de données pour différents sujets. Les équipes doivent utiliser ces scénarios en conjonction avec **Renforcer les équipes et les projets de données (3)** (Module 3).

# Ingrédients

Choisissez les ingrédients pour créer votre propre recette. Avez-vous un ingrédient qui nous manque ? Envoyer un mail à data.literacy@ifrc.org

# Exercices

## Des expériences d'apprentissage social courtes et discrètes

- Quelles sont les données dont nous avons vraiment besoin ?
- Que devrions-nous faire VS que pouvons-nous faire ?
- Responsabilité des données (scénario)
- Protection des données PMER (scénario)
- Suivi de la Polio (scénario)

# Plans de session

## Des expériences d'apprentissage social plus longues

- Club de débat - Protection des données et risques numériques
- Dans leurs baskets
- Faire coïncider les valeurs humanitaires et les principes de protection des données
- Le cauchemar de la protection des données
- La roue de l'infortune

# Diaporamas

## Présentations à utiliser et/ou à adapter :

Fournit un contexte pour l'utilisation des données et son importance au sein de la FICR.

- Comprendre et identifier les différents types de données
- Comprendre la "base légale"

# Checklists/Documents/Matériels

### Pour la documentation des éléments essentiels de l'expérience d'apprentissage

- Accords de partage des données (partie 1)
- Accords de partage des données (partie 2)
- Principes d'appariement (polycopié)
- Hygiène des données (checklist)
- Les personnes avant les données (polycopié)

# Prochaines étapes

## Modules pertinents du Data Playbook

- (Module 3 : Renforcer les équipes et les projets de données) et (Module 4 : Obtenir les données dont nous avons besoin)

## Ressources

- IFRC Data Protection guidance
- Handbook on Data Protection in Humanitarian Action, 2nd Edition (ICRC)
- IASC Operational Guidance on Data Responsibility in Humanitarian Action
- OCHA Data Responsibility Guidelines
- IFRC Digital Transformation Strategy
- Digital Dilemmas (interactive website)

## Crédit

James De France, Tom Orrell, Heather Leson, contributeurs IFRC V1 Sprint et Data Playbook Beta

# 7 - 1 Accords de partage des données

## partie 1

**Dans le cadre de notre travail, de nombreuses questions sont posées sur le "partage des données" et les "accords de partage des données". Ce document peut être utilisé avant le déploiement/la session de planification du projet dans le cadre d'une formation à l'utilisation responsable des données et à la protection des données. Il peut également être utilisé sur le terrain comme outil de référence rapide et checklist pour aider le personnel à réfléchir aux modalités du partage des données.**

Le partage des données consiste à permettre à d'autres personnes ou organisations d'accéder aux données dont vous êtes responsable. Le partage de données peut aller de l'envoi par e-mail d'une feuille de calcul à un collègue d'une autre organisation humanitaire à l'octroi d'un accès limité aux données de la Croix-Rouge et du Croissant-Rouge à des gouvernements. Ce document explique les accords de partage de données. Vous trouverez dans la partie 2 un document à remplir au fur et à mesure de la coordination.

# Qu'est-ce qu'un accord de partage de données ?

Dans le cadre des activités de la Croix-Rouge et du Croissant-Rouge, les "accords de partage des données" (APD) désignent une série de documents qui couvrent le transfert de données au sein du Mouvement et entre celui-ci et ses partenaires gouvernementaux et non gouvernementaux. Les APD doivent tenir compte d'un certain nombre de considérations et, lorsqu'ils concernent le partage de données personnelles ou sensibles, ils doivent définir clairement la manière dont ces données seront protégées et les droits des individus respectés.

Au minimum, les APD doivent établir clairement et avec un certain degré de certitude quelles données seront partagées, comment les données seront partagées, pourquoi elles sont partagées, à quoi elles serviront, qui partagera et recevra les données, quand et où le partage aura lieu, et comment s'assurer que les données sont protégées et ne sont pas utilisées à mauvais escient après le partage. Dans l'idéal, les APD devraient également inclure des conditions relatives au respect des droits de propriété intellectuelle, à la résolution des litiges liés à l'accord et à toute autre considération pertinente.

Au sein de la Croix-Rouge et du Croissant-Rouge, les APD devraient être utilisés chaque fois que des données sont transférées à l'intérieur, à l'extérieur ou entre les différentes organisations qui composent le Mouvement.

# Que comprend un accord de partage de données ?

| Contenus | Explication |
|---|---|
| **Quelles données devraient être partagées ?** | ◉ Soyez aussi précis que possible sur les ensembles de données qui seront partagés. Dans l'idéal, dressez-en la liste.<br>◉ Il est extrêmement important que vous sépariez les ensembles de données "personnelles et sensibles" des ensembles de données "non personnelles" et que vous vous assuriez de respecter toutes les lois locales applicables en matière de protection des données et de la vie privée, ainsi que les orientations de la FICR sur le partage des données personnelles. |

| | |
|---|---|
| **Qui envoie des données et qui les reçoit ?** | ◉ Indiquez tous les noms et coordonnées des organisations/personnes qui partageront les données - à la fois celles qui envoient les données et celles qui les reçoivent.<br>◉ Si tout ou partie des données partagées appartiennent à une autre organisation, assurez-vous que vous avez la permission de les partager ou incluez-la dans l'accord si elle a le contrôle des données. |
| **Quand le partage des données commencera-t-il et quand prendra-t-il fin ?** | ◉ Spécifiez les dates de début et de fin du partage des données. Précisez ce qu'il adviendra des données à la fin de l'accord - seront-elles renvoyées au fournisseur de données, supprimées, archivées, etc.<br>◉ Si vous n'êtes pas sûr de la date à laquelle le partage des données prendra fin, ajoutez une clause dans votre accord stipulant que vous réexaminerez le calendrier à un moment opportun (par exemple, vous pourriez convenir de réexaminer la situation dans un mois, trois mois ou un an, en fonction de la nature de vos besoins à ce moment-là). |
| **S'il s'agit de données à caractère personnel, quelles sont les mesures nécessaires pour s'assurer qu'elles continuent d'être protégées pendant et après le transfert (l'accès est fourni) ?** | ◉ Examiner le plan de partage des données proposé en tenant compte de tous les principes de protection des données : base juridique, minimisation, limitation de la finalité, sécurité des données, transparence, proportionnalité et droits des personnes concernées. |
| **Pourquoi les données sont-elles partagées ?** | ◉ Veillez à énumérer clairement les raisons pour lesquelles les données sont partagées.<br>◉ Si des données personnelles ou sensibles sont partagées, assurez-vous de documenter toutes les bases légales légitimes sur lesquelles ces données sont partagées. |
| **Comment les données sont-elles partagées ?** | ◉ Le DSA doit préciser comment les données seront transférées ; par exemple, par email, en accordant un accès à distance à un serveur, via le cloud, etc.<br>◉ Dans la mesure du possible, l'accord doit préciser les normes et les formats qui s'appliquent aux données partagées. |
| **D'où viennent les données partagées et où vont-elles ?** | ◉ Il est important de préciser d'où et vers où les données sont transférées, car cela peut avoir une incidence sur les lois qui couvrent le partage des données. Par exemple, en vertu du règlement général sur la protection des données (RGPD) de l'Union européenne, il existe des règles spéciales qui doivent être suivies lors des transferts internationaux de données. Chaque organisation et/ou région/pays peut avoir ses propres obligations légales en matière de protection des données.<br>◉ L'accord doit préciser quelles lois du pays (juridiction) s'appliquent à l'accord et garantir que le DSA se conforme à ces exigences. Cela peut nécessiter des conseils juridiques.<br>◉ Cela nécessitera un examen de toutes les lois nationales ou régionales applicables en matière de protection des données et de la vie privée. |

| Contenus | Explication |
|---|---|
| **Autre Considérations** | ◉ Qui détiendra les droits de propriété intellectuelle sur les résultats obtenus à partir des données partagées ?<br>◉ Qui couvrira les coûts associés au transfert, au traitement ou à l'analyse des données ?<br>◉ Comment seront utilisés les logos et emblèmes de la Croix-Rouge et du Croissant-Rouge relatifs aux données ?<br>◉ Qu'adviendra-t-il de l'accord en cas de circonstances imprévues l'interrompant (force majeure) ?<br>◉ Comment vous et les autres parties à l'accord conviendrez-vous de vous dédommager mutuellement et de vous protéger financièrement en cas de perte financière (indemnisation) ?<br><br>Si vous opérez dans un contexte d'urgence très stressant et que vous devez partager rapidement des données avec un partenaire de confiance tel qu'un collègue d'une autre agence humanitaire dans des circonstances exceptionnelles, n'oubliez pas de prendre en compte les éléments suivants :<br><br>◉ Vous pouvez partager des données non personnelles sauf s'il y a une bonne raison de ne pas le faire - NE PAS partager de données à l'extérieur qui pourraient mettre en danger des individus ou des communautés, compromettre la mise en œuvre de programmes ou d'opérations humanitaires, ou de discréditer le Mouvement.<br>◉ Si vous devez partager des données personnelles :<br>— Réfléchissez aux données précises que vous devez partager pour répondre à votre besoin urgent et à la meilleure façon de les partager ;<br>— Convenez de la manière dont les données seront utilisées, des personnes avec lesquelles elles doivent ou ne doivent pas être partagées à nouveau et des mesures qui seront prises pour les protéger ;<br>— Fixer un délai pour l'utilisation des données partagées et convenir de ce que vous ferez des données une fois qu'elles auront été utilisées. Convenez du moment et de la manière dont vous formaliserez votre partage de données ;<br>— Déterminez s'il convient de procéder à une analyse d'impact sur la protection des données (DPIA) ; et<br>— Veillez à documenter vos décisions en matière de partage de données et à conclure un accord de partage de données dès que possible. Tout partage de données personnelles ou sensibles doit être documenté et enregistré. |

## Crédit

Tom Orrell, consultant FICR Data Playbook

# 7 - 2 Accords de partage des données

## partie 2

**Dans le cadre de notre travail, de nombreuses questions sont posées sur le "partage des données" et les "accords de partage des données". Ce document peut être utilisé avant le déploiement/la session de planification du projet dans le cadre d'une formation à l'utilisation responsable des données et à la protection des données. Il peut également être utilisé sur le terrain comme outil de référence rapide et liste de contrôle pour aider le personnel à réfléchir aux exigences du partage des données. Le partage des données consiste à permettre à d'autres personnes ou organisations d'accéder aux données dont vous êtes responsable. Le partage de données peut aller de l'envoi par email d'une feuille de calcul à un collègue d'une autre organisation humanitaire à l'octroi d'un accès limité aux données de la Croix-Rouge et du Croissant-Rouge à des gouvernements. Ce document peut être utilisé avec la partie 1 (explications).**

# Coordonnez votre accord de partage des données :

| Contenus | Description |
|---|---|
| **Qui envoie des données et qui les reçoit ?** | |
| **Quand le partage des données commencera-t-il et quand prendra-t-il fin ?** | |
| **Quelles sont les données partagées ?** | |
| **Pourquoi les données sont-elles partagées ?** | |
| **Comment les données sont-elles partagées ?** | |
| **D'où viennent les données partagées et où vont-elles ?** | |
| **Autres Considérations**<br>◉ Qui détiendra les droits de propriété intellectuelle sur les résultats obtenus à partir des données partagées ?<br>◉ Si des données à caractère personnel sont concernées, quelles sont les mesures nécessaires pour garantir qu'elles continuent à être protégées pendant et après le transfert (l'accès est fourni) ? Examiner en gardant à l'esprit tous les principes de protection des données : c'est-à-dire la base juridique, la minimisation, la limitation de la finalité, la sécurité des données, la transparence, la proportionnalité et les droits des personnes concernées.<br>◉ Qui couvrira les coûts liés au transfert, au traitement ou à l'analyse des données ?<br>◉ Comment seront utilisés les logos et emblèmes de la Croix-Rouge et du Croissant-Rouge relatifs aux données ?<br>◉ Qu'adviendra-t-il de l'accord si une circonstance imprévue l'interrompt (force majeure) ?<br>◉ Comment vous et les autres parties à l'accord conviendrez-vous de vous dédommager mutuellement et de vous protéger financièrement en cas de perte financière (indemnisation) ? | |

## Crédit

Tom Orrell, consultant FICR Data Playbook

# 7 – 3 Club de débat - Protection des données et risques numériques

**Les organisations et les individus ont de nombreuses questions et préoccupations concernant la protection des données, les données responsables et le risque numérique. Au cours de cette session interactive, nous organiserons un "club de débat informel". L'objectif est de discuter ouvertement (avec humour et en jouant des rôles) de certaines de ces questions et préoccupations. Le résultat est une liste de questions/politiques et de pratiques qui nécessitent plus d'explications/une compréhension partagée.**

Chaque participant travaillera en petits groupes pour rédiger des "déclarations" informelles qui pourraient être débattues sur des sujets de haut niveau. Un exemple de déclaration est le suivant : "Les avantages de l'IA l'emportent sur tout risque de biais". Chaque groupe/individu fera des déclarations sur son "accord" ou son "désaccord" avec les déclarations. Il est recommandé de débattre des différents points de vue afin d'encourager les discussions et de mettre en évidence les nuances des sujets. Les participants doivent être encouragés à discuter du sujet dans le cadre d'un jeu de rôle animé. Cette session s'adresse à tous les publics et vise à explorer les préoccupations liées à l'utilisation responsable des données, à la protection des données et aux risques numériques. Invitez des experts en la matière à se rendre disponibles pour l'introduction et pour la discussion qui suivra cette session. Il peut s'agir par exemple d'un responsable de la cybersécurité, d'un juriste, d'un responsable de la communication ou d'un collègue chargé de la politique.

- **Personnes :** 5 à 30 personnes
- **Durée :** 60 Minutes
- **Difficulté :** Facile
- **Matériel virtuel** : plate-forme de réunion virtuelle, espace de rédaction/documentation partagé
- **Matériel en personne** : Tableau, post-it, marqueurs

# Exercice

Directives pour la session : Informez les participants qu'il n'y aura pas d'enregistrement ni de citations directement identifiables des conversations. L'objectif est de créer un espace de conversation ouvert.

## Partie 1 : Mise en situation

- Accueillir les participants à la session
- Présentez les experts invités.
- Commencez la session par une brève introduction aux sujets (quelques définitions et politiques/pratiques sur le lieu de travail) et donnez quelques exemples pour que les participants réfléchissent au contexte du travail.
- En fonction de la taille du groupe et de l'équipe, demander aux participants de partager une chose qui les préoccupe au sujet des données et des risques numériques.
- Expliquer l'exercice (parties 2 à 4)
- Montrez comment se déroule la partie "débat". Discutez avec deux personnes pour illustrer le déroulement d'un "débat".

Quelques Exemples :

- Les avantages de l'IA l'emportent sur tout risque de biais

- Le gouvernement protège tous les citoyens vulnérables et nous devons donc partager les données personnelles des citoyens avec le gouvernement.
- Nous devons partager les données relatives au VIH des bénéficiaires avec les organismes de santé des gouvernements locaux.
- Lorsqu'une délégation/un donateur paie pour un programme, ils devraient avoir droit à toutes les données du client (y compris les données personnelles).
- Nous devrions payer une rançon en cas de cyberattaque par ransomware.
- Tant que nous obtenons le consentement, nous n'aurons pas de problème de protection des données.

Chaque "présentateur" dira s'il est d'accord ou non avec l'affirmation. Encouragez les réponses colorées.

- Facultatif : Dans le cadre d'un événement virtuel, vous pouvez également proposer une série de déclarations préparées afin d'inciter les participants à réfléchir et à collaborer sur des déclarations expliquant pourquoi ils sont d'accord ou non avec l'affirmation. Demandez aux participants de mettre leurs initiales sur la ligne, puis demandez-leur d'expliquer.

## Partie 2 : Groupes de travail

En groupes de 2 à 4 personnes, présentez-vous. Créez jusqu'à 5 "déclarations" en rapport avec le thème de la session - "Quels sont les exemples de données responsables, de protection des données et de risques numériques ? "Les déclarations doivent inspirer le débat : elles doivent être controversées et créatives. Prenez des notes dans le document collaboratif ou sur des post-it. Notez également les questions qui devraient être abordées à l'avenir. Nous les utiliserons lors du "DÉBAT" en séance plénière. Choisissez vos deux meilleures affirmations pour les présenter au "club de débat".

## Partie 3 : Débat en Plénière

Chaque équipe présente à tour de rôle sa "déclaration". L'un des membres de l'équipe doit présenter le point de vue "d'accord" ou "pas d'accord". Ouvrez la discussion et demandez aux participants de partager leurs points de vue. Notez les observations, les idées et les questions.

En fonction de la durée de la session et de la taille du groupe, faites 3 ou 4 tours de déclarations.

## Partie 4 : Coordonner les questions et les idées

Demander aux participants - Quelles sont les questions en suspens qu'ils ont identifiées ? Des idées ? Notez-les dans votre document de travail ou sur un tableau.

## Bonus

Utilisez cet exercice pour favoriser la discussion au sein de l'équipe avant de partager les politiques et pratiques de votre organisation en matière de protection des données et de gestion responsable des données.

## Ressources

- IFRC Data Protection Guidance
- InterAgency Standing Committee Guidance on Data Responsibility
- Facilitation guidance (Aspiration, Exercice spectrogramme)

## Crédit

Aspiration, participants IFRC Data and Digital Week

# 7 - 4 Comprendre et identifier différents types de données

Réfléchissez aux données que vous utilisez dans le cadre d'un projet. S'agit-il de données **non personnelles**, **personnelles**, **sensibles** ou de **groupes de données** sensibles ?

Identifiez les **catégories** de données que vous utilisez. Vous pourrez ensuite élaborer un plan pour protéger et utiliser les données de manière **responsable**.

# Données personnelles

Les données à caractère personnel sont toutes les données qui peuvent être utilisées pour identifier une personne, qu'elles soient isolées ou combinées à d'autres données.

**Exemples :**

- Le nom, l'adresse, la date de naissance et le numéro de sécurité sociale d'une personne peuvent être considérés comme des données à caractère personnel s'ils peuvent être utilisés pour l'identifier.
- Les données personnelles peuvent inclure des éléments tels que les coordonnées GPS (localisation) d'une personne, son adresse IP ou les cookies de son navigateur internet.

# Données personnelles

## Le contexte est important :

- N'oubliez pas que le contexte est important. Par exemple, certains noms qui peuvent être très courants dans un pays - et donc susceptibles de ne pas constituer des données à caractère personnel en soi- peuvent être considérés comme des données à caractère personnel s'ils apparaissent dans des pays où ils sont rares - et donc plus susceptibles de permettre l'identification d'une personne.

## Agrégation (combinaison) d'ensembles de données :

- Certaines données, qui peuvent être non personnelles en soi, peuvent devenir personnelles si elles sont combinées à d'autres données.
  - **Exemple** : les données GPS d'un véhicule de la FICR sur le terrain ne sont probablement pas des données personnelles en soi, mais si elles sont combinées avec les données d'un registre des chauffeurs agréés de la FICR, elles pourraient devenir des données à caractère personnel car il est probable que le conducteur du véhicule puisse être identifié comme une personne si les deux points de données étaient accessibles à la même personne.

# Données non-personnelles

Les données non personnelles sont simplement des données qui ne peuvent pas être utilisées pour identifier une personne en particulier ou un groupe vulnérable.

Les données non personnelles ne sont généralement pas soumises à des exigences légales strictes en matière de protection des données. Cependant, ces données peuvent être **confidentielles ou sensibles** et PEUVENT nécessiter un stockage sécurisé, une maintenance et une mise à jour régulières, ainsi qu'une utilisation responsable.

---

**Exemple : Données Non-Personnelles**

- Données logistiques telles que les inventaires de fournitures médicales ou le nombre de véhicules de la FICR enregistrés dans un pays donné.

# Données sensibles

Les données sensibles sont des données à caractère personnel qui, si elles étaient divulguées, pourraient être utilisées pour discriminer une personne ou lui causer un préjudice (mental ou physique).

- Les données sensibles sont **spécifiques au contexte** et des données qui ne sont pas sensibles dans un pays peuvent l'être dans un autre en fonction des normes sociales et culturelles locales.
- Dans de nombreux pays, les données sensibles nécessitent un très haut degré de protection et/ou ne doivent pas être collectées, utilisées ou partagées, sauf en cas d'absolue nécessité.

---

**Exemple :**

- Les dossiers médicaux, le statut VIH, les données biométriques ou l'ADN, les convictions religieuses ou politiques, l'origine ethnique et la nationalité, ou l'orientation sexuelle et l'identité de genre.
- Un nom, par exemple, n'est généralement pas considéré comme sensible. Toutefois, dans certains endroits, certains noms de famille peuvent révéler la religion ou l'appartenance ethnique.

# Données de groupe sensibles

Les données sur les groupes sensibles sont des données qui ne peuvent pas être utilisées pour identifier des individus, mais qui peuvent être utilisées pour **identifier des groupes vulnérables**, soit seules, soit combinées à d'autres données.

Les données sensibles sur les groupes sont **spécifiques au contexte**, mais il est très important de les protéger dans les situations d'urgence. Idéalement, toute donnée de groupe sensible collectée ou utilisée devrait être soumise aux mêmes règles que les données sensibles.

**Exemple :**

- Photographie aérienne montrant l'emplacement d'une tribu indigène non contactée. Bien qu'aucun individu ne soit identifiable, l'image montre clairement une communauté vulnérable à de nombreux égards et qui, si elle tombait entre de mauvaises mains, pourrait subir des préjudices.

# Merci

Crédit : Thomas Orrell, James de France, Heather Leson

# 7 - 5 Comprendre la "base juridique" pour la collecte et de l'utilisation des données

# Qu'est-ce qu'une "base juridique" pour la collecte de données ?

Si vous envisagez de collecter des données personnelles ou sensibles, il est important de vous demander si vous êtes autorisé à le faire.

Il existe un nombre limité de raisons pour lesquelles des données personnelles et sensibles peuvent être collectées et utilisées. (parfois appelée "base légitime").

# Quelles sont les bases juridiques généralement acceptées pour la collecte de données ?

Les bases juridiques de la collecte et de l'utilisation des données sont les suivantes :

- Consentement pleinement informé et librement donné
- Intérêt public
- Intérêt légitime
- Intérêt vital
- Contrat
- Obligation légale

# Consentement pleinement informé et librement donné

Le consentement pleinement informé et librement donné est l'approche qui donne aux individus le plus de droits et de pouvoir pour décider si les données les concernant sont utilisées et partagées.

Dans les situations humanitaires, le consentement peut ne pas être la base juridique appropriée, car les personnes peuvent avoir l'impression qu'elles n'ont pas d'autre choix que de fournir leurs données (elles ne consentent donc pas librement). En outre, le fait de s'appuyer sur le consentement comme seule base juridique peut s'accompagner de difficultés administratives supplémentaires, en particulier dans les situations d'urgence. Il convient également de noter que les personnes peuvent retirer leur consentement à tout moment.

Le consentement convient mieux à la collecte de données non essentielles et dans des situations non urgentes. Voir les exemples dans le Guide pratique pour la protection des données dans le cadre de l'aide sous forme d'espèces et de bons.

# Consentement pleinement informé et librement donné (suite)

Pour que le consentement soit "pleinement informé", le collecteur de données doit clairement communiquer les éléments suivants à la personne auprès de laquelle ou sur laquelle des données sont collectées : comment et pourquoi ses données seront traitées, comment ces données seront protégées, si elles seront partagées, combien de temps elles seront conservées, les conséquences éventuelles d'un refus de fournir les données et comment répondre à toute préoccupation qu'elle pourrait avoir.

Pour que le consentement au traitement des données à caractère personnel soit "librement donné", la personne qui recueille les données doit être raisonnablement certaine que la personne qui fournit les informations n'a pas été contrainte ou forcée de les donner ; qu'elle a vraiment le choix de fournir les informations sans conséquences négatives.

# Intérêt public

Les données personnelles ou sensibles peuvent parfois être collectées et utilisées sur la base d'un traitement dans "l'intérêt public".

**Exemple : urgence de santé publique**

- Le gouvernement peut demander (et non exiger) d'une Société nationale qu'elle soutienne la collecte de données pour la situation d'urgence. Dans de nombreux pays, ce qui est considéré comme étant dans l'intérêt public doit être basé sur la loi existante. Cependant, il existe une tendance à considérer l'action humanitaire comme relevant de l'intérêt public. Il est préférable d'examiner les exigences juridiques de votre pays lorsque vous cherchez à vous appuyer sur cette base.

# Intérêt légitime

L'intérêt légitime est une activité qui soutient le(s) mandat(s) sous-jacent(s) de l'organisation. Par exemple, la collecte de fonds est nécessaire pour soutenir les opérations en cours. Il est dans l'intérêt légitime de l'organisation de collecter les données à caractère personnel des donateurs afin de recevoir les dons et de permettre les communications futures avec ces donateurs. Lorsque vous utilisez l'intérêt légitime comme base juridique, vous devez évaluer si les droits de la personne concernée peuvent l'emporter sur les intérêts de l'organisation. Un autre exemple pourrait être la collecte de données à caractère personnel lors d'un audit d'un projet afin de déterminer s'il a été une réussite et si/comment des améliorations peuvent être apportées.

# Exécution contractuelle

Les données personnelles et sensibles sont souvent collectées afin de remplir un accord.

**Exemple :**

- Il peut être demandé au personnel de fournir des informations sur son adresse, sa famille et ses proches, sa nationalité et ses données financières lorsqu'il rejoint le mouvement en tant qu'employé.
  - Il est nécessaire de collecter certaines données pour s'assurer que les membres du personnel reçoivent leur salaire, remplissant ainsi l'une des obligations contractuelles de la FICR à l'égard d'un membre du personnel.
  - D'autres données concernant les membres de la famille peuvent être nécessaires pour calculer correctement les prestations dues au titre du contrat de travail.

# Obligation légale

Parfois, une obligation légale exige que certaines données soient collectées et traitées.

---

**Exemple :**

- Pour les membres du personnel qui s'installent dans un nouveau pays pour y prendre leurs fonctions, la FICR doit collecter certaines données et les fournir au gouvernement afin de garantir l'obtention du permis de séjour (ou visa) approprié. Un gouvernement a imposé cette obligation afin d'obtenir le permis.

# Intérêt vital

Parfois, il peut être absolument nécessaire de collecter des données à caractère personnel pour aider quelqu'un. La collecte et l'utilisation de données à caractère personnel sur la base d'un intérêt vital sont généralement considérées comme appropriées lorsqu'il existe une menace relativement immédiate, qu'elle soit physique ou mentale.

**Exemple :**

- si une personne est gravement blessée, vous pourriez collecter toutes les données nécessaires (telles que les données relatives à la santé) pour aider cette personne sur la base de la protection de ses intérêts vitaux. Une fois que la situation d'urgence est passée et que la personne est physiquement et mentalement stable, vous pouvez alors vous appuyer sur d'autres bases juridiques pour le traitement de vos données à caractère personnel.

# Comment savoir quelle base juridique utiliser ?

- Il n'est pas facile de savoir quelle est la bonne base juridique à utiliser. Vous devez toujours évaluer les situations au cas par cas pour déterminer quelle est la bonne.
- Rappelez-vous que si des personnes ont besoin d'aide, le consentement ne peut être utilisé si l'aide est conditionnée à la réception de données. Il ne s'agit pas d'un consentement libre.
- Par ailleurs, quelle que soit la base juridique utilisée, les informations suivantes doivent toujours être fournies aux personnes concernées sous une forme compréhensible et accessible :
  - pourquoi les informations sont collectées;
  - à quoi elles serviront ;
  - avec qui elles seront partagées ;
  - combien de temps elles seront conservées
  - les personnes à contacter en cas de questions.
- En cas de doute, vous devez vous adresser à votre service juridique.

# Questions pour discussion

- Quels sont, selon vous, les défis à relever pour collecter et utiliser des données sur la base d'un " consentement pleinement informé et librement donné " dans un contexte d'urgence ? Quand serait-il approprié pour la FICR ou une Société nationale d'utiliser le consentement ? Quand cela pourrait-il être inapproprié ?
- Quelles responsabilités supplémentaires pensez-vous que le réseau de la FICR doit prendre en compte lors de la collecte et de l'utilisation de données sur une base autre que le consentement ?
- Si vous deviez collecter des données personnelles ou sensibles sur la base d'un intérêt légitime ou public, quels types d'informations vous efforceriez-vous de fournir aux personnes auprès desquelles vous collectez ces données ?

# Merci!

Crédit : Thomas Orrell, James de France, Heather Leson

# 7 - 6 Dans leurs baskets

**L'utilisation du "consentement" comme base pour la collecte et l'utilisation de données dans un contexte humanitaire nécessite une série de décisions. Dans un monde idéal, le personnel et les volontaires de la FICR seraient en mesure d'obtenir les données personnelles de chaque individu dont ils ont besoin sur la base d'un consentement pleinement informé et librement donné. En réalité, l'urgence et la complexité des situations d'urgence rendent cette tâche extrêmement difficile. Si la FICR et les Sociétés nationales sont souvent autorisées à utiliser des données personnelles ou sensibles sans avoir nécessairement obtenu le consentement des personnes, lorsqu'elles le font, elles doivent néanmoins réfléchir à la manière dont ces données doivent être utilisées de manière responsable et conformément aux bonnes pratiques en matière de protection des données.**

Cet exercice de jeu de rôle basé sur un scénario est conçu pour mettre en évidence certaines des complexités que la collecte et l'utilisation de données sur la base du consentement soulèvent. Il aborde également les obligations d'ouverture et de transparence concernant les données collectées et utilisées par la FICR, ainsi que les responsabilités qui incombent à la FICR en matière d'éthique et de gestion responsable des données. L'exercice s'adresse à un public intermédiaire et avancé qui a déjà une compréhension des bases sur lesquelles les données peuvent être collectées et utilisées, et des façons dont les valeurs humanitaires et les principes de protection des données se chevauchent.

- **Personnes :** 5 à 20 personnes
- **Durée :** 60 – 90 Minutes
- **Difficulté :** Intermédiaire
- **Matériel virtuel** : plate-forme de réunion virtuelle, espace de rédaction/documentation partagé
- **Matériel en personne** : Tableau, post-it, marqueurs

# Exercice : Jeu de Rôle

Une Société nationale se prépare à rencontrer un groupe important de personnes qui ont dû évacuer leurs terres et leurs maisons en raison de graves inondations. La communauté internationale et le pays hôte ont reconnu la crise et ont émis des mandats - tant au niveau international qu'au sein du pays hôte - pour soutenir les communautés qui ont été touchées. Le personnel est mobilisé pour établir des points de rencontre où il procédera à une évaluation rapide des familles qui arrivent et les enregistrera en vue d'un soutien (soutien envisagé : nourriture, abri, assistance de base en espèces par le biais d'un coupon, aide psychosociale et médicale). Les personnes qui arrivent sont profondément traumatisées, ayant perdu leur maison et leurs moyens de subsistance, ainsi que des membres de leur famille et des amis. Elles sont souvent démunies, épuisées et en état de choc.

## Rôles :

- Coordinateur de la réponse de la Société nationale - responsable de la planification et de l'établissement des points de rencontre, y compris des processus de collecte des données.
- Collecteur de données - membre du personnel ou bénévole sur le terrain qui recueillera les données.
- Adulte profondément traumatisé qui demande de l'aide
- Mineur profondément traumatisé voyageant seul et cherchant de l'aide
- D'autres personnes sont-elles nécessaires ?

## Partie 1 : planification - discussion de groupe

- Quels processus le coordinateur de la réponse doit-il mettre en place pour collecter les données - comment cela doit-il être fait ?
- Quelles sont les données à collecter ?
- Comment le collecteur de données doit-il aborder la collecte de données dans la pratique ?

## Partie 2 : collecte de données - simulation

- Simuler une première interaction entre le collecteur de données et les communautés affectées. Quels types de questions seraient posés ? À quoi ressembleraient les réponses ?
- Si le collecteur de données essayait d'obtenir un "consentement pleinement informé et librement consenti" de la part des communautés, qu'est-ce que cela impliquerait ? À quoi ressemblerait une conversation ?
- Quelle autre base pourrait être plus appropriée dans ce cas pour collecter des données ?
- Quelles sont les autres considérations à prendre en compte lors d'un entretien avec un mineur non accompagné ?

## Partie 3 : utilisation des données – groupe de discussion

- Une fois les données collectées, compte tenu de la vulnérabilité des communautés, quelles sont les responsabilités de la Société nationale pour les utiliser de manière responsable et les garder en sécurité ?
- Quelles informations doivent être fournies aux communautés affectées sur la manière dont leurs données seront utilisées ? Quel serait le meilleur moment pour leur fournir ces informations compte tenu de leur état de choc et de traumatisme ?
- En repensant maintenant au scénario, le consentement serait-il une base appropriée pour collecter des données dans ce cas ? Si oui, pourquoi ? Si non, pourquoi ?

### Bonus

Présentez la politique de protection des données de votre organisation et discutez des prochaines étapes et des exemples d'application des leçons dans votre travail. Voir le guide de la protection des données de la FICR.

### Crédit

Tom Orrell, James De France, Heather Leson

# 7 - 7 Valeurs humanitaires et protection des données

**L'utilisation responsable et la protection des données sont souvent des sujets difficiles à aborder avec des participants qui ne sont pas familiers avec les données et les risques potentiels des technologies numériques. Cet exercice ne nécessite qu'une compréhension de base des valeurs humanitaires et de ce que sont les données personnelles. L'objectif de l'exercice est de relier les principes humanitaires au travail sur les données et d'introduire les concepts clés de l'utilisation responsable et de la protection des données dans une perspective de valeurs plutôt que de légalité. Les participants peuvent prendre confiance en leur capacité à comprendre les termes et les concepts relatifs à la protection des données.**

- **Personnes :** 2 à 12 personnes
- **Durée :** 30-60 Minutes
- **Difficulté :** Facile
- **Matériel virtuel** : plate-forme de réunion virtuelle, espace de rédaction/documentation partagé
- **Matériel en personne** : Tableau, post-it, marqueurs

# Exercice

## Partie 1 : Explorer

En petits groupes (idéalement en paires), discutez :

1. Que signifie, selon vous, "protéger l'information" en tant qu'humanitaire ?
2. Qu'est-ce que cela signifie d'utiliser les données de manière "responsable" ?

Notez les idées et les questions sur un document commun.

## Partie 2 : Réviser

Discutez des réponses en groupe entier en demandant à chaque groupe de partager un point fort de leur conversation.

## Partie 3 : Discuter

Partagez les principes d'appariement (document à distribuer). En petits groupes, discutez des questions suivantes :

- Comment notre indépendance influe-t-elle sur la manière dont nous collectons, utilisons et partageons les données ?
- Devrions-nous être ouverts et transparents quant aux informations que nous recueillons auprès des communautés et à la manière dont elles sont utilisées ?
- Devons-nous collecter autant de données que possible sur les communautés que nous servons ou devons-nous en collecter le moins possible ? Comment trouver un équilibre ?
- Prendre des notes sur les idées et les questions sur un document commun.

## Partie 4 : Réfléchir

En plénière, demandez des réflexions et des questions. Donnez plus de détails sur la politique de protection des données de l'organisation.

## Bonus

Cet exercice pourrait également inclure un scénario pour la partie 2. Une composante d'apprentissage basée sur un scénario peut relier les concepts à des situations réelles auxquelles les participants sont confrontés et qui les amènent à réfléchir à ce que signifierait l'utilisation responsable et la protection des données.

### Exemple :

- Une ONG locale partenaire partage des données avec une Société nationale mais refuse de divulguer la manière dont les données ont été collectées, ce qui soulève des doutes quant à leur qualité. Quels défis ce scénario soulève-t-il ? Comment géreriez-vous la situation ?
- Vous avez recueilli des données sur les besoins médicaux d'un village. Vous avez obtenu leur consentement lors de la collecte des données pour ne les utiliser que dans le cadre de vos propres activités logistiques. Vous souhaitez maintenant partager ces données avec les autorités sanitaires locales. Pouvez-vous partager ces données ? Quelles informations devez-vous divulguer à la communauté au sujet de vos projets ?
- Vous collectez des données dans une zone de conflit très fragile. Les communautés locales hésitent à vous fournir des informations parce qu'elles craignent les répercussions si elles tombent entre de mauvaises mains. Quelles mesures pouvez-vous prendre pour vous assurer que leurs préoccupations sont prises en compte ?

Animateurs : vous pouvez commencer par diviser les groupes en paires afin qu'ils discutent d'abord du scénario entre eux avant d'encourager une discussion de groupe sur les thèmes clés.
Cet exercice devrait prendre environ 30 à 45 minutes par scénario, en fonction du nombre de participants.

### Considérations :

En examinant les exercices et les activités bonus, tenez compte des points suivants : 1) tout traitement de données doit être conforme aux principes de protection des données (c'est-à-dire avoir une ou plusieurs bases légales, des données exactes et minimisées, une communication transparente sur le traitement, des données utilisées uniquement à des fins compatibles, assurer la sécurité des données et respecter les droits des personnes concernées), et 2) nos actions, tout en aidant un gouvernement, doivent rester conformes aux principes fondamentaux, en particulier ici l'indépendance et la neutralité. Notre objectif doit être de servir une finalité humanitaire, et pas seulement d'aider ou d'être dirigé par une entité gouvernementale.

## Crédit

Tom Orrell, Arturo Garcia, Dirk Slater, Heather Leson, Melissa el Hamouch, James De France

# 7 - 8 Valeurs humanitaires et protection des données

**L'action humanitaire est ancrée dans l'empathie et la solidarité humaines. Elle a pour but de protéger la vie et d'apporter une aide aux plus vulnérables. Au sein de la communauté humanitaire, la valeur la plus importante est l'idée que les humanitaires doivent "*ne pas nuire*" dans leurs actions. De plus en plus, cela s'applique également à la manière dont les organisations humanitaires utilisent les outils numériques et les données.**

Mais que signifie "ne pas nuire" lors de la collecte, de l'analyse, de l'utilisation ou du partage des données des communautés et des individus ? Un bon point de départ consiste à réfléchir et à discuter plus en profondeur de la manière dont les valeurs et principes humanitaires et les principes de protection des données se chevauchent et se renforcent mutuellement. De cette manière, il est possible de commencer à trouver des réponses à des questions telles que ce que signifie "protéger" et utiliser les données de manière "responsable". Ce document établit un lien entre les principes fondamentaux du Mouvement de la Croix-Rouge et du Croissant-Rouge et une vue d'ensemble de certains principes clés de la protection des données.

# Principes fondamentaux du mouvement :

- Humanité - la nécessité d'agir pour prévenir et atténuer la souffrance humaine
- Impartialité - non-discrimination de quiconque
- Neutralité - ne pas prendre parti dans un conflit
- Indépendance - être autonome et résister à toute ingérence
- Volontariat - désir d'aider les autres, non motivé par un désir de gain personnel
- Unité - il ne peut y avoir qu'une seule société RCRC dans un même pays
- Universalité - la FICR est présente dans le monde entier et assume une responsabilité collective vis-à-vis de tous.

# Principes de protection des données :

- Ne collectez pas de données personnelles dont vous n'avez pas besoin - ne collectez des données susceptibles d'identifier une personne ("données personnelles") que si vous en avez réellement besoin.
- Maintenez vos ensembles de données à jour et en bon état, comme tout autre actif - les données personnelles collectées doivent être exactes, complètes et mises à jour.
- Soyez clair et documentez les raisons pour lesquelles vous collectez des données - les raisons pour lesquelles les données personnelles ont été collectées doivent être clairement énoncées et seules les données personnelles nécessaires à ces raisons doivent être collectées.
- N'utiliser les données personnelles que pour des raisons/activités spécifiques que vous avez déjà planifiées - les données personnelles collectées dans un but particulier ne doivent être utilisées que dans ce but.
- Assurez-vous que vos ensembles de données sont sûrs et sous votre contrôle - les données personnelles doivent être protégées contre tout accès, destruction, utilisation, modification ou divulgation/publication non autorisé(e).

- Soyez ouvert sur les données que vous possédez et sur ce que vous en faites - les informations sur les données personnelles collectées et sur la manière dont elles sont utilisées doivent être accessibles aux personnes concernées.
- Respecter le droit des individus à décider de la manière dont les données les concernant sont présentées et utilisées - les individus ont le droit de demander quelles informations les concernant ont été collectées, à quelles fins elles sont utilisées et ont le droit de les faire modifier, voire supprimer (si les données ont été collectées avec leur consentement).
- La FICR est responsable devant les communautés qu'elle sert, ce qui inclut la manière dont elle utilise leurs données - les personnes qui collectent et utilisent des données personnelles doivent être responsables devant les personnes dont elles utilisent les données et se conformer à toutes les lois internationales ou locales applicables.

## Références

Politique de protection des données de la FICR

# 7 - 9 De quelles données avons-nous vraiment besoin ?

**Cet exercice explore les principes qui guident l'utilisation responsable et la protection des données à l'aide d'une approche basée sur un scénario. Les deux concepts clés explorés dans le scénario sont la "*minimisation des données*" et le "*privacy by design*" (respect de la vie privée dès la conception)**

Quel est le "besoin" tout au long du cycle de vie des données ? Quelles données doivent être collectées, quelles informations doivent être fournies aux personnes concernées (et à leurs communautés), qui doit avoir accès aux données, que faut-il faire pour les sécuriser, doivent-elles être partagées et combien de temps doivent-elles être conservées avant d'être supprimées ?

- **Personnes :** 4 à 20 personnes
- **Durée :** 60 Minutes
- **Difficulté :** Intermédiaire
- **Matériel virtuel** : plate-forme de réunion virtuelle, espace de rédaction/documentation partagé
- **Matériel en personne** : Tableau, post-it, marqueurs

# EXERCICE

## Partie 1 : Explorer

En séance plénière, présenter le cycle de vie des données et résumer l'objectif du scénario : discuter de "quelles sont les données dont nous avons réellement besoin".

## Partie 2 : Réviser

Les scénarios sont plus efficaces en petits groupes de discussion. Dans les groupes, les participants doivent se présenter et désigner un preneur de notes. Passez en revue le scénario :

## Collecte de données régulière/ continue

Votre SN gère un centre de santé local. Afin de mieux prévoir les besoins de la communauté, de planifier les ressources nécessaires et d'évaluer la satisfaction à l'égard des services, vous recueillez régulièrement des données auprès des personnes qui se rendent au centre de soins. Vous avez expliqué aux familles de la communauté les raisons de cette collecte de données. Vous les avez également informées que si elles ne souhaitaient pas fournir certaines informations, elles pouvaient toujours accéder aux services de santé. Le consentement était donc la base juridique sur laquelle reposait la collecte des données, du moins en ce qui concerne les patients qui ne présentaient pas d'urgence médicale.

- Quelles données devriez-vous collecter dans le scénario ci-dessus (sachant que nous ne sommes pas des experts en médecine ou en approvisionnement) ?
- Une fois que vous avez évalué les besoins, que devriez-vous faire avec les données collectées ?

Juste avant de commencer à collecter les données, vous recevez un appel de vos collègues qui vous informent qu'une intervention en argent liquide est prévue pour la même communauté. Ils souhaitent que vous posiez quelques questions supplémentaires afin qu'ils n'aient pas à revenir voir les familles à l'avenir.

- Quelles informations supplémentaires seraient nécessaires pour l'intervention en argent liquide ?
- Quelles informations supplémentaires, le cas échéant, devriez-vous fournir aux personnes concernées au sujet des données que vous souhaitez recueillir dans le cadre du programme d'aide financière ?

Une ONG locale prend connaissance de votre travail et souhaite avoir accès à vos données afin d'éclairer ses propres interventions.

- Avez-vous besoin de partager les données ?
- Quelles informations doivent être partagées si vous décidez de le faire ?
- Quelles informations supplémentaires (ou quels choix) devriez-vous fournir aux personnes avant le partage ?

Un nouveau membre du personnel informatique vous informe que la base de données des données à caractère personnel peut être consultée par n'importe qui au sein des SN, et qu'elle est en outre hébergée sur un serveur cloud non protégé.

- Qui a besoin d'accéder aux données ?
- Que faut-il faire pour s'assurer qu'elles sont stockées en toute sécurité ?

Dans un contexte positif, le gouvernement local a achevé la construction d'un nouvel hôpital et a obtenu le financement nécessaire pour fournir des soins de santé à long terme à la communauté. Votre SN peut fermer la clinique et se concentrer sur d'autres initiatives.

- Quelles sont les données à conserver ?
- Pendant combien de temps et sous quelle forme doivent-elles être conservées ?
- Pouvons-nous utiliser ces données à d'autres fins ?

## Partie 3 : Discuter

En plénière, demandez des réflexions et des questions. Donnez plus de détails sur la politique de protection des données de l'organisation. Voir la politique de protection des données de la FICR.

### Bonus

Il s'agit d'un court exercice pour discuter des concepts de haut niveau. Si l'équipe dispose de plus de temps, demandez aux participants de partager des exemples tirés directement de leur travail et liés aux deux concepts de "minimisation des données" et de "privacy by design" (prise en compte du respect de la vie privée dès la conception).

### Crédit

Tom Orrell, James De France

# 7 - 10 Que *pouvons*-nous faire VS que *devrions*-nous faire ?

**Pour comprendre ce que signifie l'utilisation responsable et la protection des données dans un contexte humanitaire, il faut être capable de reconnaître la différence entre les dilemmes éthiques (bonnes pratiques en matière de données responsables) et les questions juridiques (protection des données). Cet exercice est conçu pour décomposer ces concepts en un contenu plus facile à comprendre en recadrant les exigences de protection des données et les dilemmes éthiques comme "ce que nous POUVONS faire" (exigences de protection des données) et "ce que nous DEVONS faire" (pratiques responsables en matière de données).**

Cet exercice s'adresse principalement aux participants qui ont une connaissance et une compréhension limitées des données responsables et de la protection des données et qui souhaitent élargir leurs connaissances. À la fin de l'exercice, les participants devraient être en mesure d'identifier les différences entre les exigences en matière de protection des données et les bonnes pratiques en matière de données responsables, et ce que cela signifie pour la manière dont ils devraient aborder des situations particulières.

- **Personnes :** 4 à 16 personnes
- **Durée :** 60 Minutes
- **Difficulté :** Facile
- **Matériel virtuel** : plate-forme de réunion virtuelle, espace de rédaction/documentation partagé
- **Matériel en personne** : Tableau, post-it, marqueurs

# Exercice

## Partie 1 :

En petits groupes (idéalement par deux), discutez : que signifient pour vous la protection et l'utilisation responsable des données ? Comment cela s'applique-t-il à notre travail ?

Notez les idées et les questions sur un document commun.

## Partie 2 :

Examinez les scénarios et discutez-en : "Que **pouvons**-nous faire ? et que **devrions**-nous faire ? Chaque groupe doit essayer de réaliser deux scénarios.

Scénario 1 : Un ami travaillant dans une organisation partenaire vous demande des données que vos collègues ont récemment recueillies sur les cas de VIH dans une localité donnée. Ils prévoient d'offrir un soutien médical/psychosocial supplémentaire à la communauté et ont besoin de savoir où concentrer leurs activités.

Pouvez-vous partager les données ? Le partage serait-il conforme aux exigences en matière de protection des données ? Dans l'affirmative, devriez-vous partager les données ? Pourquoi ou pourquoi pas ? Si vous décidez de partager les données, quelles sont les considérations à prendre en compte avant de fournir les informations ? Que se passerait-il s'il existait un risque particulier de violence ou de stigmatisation à l'égard des personnes séropositives au sein de la communauté ? Et si votre ami travaillait pour le gouvernement ? Et, même si nous supprimons les données d'identification, le partage présente-t-il encore des risques ?

- Vers qui vous tourneriez-vous pour savoir ce que vous pouvez faire ?
- Que devrions-nous faire ? Même si les règles le permettent, y a-t-il d'autres raisons de ne pas partager ?
- Que ne devrions-nous pas faire ? Et pourquoi ?

Scénario 2 : Vous avez récemment collecté des données auprès d'une communauté locale dans le cadre d'une situation d'urgence ; ces données contiennent des noms, des adresses et d'autres informations identifiables. Votre tablette/ordinateur portable n'ayant plus de batterie, vous avez effectué une sauvegarde rapide sur une clé USB sans protéger les données de quelque manière que ce soit (pas de mot de passe ni de cryptage). De retour au bureau, vous vous rendez compte que vous avez perdu la clé USB. Que faites-vous ? Quelles mesures pourriez-vous prendre avant de collecter des données pour vous assurer que, même si vous perdiez votre disque de sauvegarde, les données seraient toujours en sécurité ?

- Que pouvons-nous faire ?
- Que devrions-nous faire ?
- Que ne devrions-nous pas faire ?

Scénario 3 : Votre bureau est contacté par une grande entreprise technologique qui propose de vous aider à gérer les données de votre bureau gratuitement en cas d'urgence. Devriez-vous accepter cette offre ?

(Options : L'entreprise technologique #1 a une longue histoire de contribution aux urgences humanitaires et d'actions caritatives ; l'entreprise technologique #2 a d'importants contrats avec des gouvernements et d'autres entreprises qui pourraient être considérés comme ne respectant pas la vie privée ou d'autres droits de l'homme).

- Que pouvons-nous faire ?
- Que devrions-nous faire ?
- Que ne devrions-nous pas faire ?

## Partie 3 :

Discutez des résultats en séance plénière. Demandez-leur quels autres dilemmes éthiques ils devraient envisager.

### Bonus

Passez en revue la politique de protection des données de votre organisation avec les participants. Invitez votre responsable informatique ou votre responsable de la sécurité à parler des risques numériques et aux données après l'exercice de mise en situation. Cela pourrait fournir un contexte réel au travail de vos Sociétés nationales.

### Ressource

Dilemmes numériques
Politique de protection des données de la FICR

### Crédit

Tom Orrell, Heather Leson

# 7 - 11 Le cauchemar de la protection des données

**Lequel de ces scénarios pourrait vous empêcher de dormir ?**

- **Personnes :** 4 à 12 personnes
- **Durée :** 60 Minutes
- **Difficulté :** Facile
- **Matériel virtuel** : plate-forme de réunion virtuelle, espace de rédaction/documentation partagé
- **Matériel en personne** : Tableau, post-it, marqueurs

## Instruction :

Répartissez les participants en petits groupes et demandez-leur si l'un des éléments suivants pourrait les empêcher de dormir. Après avoir identifié les cauchemars potentiels, ramenez-les en grand groupe pour qu'ils parlent des politiques de protection des données de leur organisation.

# Exercice

## Partie 1 : Explorer

Répartissez les participants en petits groupes et demandez-leur si l'une des situations suivantes pourrait les empêcher de dormir :

1. Nous n'avons pas obtenu le consentement
2. Nous n'avons pas de procédures adéquates de stockage des données
3. De temps en temps, l'un de nos ordinateurs portables/appareils disparaît.
4. Nous n'avons pas sauvegardé nos données critiques
5. Nous n'avons pas décelé de biais dans nos données
6. Nous pourrions avoir un accès non autorisé aux données
7. Nous ne savons pas exactement quelles données peuvent être sensibles
8. Nous avons partagé/posté des données personnelles (informations identifiables) sans nous en rendre compte.
9. Des personnes ont refusé que leurs données soient utilisées, mais nous les avons quand même utilisées.
10. Nos politiques en matière de données ne sont pas assez solides

Posez la question : Y a-t-il d'autres scénarios qui pourraient vous empêcher de dormir ?

## Partie 2 : Discuter

Une fois qu'ils ont identifié les cauchemars potentiels, ramenez-les en grand groupe pour parler des politiques de protection des données dans leurs organisations. Partagez la politique de protection des données de votre organisation. Abordez toutes les questions en suspens qui pourraient nécessiter une résolution avec votre équipe. Cet exercice peut également être utilisé dans le cadre de la planification de la transformation numérique afin d'identifier les besoins de l'organisation et de l'équipe. Voir - digital.ifrc.org.

## Crédit

Dirk Slater

# 7 - 12 Le partageriez-vous ?

**Le partage responsable des données peut être difficile à mettre en œuvre. Alors que le partage d'informations est d'une importance vitale pour le travail d'urgence et humanitaire, il y a souvent des hésitations et des incertitudes sur ce qui doit ou ne doit pas être partagé, en gardant à l'esprit les besoins de protection des données. Cet exercice est conçu pour aider les participants à mieux comprendre les bases de la protection et du partage des données et comment elles se recoupent. La session a été inspirée par le travail entrepris par une Société nationale pour former le personnel de l'Unité d'intervention d'urgence (UIU) avant le déploiement.**

La première partie de l'exercice vise à donner aux participants une compréhension plus approfondie de l'utilisation responsable des données, de la protection des données et du partage des données en s'appuyant sur la perception qu'ont les individus des informations les concernant qu'ils seraient ou ne seraient pas prêts à partager. La deuxième phase consiste en des discussions de groupe basées sur des scénarios qui reproduisent des exemples humanitaires réels dans lesquels des questions de partage de données se posent. Ces scénarios peuvent être proposés par les participants eux-mêmes dans le cadre de l'exercice, ou introduits par l'animateur si une question spécifique doit être abordée.

- **Personnes :** 4 à 12 personnes
- **Durée :** 60 Minutes
- **Difficulté :** Intermédiaire
- **Matériel virtuel** : plate-forme de réunion virtuelle, espace de rédaction/documentation partagé
- **Matériel en personne** : Tableau, post-it, marqueurs

# Exercice

## Partie 1 : Le partageriez-vous ? 30mins

Répartissez les participants en petits groupes de quatre personnes maximum et demandez-leur de discuter et de répondre à chacune des affirmations (ci-dessous). Chaque individu doit répondre aux affirmations et les réponses doivent être basées sur les préférences individuelles. Cette partie devrait prendre environ 10 minutes. Le contenu peut être placé dans un tableau ou un diagramme (selon que l'événement est virtuel ou en personne). Les participants sont encouragés à partager des exemples de leur vie personnelle et professionnelle. Aux fins de cet exercice, veuillez-vous concentrer sur les données à caractère personnel (c'est-à-dire les données qui, seules ou avec d'autres données, peuvent être utilisées pour identifier une personne physique).

| Déclaration : | Réponses : |
|---|---|
| **Il est utile de partager ce type de données :** | |
| **Je veux partager ce type de données :** | |
| **Je ne veux pas (ou je ne vais pas) partager ce type de données :** | |
| **Je ne veux pas (ou je ne vais pas) partager ce type de données :** | |
| **Je n'ai pas d'autre choix que de partager ces données :** | |

Une fois le groupe réuni, demandez aux participants d'examiner les réponses des uns et des autres et de faire des commentaires sur les similitudes/différences. Vous pouvez demander aux participants comment leurs réponses pourraient changer s'ils vivaient dans un contexte de conflit ou de catastrophe. Cette partie de l'exercice devrait prendre environ 20 minutes.

## Partie 2 : Apprentissage par scénarios (45-60 mins)

Pour cette partie de la session, des scénarios ont été préparés (ci-dessous). Vous pouvez également créer votre propre scénario spécifique à votre organisation. Il est recommandé de le faire suffisamment à l'avance avec un coéquipier.

**Exemple de scénario 1 : Données de la branche**
Dans le cadre d'une précédente opération de secours, votre branche de SN a recueilli des données sur les bénéficiaires qui ont demandé des soins médicaux pour une maladie infectieuse. Les données collectées sont stockées dans un fichier Excel contenant les champs suivants : Numéro d'identification (qui n'est pas un numéro d'identification officiel, mais un numéro attribué par votre branche de SN), état de santé, âge, région et village, nombre d'enfants dans le foyer, éducation et numéro de téléphone (si la personne en a un). Le service de santé du gouvernement local vous a demandé de fournir les données sur les personnes. Quel type de données partagerez-vous ou ne partagerez-vous pas ? Pourquoi ? Quels sont les avantages (ou les risques) du partage de ces données ?

**Example Scenario 2 : Données relatives à l'assistance en espèces et en bons d'achat**
Au lendemain d'un tremblement de terre, une Société nationale tente d'identifier les personnes qui ont perdu leur logement, car elles peuvent prétendre à une aide en espèces ou sous forme de bons. Une association du village le plus touché propose de partager une liste de personnes actuellement sans abri à cause du tremblement de terre. Quelles informations demanderiez-vous à l'association du village de partager avec vous ? Quels types de questions pensez-vous que cela pourrait soulever - par exemple, comment l'association elle-même a recueilli les données, quel est le degré de fiabilité de ces données, etc. Quelles mesures pourriez-vous prendre pour atténuer ces problèmes ?

La session doit commencer par la définition par le groupe d'une liste de types de données susceptibles d'être partagées au cours du scénario. Ils doivent également dresser une liste des types de données qui ne doivent pas être partagées. Cela permet de s'assurer que les participants partagent le même cheminement tout au long des scénarios. (Remarque : il se peut que toutes les questions ne soient pas applicables ou qu'il manque des informations). Prenez des notes sur les idées ou les questions dans un document commun.

| Question | Réponse |
|---|---|
| **Qui a besoin des données ? Quel est leur rôle ? Quel est l'objectif du partage ?** | |

| Question | Réponse |
|---|---|
| **D'où viennent les données ? Qui y a accès ? Est-il possible de publier ouvertement les données ?** | |
| **Qui peut partager les données ?** | |
| **Existe-t-il un enregistrement du partage des données dans le système et/ou pour l'organisation ?** | |
| **Existe-t-il un accord de partage des données/un protocole d'accord avec la partie avec laquelle les données ont été partagées ?** | |
| **Si des données à caractère personnel sont partagées, quels sont les autres éléments à prendre en compte ? Pouvez-vous agréger, pseudonymiser ou anonymiser les données ? Pouvez-vous/devez-vous supprimer certains champs ?** | |
| **Existe-t-il des conditions de service et une licence pour les données ?** | |
| **Quelles sont les capacités d'importation, d'exportation et d'échange de données requises et dans quel format ?** | |

## Bonus

Optionnel : Créer un nouveau scénario : Les équipes peuvent créer leur propre scénario pour cet exercice. Il est recommandé de le faire bien avant la session avec des collègues.

- Faire parler les participants de problèmes réels de partage de données. La méthode utilise des scénarios comme exemples : soit du monde réel, soit illustratifs. La composante interactive permet de visualiser les étapes et les actions pour "simuler" la prise de décision. Donnez-leur un exemple. Souvent, il est préférable de demander à un membre de l'équipe de préparer cet exemple avant la session.
- OU/ Engagez une conversation sur les "étapes de mise en œuvre" et les "exigences" en matière de partage des données.

## Crédit

Dirk Slater, Heather Leson, Arturo Garcia, Melissa el Hamouch, Tom Orrell, James De France

# 7 - 13 Checklist de l'hygiène des données

Voici les catégories de données à prendre en compte lors de l'évaluation des besoins en matière de protection des données.

| Catégories de données | Notes |
|---|---|
| **Informations d'identité de base telles que le nom, la localisation (adresse, localité, etc.) et les numéros de carte d'identité** | |
| **Données web telles que la localisation, l'adresse IP, les données des cookies et les tags RFID** | |
| **Données de santé et génétiques** | |
| **Données biométriques** | |
| **Donnée raciale ou ethnique** | |
| **Opinions politiques** | |
| **Orientation sexuel** | |

La deuxième partie de cette analyse consiste à faire correspondre les catégories de données aux termes formels ci-dessous :

| Catégories de données | Jeu de données | Notes |
|---|---|---|
| **Données non-personnelles** | E.G. données logistiques telles que le nombre de véhicules dont dispose une société nationale | |
| | Etc | |
| **Données personnelles** | E.G. Noms et adresses des familles bénéficiant d'un soutien dans la communauté | |
| | Etc | |
| **Données sensibles** | E.G. Données biométriques, données relatives à la santé, données raciales ou ethniques | |
| | Etc | |
| **Données de groupe sensibles** | E.G. Photographies/images satellites à partir desquelles des groupes de personnes vulnérables peuvent être identifiés - par exemple, camps de réfugiés, villages de populations indigènes. | |
| | | |

# 7 - 14 La roue de l'infortune des données

**La roue de l'infortune des données peut contribuer à susciter la discussion tout en mettant en évidence les questions de protection des données et de maîtrise des données. Utilisez-la comme introduction interactive à la politique de protection des données de l'organisation.**

- **Personnes :** 2 à 24 personnes
- **Durée :** 30 Minutes
- **Difficulté :** Moyen

# Fabrication de la roue

Temps de fabrication : Pas plus de 2 heures

## Fournitures

- 8 couleurs de grand papier cartonné
- Ciseaux
- Bâton de colle
- Support de rotation

Mesures : 50 × 50cm

17 sections, environ 3-4 par quartier

## Identifier

Identifiez 17 catégories. Les 17 catégories ci-dessous sont mises en évidence à titre d'exemple, mais vous êtes libre de les choisir et de les remixer en fonction du contexte de vos participants.

1. Consentement
2. Stockage des données
3. Perte de données
4. ordinateur portable/appareil volé
5. Sauvegardes
6. Biais des données
7. Plan d'archivage
8. Accès non autorisé aux données
9. Comprendre quelles sont les données sensibles
10. Lassitude à l'égard des enquêtes
11. Existe-t-il des normes externes (par exemple l'IITA) que nous devrions adopter ?
12. Données personnelles (informations identifiables)
13. Suivi des personnes à l'aide de données
14. Personne concernée refusant l'utilisation des données ou s'y opposant
15. Données erronées/fausses
16. Pas de données
17. Demande de données du gouvernement

# Exercice

- Ayez toutes les catégories sélectionnées
- Lors de la session, ouvrez la discussion en demandant à quelqu'un de faire tourner la roue pour déterminer le sujet. Demandez aux participants s'ils ont une histoire ou une question à ce sujet. (Faites quelques tours pour lancer la conversation, puis passez à d'autres sujets clés qui, selon eux, manquent ou sont des priorités absolues, qu'il s'agisse de lacunes ou d'opportunités).

Après la session, laissez-la dans le couloir (ou sur une version numérique) avec quelques notes demandant aux gens de partager anonymement leurs histoires de données ou des questions de données responsables qu'ils considèrent comme une priorité.


## Ressources :

- How to Build a Wheel of Fortune Wheel (with Pictures) – wikiHow
- How To Make Pinwheels – Paper Source
- How We Made Wheel of Fortune From Cardboard – PLAYTIVITIES

## Crédit

Heather Leson

# 7 - 15 Simulation de données PMER

**Dans cette session, nous utiliserons un exemple d'urgence pour guider les conversations sur les risques, les rôles, les décisions, les lacunes et les besoins de preuves pour notre travail. Cette séance doit être associée à Renforcer les équipes et les projets de données (3) (Module 3).**

# Scénario : Déportation massive de travailleurs migrants du Randowsa

Le pays Randowsa dépend des travailleurs migrants réguliers et irréguliers. Le gouvernement du Randowsa a mis en place des politiques visant à empêcher la migration irrégulière et les travailleurs de travailler sans les documents nécessaires.

En raison de l'instabilité politique récente, le gouvernement du Randowsa applique sa politique à l'égard des travailleurs migrants en situation irrégulière, ce qui fait craindre à ces derniers d'être arrêtés ou expulsés. Au cours des sept derniers jours, plus de 400 000 personnes ont quitté le pays dans la peur - beaucoup volontairement, d'autres ont été expulsées, et les entreprises sont condamnées à de lourdes amendes s'il s'avère qu'elles ont employé des travailleurs en situation irrégulière. De nombreux migrants ont traversé la frontière pour se rendre à Dakandka. Un camp se développe et le RCRC intensifie ses activités pour soutenir les mandats complexes.

PMER a été engagé pour soutenir les efforts des différents secteurs sur la conception de l'enquête avec les Sociétés nationales ainsi que pour planifier le processus de collecte mobile de données. Vous dirigez un projet de collecte mobile de données impliquant plusieurs Sociétés nationales. Le traitement des données a lieu dans le pays ainsi qu'à distance par l'intermédiaire des équipes de soutien à la gestion de l'information (SIMS) des Sociétés nationales et d'une tierce partie (un groupe de recherche). Des enquêtes régulières sur la santé, les abris, l'hygiène et les abus sexuels sont menées afin de recueillir des informations complètes, accompagnées d'entretiens avec des informateurs clés. Chacune de ces enquêtes est différente et menée par des Sociétés nationales différentes. Vous avez récemment réalisé un examen des différentes enquêtes.
Le rapport a suscité beaucoup d'intérêt. La plupart des partenaires sont préoccupés par l'aggravation de la situation, même si certains doutent des chiffres. Le gouvernement est particulièrement critique à l'égard des chiffres.

# Exercice

Chaque équipe de 3 à 4 personnes dispose de 30 minutes pour prendre des décisions et répondre aux questions clés.

## Questions clés

- Quels sont les risques, les lacunes et les besoins ? Comment allez-vous protéger les flux de données pour protéger les personnes les plus vulnérables ?
- Quelles sont les étapes, les rôles et les décisions à prendre dans le cadre de cette initiative ?
- Quel est l'ensemble minimal de données qui peut être partagé et avec qui ? Pourquoi ?

## Vos points de décision

Vous avez reçu une demande de données pour le dernier tour de la part des partenaires suivants. Devrions-nous partager les données avec cet acteur ? Et à quel stade du processus le feriez-vous ? Comment allez-vous gérer/partager les données avec des fournisseurs externes ?

1. L'unité PMER de la FICR souhaite examiner les données pour voir s'il est possible de créer un graphique convaincant à partir des données pour accompagner un communiqué de presse qui sera publié sur l'aggravation de la situation. Elle a demandé l'ensemble des données.
2. Le bureau du gouverneur et les régions les plus touchées identifiées dans le dernier cycle de l'enquête disent qu'ils aimeraient prendre des mesures et ont besoin des données.
3. Le responsable de projet des donateurs aimerait voir les données.
4. L'un des informateurs clés/membres de la communauté qui a participé à l'enquête estime que votre rapport n'a pas rendu compte avec précision du problème dans sa région.

## Crédit

IFRC Migration team, Heather Leson, Miki Tsukamoto

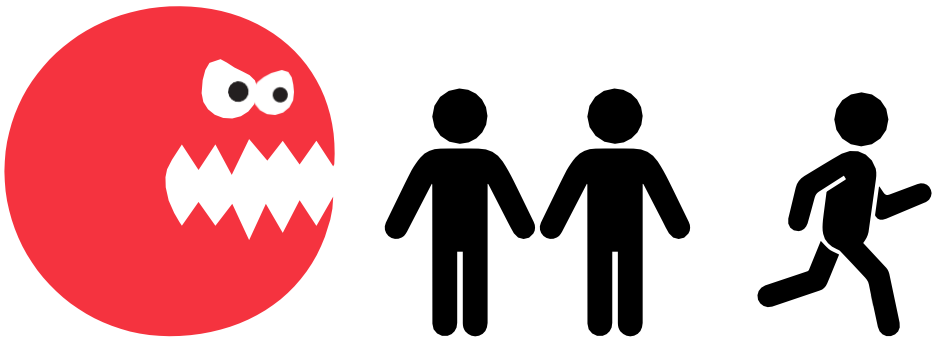
# 7 - 16 Les gens avant les données

(polycopié)

## Crédit

Jennifer Chan

## Le passé

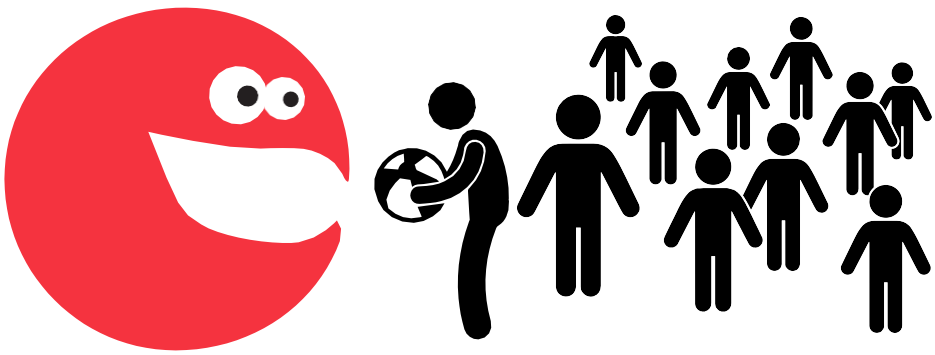


Collecte de données

## Peut-être maintenant

Métriques de données **Les gens et les données apprennent à se parler**

## Le Futur



Métriques de données **Les gens exploitent les données dans un but et avec un sens**

# 7 - 17 Suivi de la campagne contre la polio en Syrie

## Scénario

**Le Croissant-Rouge du Qatar participe à une campagne de lutte contre la polio en Syrie en tant que tierce partie. Cette campagne est soutenue par l'Organisation mondiale de la santé (OMS).**

En examinant le scénario présenté ci-dessous, veuillez prendre en considération les questions suivantes concernant les mesures de protection (notamment la fourniture d'informations) et de responsabilité en matière de données qui devraient être envisagées tout au long de la campagne.

- Quels sont les risques, les lacunes et les besoins pour soutenir la campagne ? Comment allez-vous sauvegarder les flux de données pour protéger les personnes les plus vulnérables ?
- Quels sont les étapes, les rôles et les décisions de cette campagne ?
- Quel est l'ensemble minimal de données qui peut être partagé et avec qui ? Pourquoi, et quelles sont les questions à prendre en compte avant le partage ?
- Devons-nous nous appuyer sur le consentement pour la collecte des données et, dans l'affirmative, comment l'obtenir ?
- Comment les données doivent-elles être stockées et, si nécessaire, transmises ?
- Toute autre question relative à la protection des données ou aux données responsables ?

# Le travail de l'équipe se déroule comme suit :

1. Préparer les formulaires de collecte de données sur papier. (Remarque : veillez à définir clairement quelles données peuvent et doivent être collectées. Respectez les directives applicables en matière de protection des données (lois et/ou politiques).
2. Saisir les champs de données dans la plate-forme de collecte de données (DHIS2).
3. Un moniteur collecte les données auprès des centres et des communautés.
4. Un superviseur, chargé de diriger une équipe de moniteurs dans une zone de rapport définie, fournit des mises à jour au superviseur de district.
5. Le superviseur de district peut ensuite fournir des rapports agrégés sur la campagne.
6. Les rapporteurs analysent les données collectées et extraient des rapports prédéfinis pour présenter les indicateurs de vaccination, qui sont ensuite communiqués à l'OMS et au groupe spécial pour la vaccination.

La surveillance par des tiers s'effectue en trois étapes principales au cours de la campagne :

1. Pré-campagne (visite des centres et vérification de l'état de préparation des centres, des vaccins et des équipes de vaccination).
2. Intra-campagne (pendant la campagne, les contrôleurs vérifient les progrès de la vaccination dans les centres et se rendent dans les foyers et sur les marchés pour contrôler la couverture vaccinale).
3. Post-campagne (après la campagne, les contrôleurs se rendent dans les foyers et sur les marchés pour recueillir des données sur la couverture de la campagne).

Nous visitons généralement les centres de vaccination un ou deux jours avant la campagne pour vérifier la préparation du centre et de l'équipe et nous assurer que tout se déroule comme prévu.

Nous choisissons également des personnes au hasard sur les marchés et leur demandons si elles savent quelque chose sur la campagne et le vaccin et où elles en ont entendu parler.

# Contexte

En mars 2016, lors de la phase de pré-campagne, un organisme indépendant pour la zone assiégée de Homs a analysé les données et a constaté que les flacons de vaccin étaient défectueux. Nous avons envoyé des photos des flacons à l'OMS, qui a décidé de mettre fin à la campagne jusqu'à ce qu'elle dispose d'un nouveau vaccin.

L'importance de la phase de pré-campagne ne se limite pas à vérifier le vaccin et l'équipe de vaccination, il s'agit également de recueillir des informations dans un endroit ciblé, afin de mesurer les connaissances de la population sur la campagne et le vaccin.

En août 2017, les indicateurs de pré-campagne ont montré une diminution des connaissances sur la campagne. 40 % des personnes n'étaient pas au courant de la campagne qui était censée commencer le lendemain ! La campagne a donc été reportée d'une semaine.

## Crédit

Hesham Othman Hassan et Nami Ghadri, Croissant-Rouge du Qatar

# 7 - 18 Monologues de données

**Un "monologue de données" est un résumé d'une "leçon de projet de données" ou d'un "échec de données". Les personnes fournissent le scénario, les problèmes, les mesures d'atténuation et les résultats.**

### DES DONNÉES RESPONSABLES, C'EST :

"La responsabilité des données dans l'action humanitaire est la gestion sûre, éthique et efficace des données personnelles et non personnelles en vue d'une réponse opérationnelle."

**Protection des données :**

La protection des données est un ensemble de principes et de pratiques mis en place pour garantir que les données personnelles collectées et utilisées par la Fédération ou en son nom sont exactes et pertinentes, et que les données personnelles ne sont pas utilisées à mauvais escient, perdues, corrompues ou consultées et partagées de manière inappropriée. (Politique de la FICR sur la protection des données personnelles)

**La protection des données personnelles des individus fait partie intégrante de la protection de leur vie, de leur intégrité et de leur dignité. C'est pourquoi la protection des données personnelles est d'une importance fondamentale pour les organisations humanitaires. (Brussels Privacy Hub/Manuel du CICR sur la protection des données, CICR, 2017)**

# Objectifs de la session

Cette session d'une heure à une heure et demie vous aidera, vous et votre équipe, à parler de l'utilisation responsable des données et des lignes directrices en matière de protection des données. Objectifs de cette session :

- Développer les défenseurs et l'expertise pour soutenir l'utilisation responsable des données dans la réponse humanitaire.
- Construire un langage commun autour de l'utilisation responsable des données.
- Favoriser la protection des données et la connaissance des données responsables pour le CRCR.
- Introduire des politiques de protection des données, obtenir des commentaires sur les besoins de formation.
- Introduire le Manuel sur la protection des données dans l'action humanitaire internationale (2e édition, publication du Privacy Hub CICR/Bruxelles).

- **Personnes :** 12 à 24personnes
- **Durée :** 90 Minutes
- **Difficulté :** Facile
- **Matériel virtuel** : plate-forme de réunion virtuelle, espace de rédaction/documentation partagé
- **Matériel en personne** : Tableau, post-it, marqueurs
- **Préparation :** Demandez à 3 ou 4 personnes d'aider à guider la session. Expliquez-leur les objectifs, les formats et les résultats de la réunion. Attribuez-leur différentes parties de la pièce.

- Disposer les chaises ou les bureaux en cercle ou en petits groupes/utiliser des sessions virtuelles en petits groupes
- Placer des panneaux d'accueil sur la porte / disposer d'un espace de documentation partagé
- Chaque groupe aura besoin de :
- Un animateur désigné
- Un ou des preneur(s) de notes dédié(s)
- Des exemples de scénarios en format papier et numérique
- Accueillez les participants dès leur arrivée. Demander aux participants de ranger leurs ordinateurs portables et leurs téléphones. Commencez et arrêtez à l'heure.

## Partager de manière saine

- Il serait souhaitable d'encourager la création d'un lieu sûr en utilisant les "règles de Chatham House" - se concentrer sur le sujet et les leçons plutôt que sur les personnes/organisation/division.
- "règle ou principe selon lequel les informations divulguées au cours d'une réunion peuvent être rapportées par les personnes présentes, mais la source de ces informations ne doit pas être explicitement ou implicitement mentionnée."

**Fournir aux participants le résumé suivant** : L'objectif de la session est de partager et d'informer les participants sur l'attention croissante accordée aux pratiques responsables en matière de données, y compris le Manuel du CICR sur la protection des données dans l'action humanitaire, la politique de protection des données de la FICR, l'IITA et d'autres sujets connexes.

**Contexte pour la session :** le traitement plus facile et plus rapide de quantités croissantes de données à caractère personnel a suscité des préoccupations éthiques quant à l'équilibre entre la transparence et le libre accès à l'information, d'une part, et les questions de confidentialité et l'intrusion éventuelle dans la sphère privée des individus, d'autre part. D'un point de vue organisationnel, cela nécessite de prêter attention aux pratiques responsables en matière de données, à la planification de la protection des données et à la maîtrise générale des données, à la transparence et à la confidentialité. Ainsi, des organisations telles que la FICR, le CICR, le CRS et Oxfam ont publié ou travaillent sur des politiques en matière de données. Cette session partagera les principales leçons et considérations sur ce sujet.

## Qu'est-ce qu'un monologue Data ?

- Un "monologue de données" est un résumé d'une "leçon de projet de données" ou d'un "échec de données". Les participants fournissent le scénario, les problèmes, les mesures d'atténuation et les résultats.
- Le groupe partagera quelques histoires de projets basés sur des données, sélectionnera le meilleur exemple d'un problème complexe, puis préparera un "pitch" pour illustrer quelques questions/observations fondamentales.

- Les "monologues de données" peuvent comporter des noms de personnes ou d'organisations supprimés. Les règles de Chatham House s'appliquent (c'est-à-dire que nous demanderons aux participants de ne pas partager leurs données tant qu'ils n'en auront pas reçu l'autorisation). Les participants décriront le problème, les risques, les mesures d'atténuation prises, les résultats et ce qui pourrait être amélioré.

## Partie 1 : Monologues de données : Discussion en petits groupes (20 minutes)

- Répartir en groupes de 4 à 5 personnes
- Partager les histoires de données pendant 20 minutes
- Chaque personne partage un exemple de problèmes/scénarios qu'elle a rencontrés.
- Essayez d'utiliser des exemples personnels/ organisationnels, plutôt que des exemples de tiers.

## Partie 2 : Monologues de données (40 minutes)

- Choisissez un des exemples à partager en plénière, y compris ce qui s'est passé, les résultats et les mesures d'atténuation.
- L'animateur du groupe consigne les questions/concepts fondamentaux sur un tableau
- Retour en plénière
- Le "pitch" du monologue de données doit ressembler à un exposé "Pecha Kucha" ou "ignite" : résumé, leçons et prochaines étapes. Un monologue ne doit pas durer plus de cinq minutes. Il y aura 4 ou 5 présentations.

## Partie 3 : Ajout de la protection des données et de l'utilisation responsable des données (15 minutes)

- Au cours des discussions, les participants aborderont inévitablement les questions du consentement, de la violation des données, du partage des données, du stockage des données, de la protection des données, etc.
- Préparer des diapositives pour illustrer ces termes clés.
- Fournir des ressources pour en savoir plus sur la mise en œuvre de la protection des données et l'utilisation responsable des données dans le travail humanitaire.

## Partie 4 : Conclure (10 minutes)

- Terminez par un rapide tour de table en demandant aux participants de partager un "aha" ou un apprentissage tiré des monologues avant de conclure.

## Après l'événement :

- Rassembler les questions critiques des groupes.
- L'exemple "Monologues de données" ne doit être réutilisé que s'il est autorisé.

- Envoyer des notes de remerciement aux assistants et aux participants.

## Ressources

Heather Leson et le réseau PMER, politique de protection des données de la FICR, orientations opérationnelles de l'IASC sur la responsabilité en matière de données.