

Cycle de formation à la gestion responsable des données

Ce matériel de formation est protégé par une licence internationale Creative Commons Attribution-ShareAlike 4.0.



Session 3

La gestion responsable des données en action - partie 1

Introduction à la session 3

Et maintenant...



1/ Les différentes dimensions de la gestion responsable des données



2/ Focus sur la protection des données



3/ Les concepts de la gestion responsable des données en action- partie 1



4/ Les concepts de la gestion responsable des données en action- partie 2



5/ Découvrir comment les enjeux actuels s'appliquent à vous

Agenda de la session 3

- Introduction à la session d'aujourd'hui
- Vue d'ensemble des étapes de "production" du cycle des données
- 2 focus sur des sujets de grand intérêt
 - Collecte sur mobile et protection des données
 - Sécurisez vos données et vos outils
- Travail en groupe
- Conclusion

Travail sur :

1. Minimisation des données
2. Plan d'analyse
3. Formation des enquêteurs
4. Identifiants uniques
5. Travailler avec les partenaires locaux
6. Registre des données

L'élaboration de ce matériel de formation est soutenue par le Ministère français de l'Europe et des Affaires étrangères (MEAE-CDCS). Néanmoins, les idées et opinions présentées dans cette formation ne représentent pas nécessairement celles du MEAE-CDCS.

Questions & réponses

Vous trouverez toutes les questions et réponses de la dernière session, y compris celles auxquelles nous n'avons pas eu le temps de répondre en direct, dans le fidèle compagnon de la session 2.

Avez-vous des questions supplémentaires sur la dernière session ?





Quiz

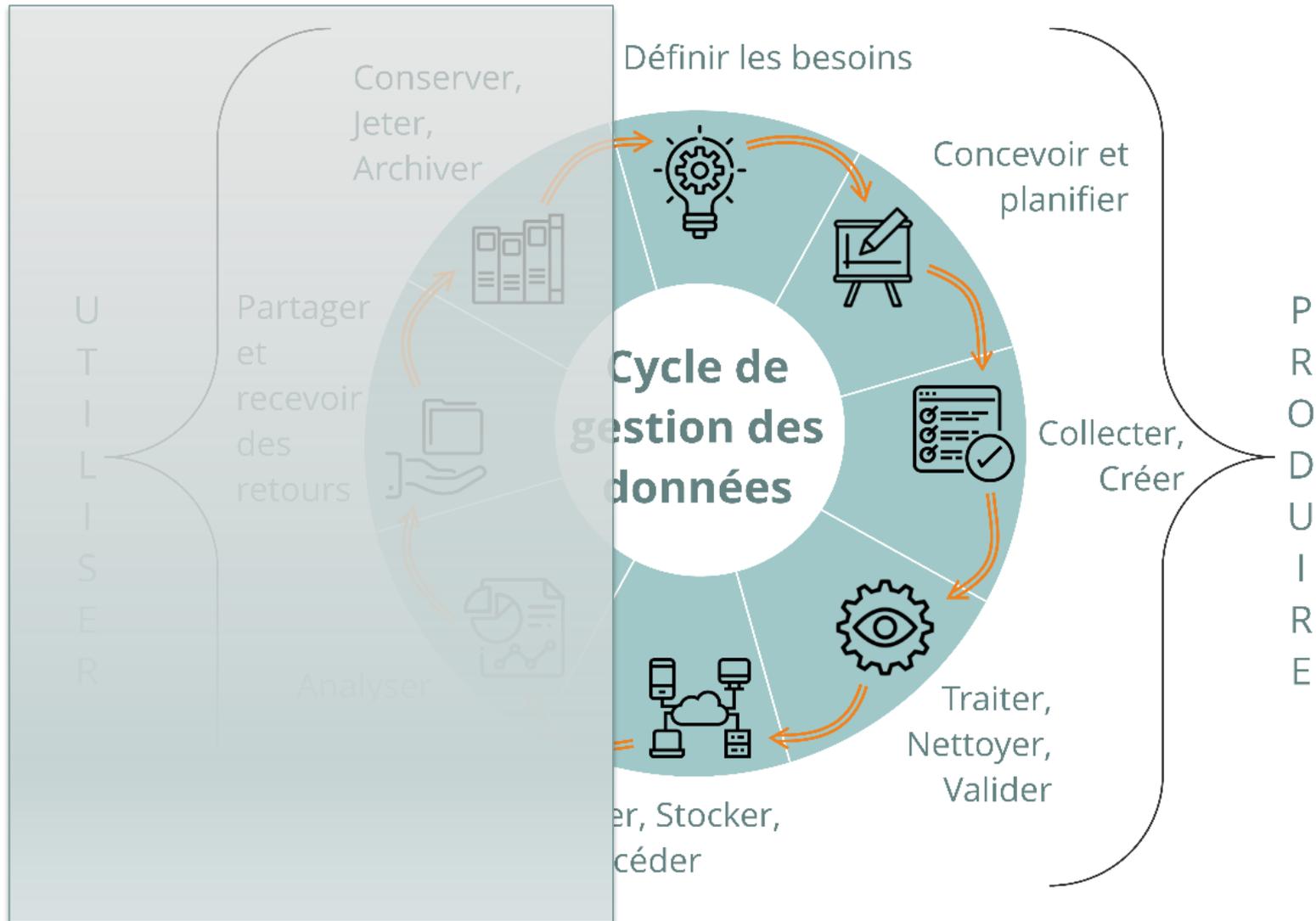


Retours sur les devoirs



La gestion responsable appliquée à la production des données

Cycle de gestion des données



Étape 1 :



- Définir l'**objectif de** la collecte des données (et la base juridique)
- En fonction de ces besoins :
 - Vérifier la **compatibilité** avec les lois applicables
 - **Évaluer les risques** associés à la collecte de données et déterminer les **mesures d'atténuation correspondantes.**
 - Appliquer les principes de **minimisation et de proportionnalité.**

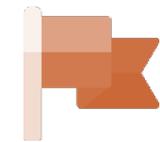
Cf. session précédente pour plus d'informations, de ressources, etc.

Vous souvenez-vous d'Akachaland et de notre ONG Licorne ?

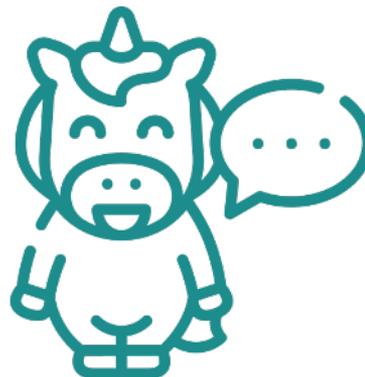


Rappelez-vous...

Dans le pays **Akachaland**, une inondation majeure durant la saison lunaire a dévasté une trentaine de villages, situés dans le nord. Vous êtes membre de l'ONG "**Licorne**", de Finobaka, spécialisée dans la protection des enfants et des femmes à qui vous fournissez également de la nourriture et des NFI.



Akachaland



Confidentialité

- Définir une **gestion** adéquate **des utilisateur·rices et des rôles** pour l'accès aux données
- Déterminer les moyens permettant aux populations concernées de fournir des retours d'informations (feedback) ou de formuler des demandes concernant leurs données.
- **Partage des données de conception / accords de non-divulgence**



Sécurité

- **Sélectionner des outils** "privacy by design & default" pour collecter, stocker et partager des données
- **Configurer les outils**

Qualité

- **Élaborer le plan d'analyse**
- Discuter de la faisabilité avec les **partenaires / communautés (et susciter l'engagement)**
- Tester/améliorer les outils de collecte de données dans un souci de qualité (identifiants uniques, traduction, calculs intégrés, etc.)



Culture des données

- **"Onboarding"** du personnel concerné
- Planifier **des formations** internes ou **avec des partenaires**



Témoignage



À quoi cela ressemblerait-il à Akachaland ?



Pour commencer l'assistance le plus tôt possible, votre équipe de la Licorne devez mener la collecte de données sur le terrain. Quelles sont les **premières étapes de la planification d'une collecte de données** ? Comment choisir l'outil et la méthode de collecte de données adéquats? Comment s'assurer que la collecte de données est conforme à son objectif? Que les populations peuvent également faire des retours?

La Licorne travaille en **consortium avec Akachaland soins**. Les 2 ONG ont décidé de partager la base de données, afin d'éviter de collecter trop de données. Licorne travaille également avec une chercheuse comme consultante externe.

Comment allez-vous prévoir de **partager les données personnelles et sensibles avec vos partenaires** en toute sécurité ? Comment respecter la confidentialité ?

Equipe du partenaire local spécialisé en assistance médicale, « Akachaland care »,

ayant accès aux données en en création/modification : **XX**

Rôles de Unicorn ayant accès aux données en lecture : **XX**

Research question	Indicator / variable	Questionnaire question	Data collection unit	Desired disaggregation	Analysis type
What are the characteristics of the population in terms of age, gender and dependency ratio?	Household composition	1. What is the sex of the head of household? 2. What is the age of the head of household? 3. Is the household member currently pregnant? 4. What is the total number of household members? 5. What is the sex of the household member? 6. What is the age of the household member (years)?	Household	Region, district	Population pyramid Proportion distribution by gender Histogram of average dependency of age Histogram of variance of age
What are the most common causes of household base morbidity and its associated health care utilization (consultations, hospitalizations, etc.)?	Demographic data	What is the age of the household member (years)?	Household	Region	Demographic breakdown between population above and below 15 years and percentage of dependent (15 or age or over 15 years and the ratio population aged 15 or over population in labor population including working age population between 15 and 64 years)
What are the most common causes of household base morbidity and its associated health care utilization (consultations, hospitalizations, etc.)?	Healthcare utilization	What are your household's base needs (as you see them)?	Household	Region	Frequency distribution



AGREEMENT
CONCERNING THE PROTECTION OF PERSONAL DATA
FOR THE SHARING OF PERSONAL DATA
OF REFUGEES AND HUMANITARIAN AID BENEFICIARIES
(DATA SHARING AGREEMENT, this "Agreement")
Between
UNICORN
And
Akachaland Care
.....

Preamble

fferent stakeholders signing this DSA, list the legal framework binding d by the present agreement and list all relevant other surrounding law. ve any implication here.



Data sharing with a third party - Checklist

Date: _____
 Program: _____
 Country: _____
 Names of the persons who filled this checklist: _____

Data sharing analysis	Description	Comments
Describe the project (aim, duration, implementation area, main activities, targeted beneficiaries, ...), and the type of data sharing	https://www.cartong.org/fr/faq/faq-protection-donnees-personnelles-et-protection-des-donnees-personnelles/	
Profile of the third party	<input type="checkbox"/> Power <input type="checkbox"/> International NGO/Association <input type="checkbox"/> University <input type="checkbox"/> Authority <input type="checkbox"/> Local NGO/Association <input type="checkbox"/> Others: _____	
Description of the third party (Specify: how did you contact with this third party? Capabilities/ skills: Does this third party have the technical capabilities and resources to protect the shared data?)	Yes / No / NA Description: _____	
Is the third party ready to sign a data sharing agreement?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Not identified with the third party <input checked="" type="checkbox"/> Not identified with the third party	
General analysis of the third party	<input type="checkbox"/> Data sharing purpose is specific, legitimate and in the best interest of the beneficiaries <input type="checkbox"/> No data sharing purpose Description: _____	

API access

Allow access API access

Mobile app settings

User management

Access control

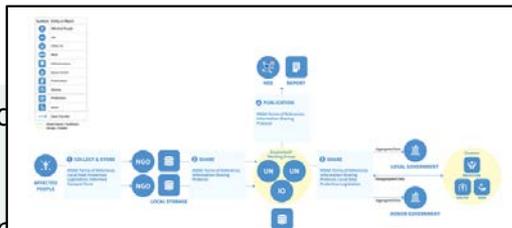
Copy from:

- Can edit forms
- Can submit responses
- Can view forms data in aggregate
- Can view individual responses
- Can modify or delete rows
- Can add forms
- Can delete forms
- Can see server details
- Can edit server controls
- Can edit server settings
- Can modify or delete server control data
- Can add forms
- Can delete forms
- Can view forms in or out of group
- Can move datasets in or out of group
- Can edit groups
- Can add groups
- Can delete groups

Ressources / modèles disponibles

Confidentialité

- Définir une **gestion adéquate des données** des **utilisateurs et des fournisseurs** et des **accès aux données**
- Déterminer les moyens de **protéger les données** des **populations concernées** et de **fournir des retours d'expérience** (feedback) ou de **formuler des demandes** concernant les **données**.
- **Partage des données** dès la **conception / accords de non-divulgaration**



Data Sharing Agreement

Overview/Background:

- A data sharing agreement establishes the terms and conditions that govern the sharing of specific personal and sensitive non-personal data between two or more parties.
- This type of agreement is essential to upholding legal, policy and normative requirements related to the sharing of personal and sensitive non-personal data, as well as to establish the roles and responsibilities of the Parties in the data sharing vis-à-vis data subjects.
- Organizational policies and applicable legislation may require a data sharing agreement for personal data. Always consult colleagues responsible for personal data protection in your organization, and refer to policies and legislation as these take precedence over this template. If no other guidance or template is available, refer to this template to develop a data sharing agreement.

This template is provided for use as a starting point in the development of a data sharing agreement.

SAMPLE NON-DISCLOSURE AGREEMENT

MUTUAL NON-DISCLOSURE AGREEMENT

THIS AGREEMENT is dated the _____ day of _____, 20____

BETWEEN [Name], registered in [country] whose registered address is [Address], ("NGO")

AND [Name], [address] ("Operator")

(individually referred to as "Party" and collectively referred to as "Parties")

Qualité

- **Élaborer le plan d'analyse** et de **collecte de données** dans un souci de **qualité** (identifiants uniques, traduction, calculs intégrés, etc.)
- Discuter de la faisabilité avec les **partenaires / communautés (et susciter l'engagement)**

Sécurité

- **Sélectionner des outils** "privacy by design & default" pour collecter, stocker et partager des données
- **Configurer les outils**

Culture des données

- **"Onboarding"** du personnel concerné
- Planifier **des formations** internes ou **avec des partenaires**

Ressources / modèles disponibles

Confidentialité

- Définir une **gestion** adéquate **des utilisateur-rices et des rôles** pour l'accès aux données
- Déterminer les moyens permettant aux populations concernées de fournir des retours d'informations (feedback) ou de formuler des demandes concernant leurs données.
- **Partage des données de**



Sécurité

- **Sélectionner des outils** "privacy by design & default" pour collecter, stocker et partager des données
- **Configurer les outils**

/ accords de non

plan d'analyse
la faisabilité avec



Culture des

- **"Onboarding"** du personnel concerné
- Planifier **des formations** internes ou **avec des partenaires**



Qualité

communautés (et susciter l'engagement)

- Tester/améliorer les outils de collecte de données dans un souci de qualité (identifiants uniques, traduction, calculs intéressants)

Section de la boîte à outils du MDC et ressources de Clear Global sur les langues

Webinaire (et présentation) de CartONG sur la collecte de données axée sur la qualité



Et plus transversalement :

- Élaborer des **plans de contingence** (en cas de violation des données ou de fuite de données)
- Définir des **procédures opérationnelles standard (SOPs)** claires, avec les rôles et les responsabilités,
- remplissez votre **registre de données**
- Inclure la gestion responsable des données dans votre **budget** (outils, formations, tests pilotes sur le terrain, traduction dans les langues locales, soutien externe pour l'anonymisation etc..).

Standard Operating Procedure for Data Incident Management

Overview/Background:

- A Standard Operating Procedure (SOP) for Data Incident Management establishes internal and cross-organizational approaches to identifying, resolving, tracking, and communicating about data incidents. In addition to the SOP, this requires a central registry or log that captures key details about the nature, severity, and resolution of different incidents.
- Data incident management helps reduce the risk of incidents recurring, supports the development of a knowledge base, and fosters more coordinated approaches to incident management over time.

Instructions for Use

- This template is designed to be adapted and tailored to specific contexts, and should be supplemented with additional directives and instructions as necessary. The relevant

FICHE DE REGISTRE DE L'ACTIVITÉ
Clavier et, Nom du client
(Créer cette fiche pour chaque activité listée en page 2)

Date de création de la fiche	Clavier et pour entrer une date.
Date de dernière mise à jour de la fiche	Clavier et pour entrer une date.
Nom du responsable conjoint du traitement (dans le cas où la responsabilité de ce traitement de données est partagée entre ses autres organisations)	Clavier et.
Nom du logiciel ou de l'application (s'il y en a un)	Clavier et.

Objectifs poursuivis
Décrivez clairement l'objet du traitement de données personnelles et ses fonctionnalités.
Exemple : pour une activité « formation des personnels », autre des demandes de formation et des périodes de formation éligibles, organisation des sessions et résolution des consultations.
Clavier et.

Catégories de personnes concernées

SOP TEMPLATE – SHARING OF SENSITIVE DATA INTERNALLY AND EXTERNALLY

The aim of this SOP is to define the procedures for internal sharing of sensitive data. This template needs to be adapted by the operation based on their contextual needs.

I. SHARING SENSITIVE DATA
Ensured sharing of sensitive data needs to be decided as part of the data collection process, to define first of all the sensitivity of the collected data, and then what and how it can be shared, based on data protection ethical principles.

The person who will consider whether the data should be shared and validate what can be shared for this dataset is: *XX project manager/ head of mission...*

II. THE SPECIFICITY OF SHARING DATA EXTERNALLY
All that is relevant for internal sharing is of course even more relevant for external sharing (checking that all Personal Identifiable Information (PII) and useless data is removed, that all possible data for which it is necessary is aggregated etc.).

The person in charge of validating the sharing of the data should evaluate its relevance (even if it is requested by the donor himself), and ensure that first and foremost the "Do no harm" principle is respected.

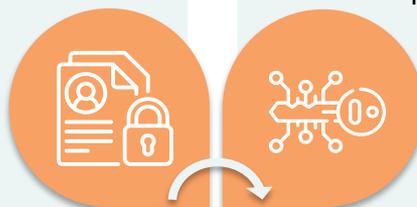
Sharing of any type of sensitive data through USB or external hard drive should be avoided at all cost.

Étape 3 :



Confidentialité

- Utiliser une **base légale adéquate**
- Informer sur l'utilisation des données



Sécurité

Respecter les procédures opérationnelles standardisées (SOPs) relatives aux logiciels et à l'équipement informatique.

Qualité

- Veiller à ce que la collecte de données se fasse dans la **bonne langue**
- Vérifier la qualité de la collecte des **données en cours**



Culture des données

- **Formation des** enquêteur.rices

À quoi cela ressemblerait-il à Akachaland ?



La Licorne a choisi son outil et sa méthode de collecte de données. Les enquêteur.rices seront bientôt déployé.es sur le terrain. La Licorne a mis en place des SOPs internes concernant la collecte de données. La population parle le warazu et la majorité des enquêteur.rices parlent cette langue.

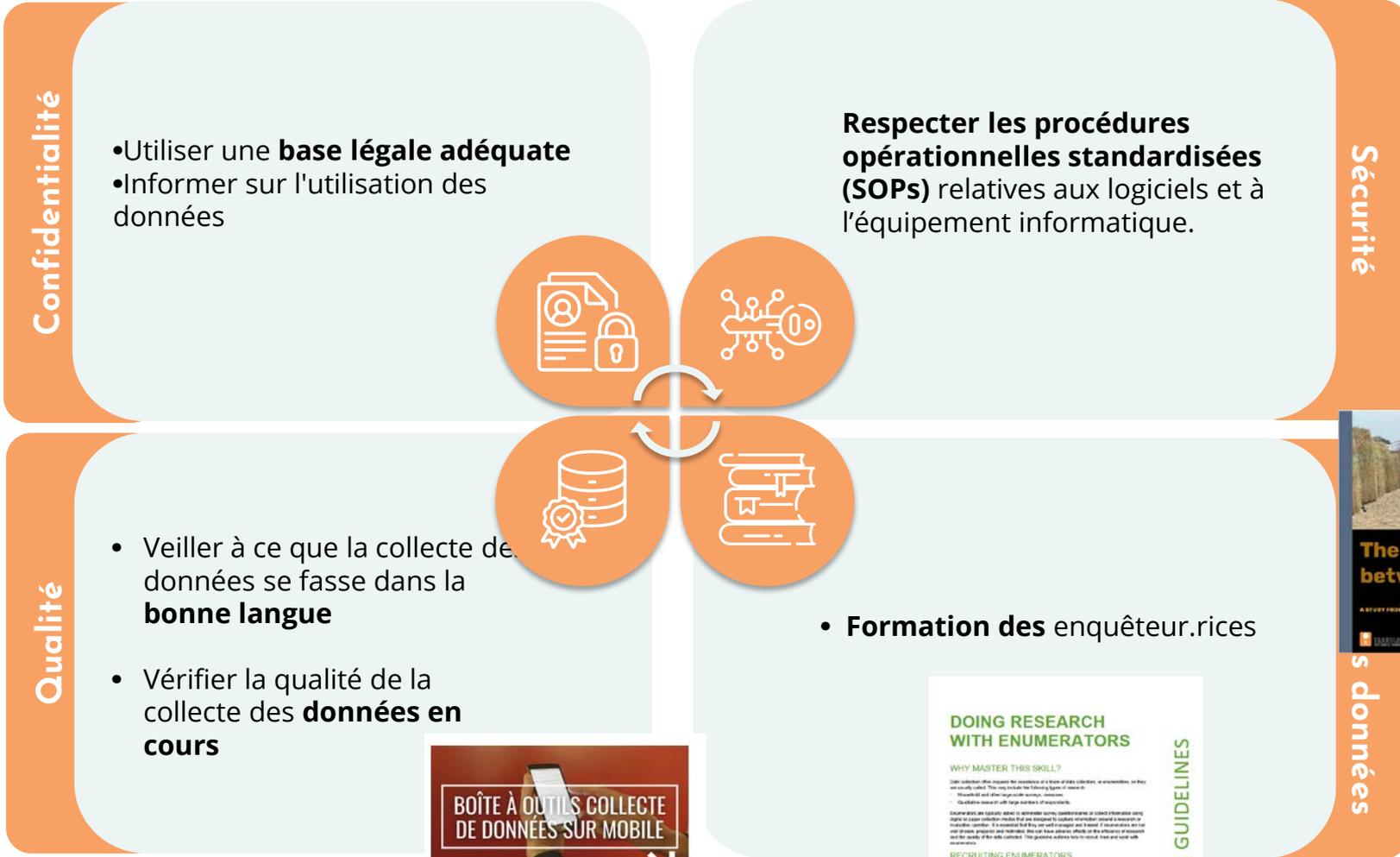
Que **faire avant de lancer la collecte** ? Comment choisir la base légale appropriée ?

Comment assurez-vous la **qualité de la collecte des données** ? Les enquêteur.ices connaissent-ils.elles l'outil, le questionnaire et le contexte ?

Comment vous assurez-vous que les **SOPs** de la Licorne sont respectées pendant la collecte ?



Ressources / modèles disponibles



Confidentialité

- Utiliser une **base légale adéquate**
- Informer sur l'utilisation des données

Respecter les procédures opérationnelles standardisées (SOPs) relatives aux logiciels et à l'équipement informatique.

Sécurité

Qualité

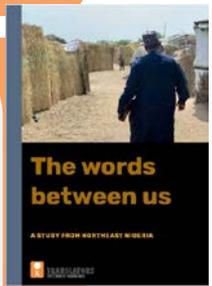
- Veiller à ce que la collecte de données se fasse dans la **bonne langue**
- Vérifier la qualité de la collecte des **données en cours**

- **Formation des enquêteur.rices**

s données



Collecte de données sur mobile
Initiez-vous à la collecte de données sur mobile



Étapes 4 & 5 :



Confidentialité

- S'assurer que les données ne sont **accessibles** qu'**au personnel autorisé (attention aux accès obsolètes), avec des droits spécifiques**.
l'examen régulier des droits d'accès
- Application des **droits de la personne concernée** (opposition, portabilité des données, rectification et effacement, accès...).



Sécurité

- Assurer la **sécurité physique et informatique** des données (papier et numérique) et de l'équipement informatique sur lequel elles se trouvent (antivirus, pare-feu, dernière version de l'outil, etc.)
- **Respecter les SOPs** en matière de nettoyage, de validation, d'accès... Sauvegarder les données ou s'assurer que le logiciel utilisé le fait. Interdiction des comptes partagés

Culture des données

Qualité

- Vérifier la **pertinence, l'exactitude et l'exhaustivité** des données
- les **triangler**
- Assurer la **comparabilité et l'intégrité des données** ainsi que la cohérence avec les bases de données secondaires

- S'assurer de la bonne compréhension de la qualité des données, des biais, des équipes impliquées dans le nettoyage, ainsi que des limites des données collectées.

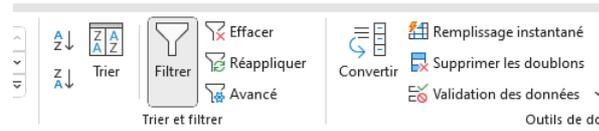
À quoi cela ressemblerait-il à Akachaland ?



L'équipe d'enquêteur.rices de la Licorne a collecté des données sur les enfants et les femmes pour lancer son aide et les a stockées. Seuls certains membres de la Licorne auront besoin de ces données pour travailler avec la population. Le bureau est partagé par toute l'équipe et est situé dans la zone nord, là où les " Akaidnappers " sont actifs.

Quelles **mesures de sécurité** prenez-vous concernant le matériel et les données stockées ? Les enfants et les femmes ont-ils la possibilité d'accès à leurs données ? Leurs données sont-elles traitées de manière confidentielle ?

Comment **mettez-vous en œuvre les SOPs** concernant le nettoyage des données ? Comment garantessez-vous **la qualité** de la base de données ?



PLAN D'ANALYSE					
Question de recherche	Indicateur / variable	Question de questionnaire	Unité de mesure / des données	Désignation des données	Type d'analyse
Quelles sont les données démographiques de la population en termes d'âge et de genre ?	Démographie (âge)	1. Quel est le genre de votre ménage ? 2. Quel est l'âge de votre enfant ? 3. Le nombre de ménages dans votre ménage ? 4. Quel est le nombre de membres du ménage ? 5. Quel est le genre du membre du ménage ? 6. Quel est l'âge des membres du ménage (années) ?	Ménage	Ménage - Individuel	Profil des ménages, Caractéristiques démographiques de la population, Structure de la population par âge
	Démographie (âge)	Quel est l'âge de votre ménage (années) ?	Ménage	Ménage	Profil des ménages, Structure de la population, Caractéristiques démographiques de la population, Structure de la population par âge
Quelles sont les données de base sur les enfants et les femmes dans votre ménage ?	Profil des enfants / femmes	1. Quel est le genre de votre ménage ? 2. Quel est l'âge de votre enfant ? 3. Le nombre de ménages dans votre ménage ? 4. Quel est le nombre de membres du ménage ? 5. Quel est le genre du membre du ménage ? 6. Quel est l'âge des membres du ménage (années) ?	Ménage	Ménage - Individuel	Profil des ménages, Caractéristiques démographiques de la population, Structure de la population, Caractéristiques démographiques de la population, Structure de la population par âge



Témoignage



Ressources / modèles disponibles

Confidentialité

- S'assurer que les données ne sont **accessibles** qu'**au personnel autorisé (attention aux accès obsolètes), avec des droits spécifiques.**
- **L'examen régulier** des droits d'accès
- Application des **droits de la personne** (opposabilité des données, effacement,

- Assurer la **sécurité physique et informatique** des données (papier et numérique) et de l'équipement informatique sur lequel elles se trouvent (antivirus, dernière version de...)
- **Respecter les SOPs** de nettoyage, de validation. Sauvegarder les données. S'assurer que le logiciel interdit les comptes partagés

Vérifier les mesures de sécurité des données de votre organisation

DÉTECTER LES DONNÉES DONT LA QUALITÉ EST DISCUTABLE

Résumé - Repérer les données dont la qualité est discutable

- **l'exhaustivité** des données
- les **triangler**
- Assurer la **comparabilité et l'intégrité des données** ainsi que la cohérence avec les bases de données secondaires

- S'assurer de la bonne compréhension de la qualité des données, des biais, des équipes impliquées dans le nettoyage, ainsi que des limites des données collectées.

Culture des données

BOÎTE À OUTILS ANALYSE DE DONNÉES QUANTITATIVES

Analyse de données quantitatives
Apprenez à maîtriser tous les trucs et astuces de l'analyse de données quantitatives

BOÎTE À OUTILS EXCEL

Comment Excel-er sur le terrain !
Devenez un inconditionnel de cet outil fabuleux qu'est Excel

2 Points clés

Collecte sur mobile et protection des données



Quiz



Vous voulez un outil sûr ?

Échelle de la sécurité des données

- Chiffrement des formulaires ou des données
- Chiffrement de l'application
- Localisation du serveur
- Hébergement de la plateforme
- Marquage des ensembles de données sensibles
- Dates d'expiration des données
- " Cold-room computer"
- ...



Avantages :

- Les données qui doivent être sécurisées le sont (pour des raisons éthiques et de conformité).

Inconvénients :



- Plus difficile à mettre en place et à utiliser
- Fonctionnalités distinctives nécessitant un coût plus élevé

Q&R ouvertes sur vos outils de collecte utilisés



Sécurisez vos systèmes



Quiz



Pourquoi ?

"Des garanties de sécurité adaptées à la sensibilité des informations doivent être mises en place avant toute collecte d'informations."

Normes professionnelles pour le domaine de la protection

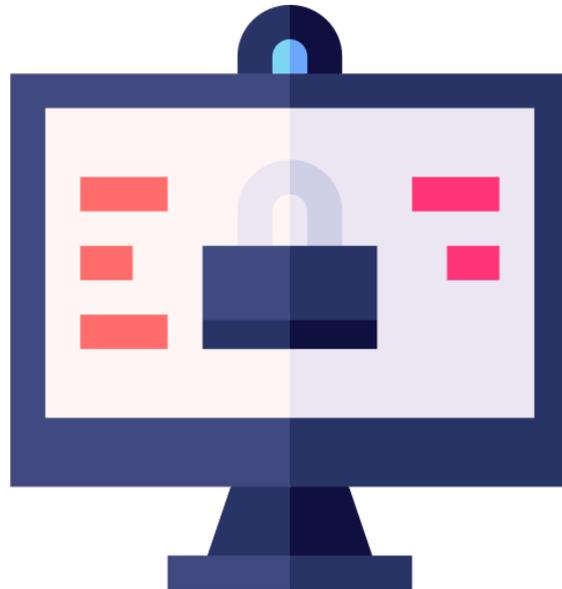


Source: centre for humanitarian data

Sur le terrain, l'**hygiène de base en matière de sécurité numérique fait souvent défaut**. La gestion des mots de passe et le chiffrement sont faibles, voire inexistants, et l'authentification multifactorielle et la détection des intrusions ne sont pas des pratiques courantes à l'heure actuelle. Les données contenues dans des appareils insuffisamment protégés peuvent être exposées lors du passage des points de contrôle de sécurité et des frontières. Les appareils non protégés peuvent être confisqués, corrompus et compromis.

Mai 2019 - Événement à Wilton Park - OCHA

*Nous essaierons ici de nous concentrer sur les **choses qui peuvent être faites au niveau de l'individu ou de la mission**, mais en fonction de votre organisation, certains de ces aspects doivent être abordés au niveau de l'organisation.*



1/ Sécuriser son poste de travail

Objectif : Empêcher les accès frauduleux, le lancement de virus ou la prise de contrôle à distance, notamment via Internet.

Comment ?

- **Mises à jour** régulières des logiciels et des antivirus
- **Déconnectez-vous** lorsque vous vous éloignez de votre ordinateur
- Limiter l'utilisation de stockages de support mobile type USB
- **Ne pas utiliser d'équipement personnel** dans un contexte professionnel (aussi appelé *BYOD* - "*Bring your own device*")
- Ne vous connectez pas à des **réseaux Wi-Fi publics** et **utilisez des réseaux privés virtuels (VPN)** si nécessaire.

2/ Se protéger contre le phishing

Objectif : Prévenir les accès frauduleux par hameçonnage

Définition : communication frauduleuse se faisant passer pour une source fiable, destinée à inciter les utilisateurs à divulguer des données sensibles ou à installer des programmes malveillants. Ces attaques ont souvent lieu par courrier électronique, mais peuvent également se produire sur les réseaux sociaux (**source : CyberPeace institut**).

Comment ?

- **Ne jamais cliquer sur un lien provenant d'un contact inconnu**
- **Vérifier l'adresse électronique de l'expéditeur**
- **En cas de doute, contactez l'expéditeur par un autre moyen de communication pour obtenir une confirmation.**

3/ Des échanges sécurisés

Objectif : Sécuriser les transmissions de données personnelles et sensibles

Comment ?

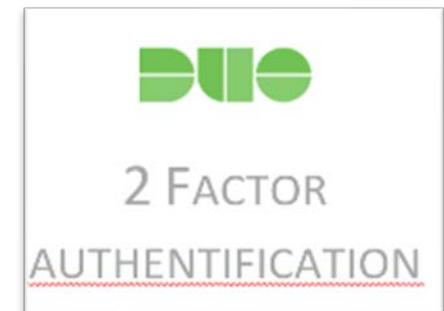
- **Déidentifier les** données si possible
- Utiliser des **plateformes de partage** sécurisées
- **Chiffrement des** données
- **Éviter les pj associées aux courriels**
- **Partager les mots de passe par le biais de canaux sécurisés**
- **Sensibilisez votre destinataire !**

4/ Gestion de l'authentification

Objectif : Sécuriser l'accès aux applications

Comment ?

- Utilisez des outils permettant un **accès individuel** et évitez à tout prix les comptes partagés.
- Ne plus écrire les mots de passe sur des **post-it**
- Utiliser des **mots de passe uniques** et **forts** (12 caractères, caractères spéciaux, etc.)
- Utiliser un **gestionnaire de mots de passe à l'échelle de l'organisation** (afin de pouvoir gérer facilement tous les mots de passe).
- Pensez à utiliser l'**authentification à 2 facteurs pour les outils contenant des données personnelles ou sensibles**



(Exemples)

5/ Sécurisation des équipements mobiles

Objectif : Anticiper les violations de données potentielles liées au vol ou à la fuite de supports de stockage mobiles.

Comment ?

- **Chiffrer autant que possible les** équipements mobiles et les supports de stockage (disques durs internes/externes ; smartphones ; clés USB).
- **Vérifier** que des mesures de **sauvegarde** et de **synchronisation** sont en place
- Veiller à ce que les **systèmes de verrouillage des** équipements soient suffisamment robustes
- Ne vous connectez jamais à un réseau **Wi-Fi public** et **utilisez un réseau privé virtuel (VPN)** si nécessaire.



(Exemples)

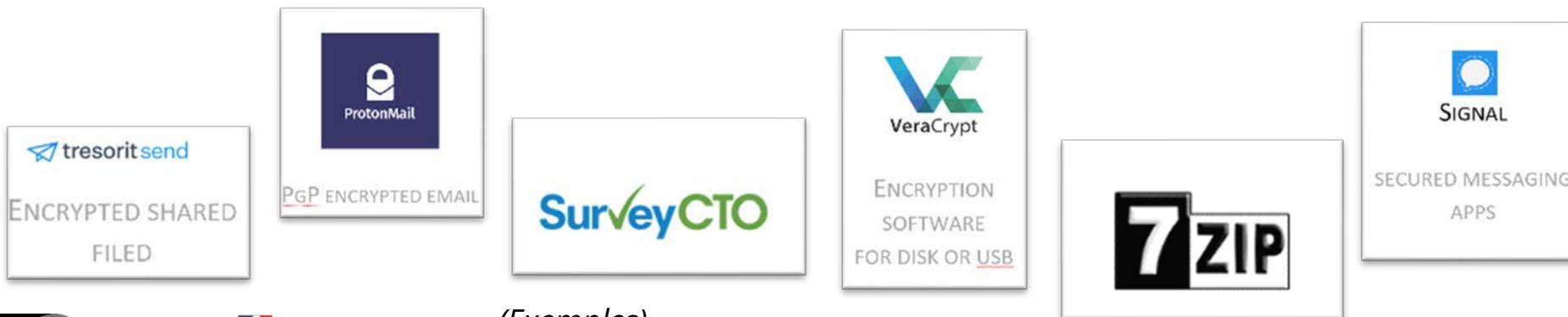
6/ Chiffrer les données si nécessaire

Objectif : garantir l'intégrité et la confidentialité des données :

Définition : codage d'un message ou d'une information de manière à ce que **seules les personnes autorisées** puissent y accéder et que celles qui ne le sont pas ne le puissent pas.

Comment ?

- Favoriser les outils qui permettent le chiffrement des données personnelles ou sensibles (ex : SurveyCTO vs Kobo, Signal vs SMS...).
- S'assurer qu'ils utilisent un **algorithme reconnu et sécurisé** (par exemple SHA-256, AES-256...).



(Exemples)

7/ Assurer la continuité

Objectif : Réduire les conséquences d'une **perte de données non désirée.**

Comment ?

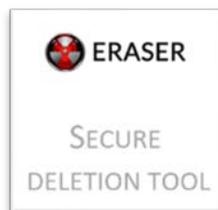
- Utilisez vos outils institutionnels, si vous en disposez (ou mettez-les en place), **pour effectuer des sauvegardes fréquentes de vos données.**

8/ Superviser la destruction des données

Objectif : Garantir la **destruction correcte des données à la fin du cycle de vie du matériel informatique et des logiciels.**

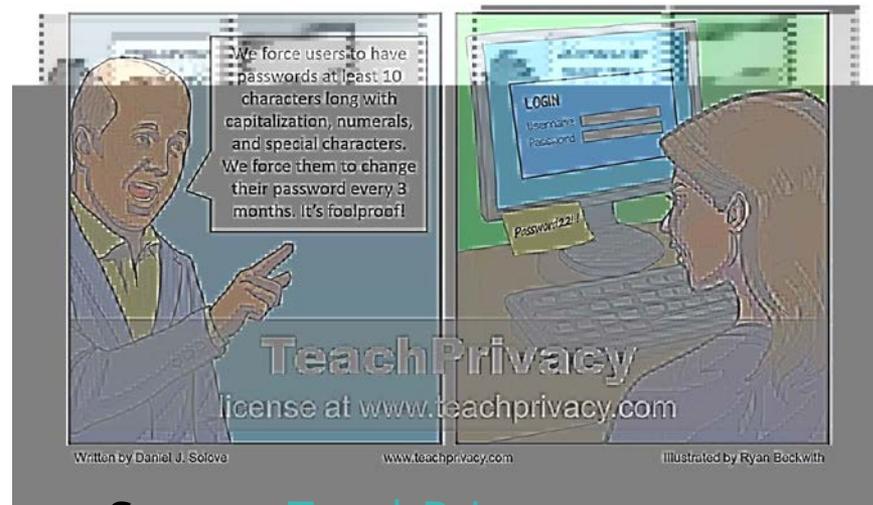
Comment ?

- **Fixer une date de suppression/d'archivage pour tous les ensembles de données personnelles/sensibles et prévoir des procédures pour garantir le respect de cette date.**
- **Effacer en toute sécurité les données de l'équipement** (avant de s'en débarrasser ou de l'envoyer en réparation) et des **logiciels utilisés.**



Conclusion sur la sécurité des données

- Garder à l'esprit la **tension entre l'efficacité opérationnelle et les mesures de sécurisation**
- Tenir compte du **niveau de sécurité existant et souhaitable des outils organisationnels** utilisés pour la **gestion des données programmes** (collecte, stockage et analyse des données, etc.).
- La sécurité des données est un sujet qui nécessite, entre autres, **l'appui d'experts en cybersécurité**



Source: [TeachPrivacy](http://www.teachprivacy.com)

Vous avez des questions sur le thème de la sécurité ?



Pause

Exercice en groupe

Discussion en groupe !



Votre groupe se verra **attribuer** un **thème**

On attend de vous

- de **dresser une liste des choses à faire et à ne pas faire en termes de bonnes pratiques sur le sujet**

- de **répondre à votre question "casse-noix"** en rapport avec le thème

Groupes :

1. minimisation des données
2. Plan d'analyse
3. Formation des enquêteurs
4. Identifiants uniques
5. Travailler avec des partenaires locaux
6. registre des données

Correction - quelques éléments de réflexion et ressources

La minimisation des données comme mantra pour avoir moins de données à protéger !



- Faire preuve **de créativité pour minimiser** la collecte et le partage des données
- Par exemple, une fois votre stratégie d'échantillonnage définie, avez-vous vraiment besoin de collecter les noms des enquêtés ?



DATA MANAGEMENT AND PROTECTION STARTER KIT
TIP SHEET 2
DATA MINIMIZATION
elan
The Electronic Cash Transfer Learning Action Network

WHAT IS DATA MINIMIZATION?

Data minimization is a privacy principle that requires the people collecting data to be intentional about what type of data is collected and how long it is retained. To meet this principle, teams should limit data collection to what is directly relevant and necessary to accomplish a specified purpose. In practice, this means assessing whether personally identifiable information (PII) must be a part of a data set and how long to keep data before disposing of it. Data minimization also refers to de-identification practices in which PII is stripped out of data sets before they are shared with others or made accessible to the public.

Data minimization applies to most program phases. Collecting the minimum amount of data, sharing only with those who need it, and keeping data only as long as necessary has clear privacy advantages; the less you have and the quicker you dispose of it, the less likely data can be inadvertently disclosed. But data minimization also has financial advantages; organizations spend less time and money collecting unnecessary data, cleaning it up once collected, and storing and archiving excess data.

Programs should strive to maintain a balance between responsibly minimizing data, while ensuring that data collection meets program needs.

Regulations and guidelines

There are few legal regulations that govern what type and quantity of data you can collect, but there are guidelines which can assist in making decisions related to data minimization.

One, the *OECD Privacy Principles*, states:

DATA MINIMIZATION
KEY TO PROTECTING PRIVACY AND REDUCING HARM

accessnow
Access Now defends and extends the digital rights of users at risk around the world. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots organizing, legal interventions, and campaigns such as Right2Know, we fight for human rights in the digital age.

Un plan d'analyse pour soutenir la qualité des données



- Un plan d'analyse est la clé de la qualité et permet de **documenter en détail votre analyse**
- Ce n'est pas parce que cela s'appelle " analyse " qu'il faut attendre d'être arrivé à ce stade pour la préparer
- Cela vous facilitera justement la vie au moment de l'analyse !



Boîte à outils analyse de données quantitatives

Rechercher

2.3 Se mettre en route / 2.4 Comment démarrer une analyse? / 2.4.3 Formuler un plan d'analyse

2.4.3 Formuler un plan d'analyse

28-Feb-2022 14 mins

TABLE DES MATIÈRES

- Plan de recherche
- Echantillonnage
 - Méthodes d'échantillonnage non-aléatoire

1 **Terre des hommes**

2 **Helping children worldwide.**

3

4

5 Inspiré de la guidance d'ACAPS : <https://www.acaps.org/en/>

6 **Le Plan d'analyse : Pourquoi ?**

7 Vous avez peut-être fait face à ces situations lors d'une enquête:

8 1) Vous ne savez pas par où commencer avec ce travail de collecte de réutiliser le même bon vieux questionnaire

9 2) Vous réalisez que les données collectées ne font pas sens, sont incohérentes ou pas comprises... Ou bien vous vous rendez compte que vous avez

10 3) Vous avez oublié d'inclure des questions importantes dans votre questionnaire trop tard maintenant.

11 4) La base de données est un vrai désordre, trop lourde, vous ne trouvez pas

Sources: Tdh & boîte à outils analyse quantitative de CartONG

Former les enquêteurs -votre "première ligne" de la gestion responsable des données



- Donner **un sens à leur travail**, expliquer pourquoi ils collectent des données
- **Leur faire " vivre " les situations** délicates de qualité/ responsabilité des données, à travers des " tests de standardisation", des situations réelles, des sites pilotes, etc.
- Leur donner des **retours** sur leur travail pendant et après la collecte des données.



SÉRIE DE WEBINAIRES Mardi 19 septembre 2023

SE FORMER À LA COLLECTE DE DONNÉES :
WEBINAIRE À DESTINATION DES ORGANISATIONS
NATIONALES OU LOCALES DE LA SOCIÉTÉ CIVILE

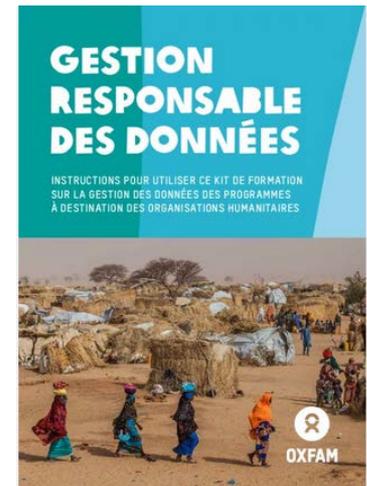
focus sur...

 Trucs et astuces pour améliorer votre collecte de données sur mobile

Un séric processé par  Avec le soutien de  



Collecte de données sur mobile
Initiez-vous à la collecte de données sur mobile



Sources: boîte à outils collecte données sur mobile de CartONG & Oxfam

Identifiants uniques



- Construire des identifiants uniques **qui ne permettent pas d'identifier directement les personnes** (ex: éviter « villageParisHHFinas »)
- Suivre une **procédure interne** là-dessus si elle existe pour homogénéiser les pratiques



Source: Enisa (UE)

Partenariats locaux



- **Questionner vos pratiques / relations avec vos partenaires locaux** en termes de données à usage opérationnel / S&E
- Pensez à long terme - il ne suffit pas de signer un contrat stipulant que "vous devez utiliser les données de manière responsable", vous devez leur donner les moyens (financiers, en termes de renforcement des capacités ou en compétences, etc.)



Dans le passé, nous avons organisé un atelier avec une échelle de « *localisation-washing* ».



Source: CartONG

Registre des données



- Le registre des données est un outil qui peut aider votre organisation à:
 - documenter les traitements des données
 - cartographier les données personnelles
- A voir quelles procédures votre organisation veut mettre en place, entre ceci, un diagramme R&R, etc.
- Mais il est important de savoir **qui est responsable d'un jeu de données** (sa sécurisation, sa RAD etc...), d'avoir un endroit où les mesures de mitigation sont listées etc...



FICHE DE REGISTRE DE L'ACTIVITÉ
Cliquez ici, Nom de l'activité
{Créer cette fiche pour chaque activité listée en page 2}

Date de création de la fiche	Cliquez ici pour entrer une date.
Date de dernière mise à jour de la fiche	Cliquez ici pour entrer une date.
Nom du responsable conjoint du traitement <small>(dans le cas où la responsabilité de ce traitement de données est partagée avec une autre organisation)</small>	Cliquez ici.
Nom du logiciel ou de l'application <small>(si pertinent)</small>	Cliquez ici.

Objectifs poursuivis
Décrivez clairement l'objet du traitement de données personnelles et ses fonctionnalités.
Exemple : pour une activité « formation des personnels » : suivi des demandes de formation et des périodes de formation effectuées, organisation des sessions et évaluation des connaissances.
Cliquez ici.

Catégories de personnes concernées

Source: la CNIL

Conclusion

Messages clés à retenir

- Une grande partie des exigences en matière de gestion responsable des données est définie au **stade de la planification/conception**.
- **Il existe de nombreux modèles/ressources pour vous aider** dans votre démarche / aider votre organisation à structurer/harmoniser ses procédures - il ne s'agit pas d'une montagne insurmontable.
- Certains sujets manquent encore de ressources / procédures prêtes à l'emploi - mais **suivez votre bon sens acquis de "responsabilité des données "** en attendant 😊 !

Devoirs pour la prochaine session



Merci de votre attention ! Des dernières questions?



info@cartong.org



www.cartong.org