Cycle de formation à la gestion responsable des données

cartong

MINISTÈRE DE L'EUROPE ET DES AFFAIRES ÉTRANGÈRES

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.

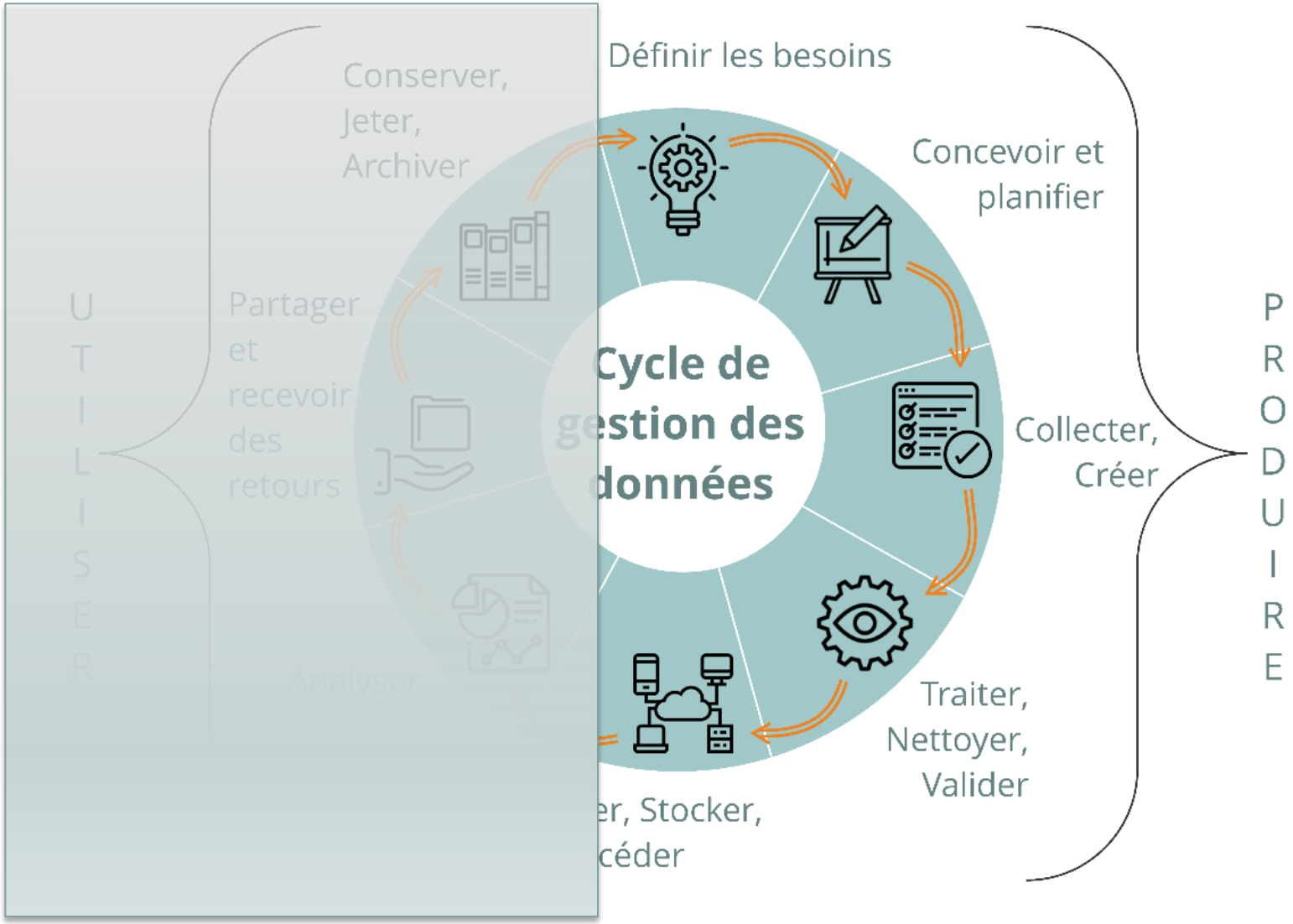
Avez-vous des questions supplémentaires sur la dernière session ?

Quiz

Retours sur les devoirs

La gestion responsable appliquée à la production des données

Cycle de gestion des données



Source: [Etude CartONG 2020]

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

Étape 2 : Concevoir et planifier

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 divulgation**

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

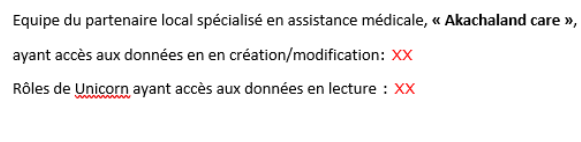
- **"Onboarding"** du personnel concerné
- Planifier **des formations** internes ou **avec des partenaires**

Témoignage

À quoi cela ressemblerait-il à Akachaland ?

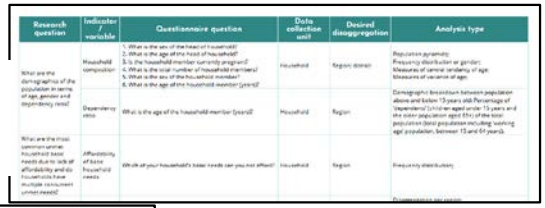
Pour commencer l'assistance le plus tôt possible, votre équipe de la Licorne devez mener la collecte de données sur le terrain. Quelles sont les **premières étapes de la planification d'une collecte de données** ? Comment choisir l'outil et la méthode de collecte de données adéquats? Comment s'assurer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

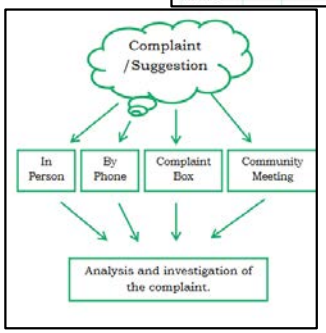
La Licorne travaille en **consortium avec Akachaland soins**. Les 2 ONG ont décidé de partager la base de données, afin d'éviter de collecter trop de données. Licorne travaille également avec une chercheuse comme consultante externe.
Comment allez-vous prévoir de **partager les données personnelles et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

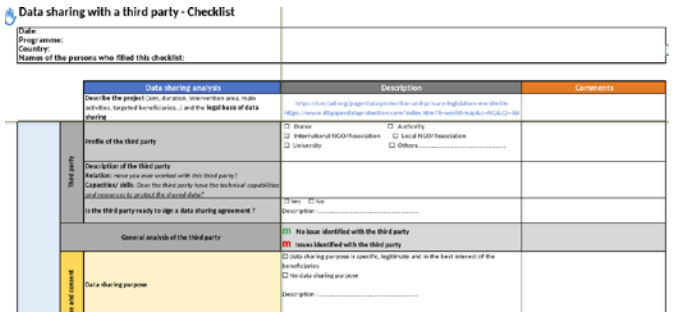
Rôles de Unicorn ayant accès aux données en lecture : XX

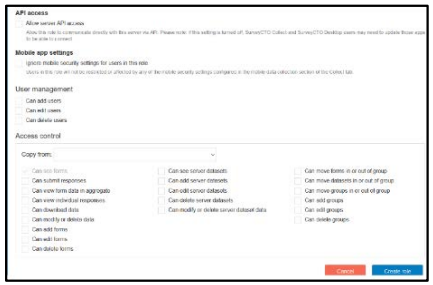



AGREEMENT
CONCERNING THE PROTECTION OF PERSONAL DATA
FOR THE SHARING OF PERSONAL DATA
OF REFUGEES AND HUMANITARIAN AID BENEFICIARIES
(DATA SHARING AGREEMENT, this "Agreement")
Between
UNICORN
And
Akachaland Care
.....

Preamble

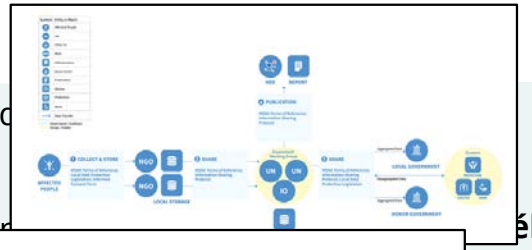
fferent stakeholders signing this DSA, list the legal framework binding d by the present agreement and list all relevant other surrounding law. ave any implication here.

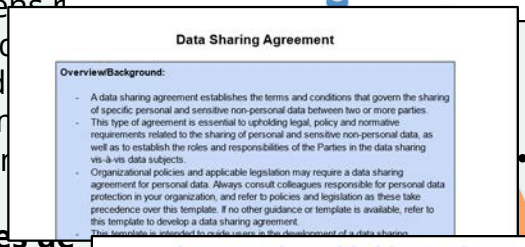


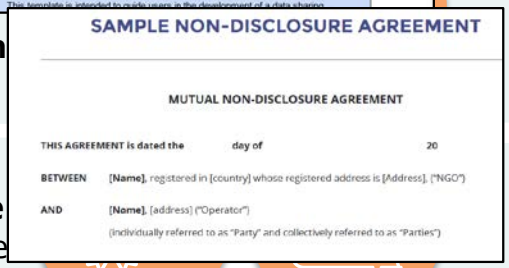


Sources : capture d'écran de SurveyCTO, orientations du groupe de travail PSEA, accord de partage des données SI, plan d'analyse CartONG

Ressources / modèles disponibles







Confidentialité

- Définir une **gestion** adéc
  utilisateur·rices et des
  l'accès aux données
- Déterminer les moyens
  aux populations conc
  fournir des retours d
  (feedback) ou de forr
  demandes concernar
  données.
- **Partage des données de**
  conception **/ accords de n**
  divulgation

Sécurité

- **électionner 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 ave
  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**

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**
  / accords de non
  n

Sécurité

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

Qualité

- **plan d'analyse**
  la faisabilité ave
  ires /
  communautés (et suscite
  l'engagement)
- Tester/améliorer les outils de collecte de données dans u souci de qualité (identifiants uniques, traduction, calculs inté

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

Culture des

- **"Onboarding"** du personnel concerné
- Planifier **des formations** nternes ou **avec des** artenaires

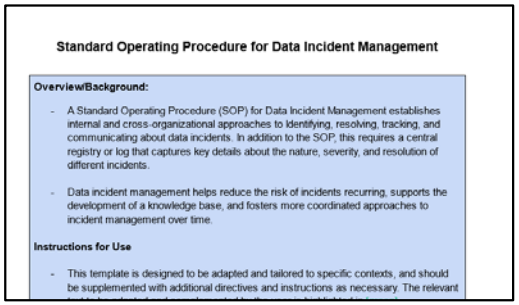
cartong

MINISTÈRE DE L'EUROPE ET DES AFFAIRES ÉTRANGÈRES

Étape 2 : Concevoir et planifier

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

Cliquez ici, Nom de l'activité

(Créer cette fiche pour chaque activité listée en page 2)

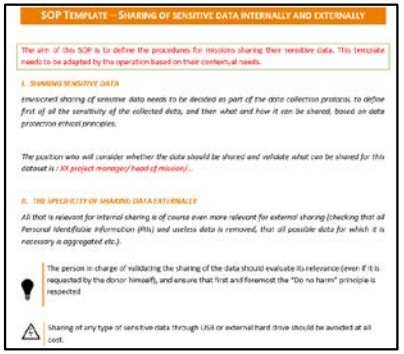
Date de création de la fiche	Cliquez ici pour entrer une date.
Date de dernière mise à jour de la fiche	Cliquez ici pour entrer une date.
Nom du responsable conjoint du traitement *(dans le cas où la responsabilité de ce traitement de données est partagée avec un autre organisme)*	Cliquez ici.
Nom du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



SOP TEMPLATE – SHARING OF SENSITIVE DATA INTERNALLY AND EXTERNALLY

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

I. SHARING SENSITIVE DATA

Ensconced sharing of sensitive data needs to be decided as part of the data collection protocol, 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 position 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 (PIIs) 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.

Sources : Task Force de l'IASC, CNIL, exemple de Tdh SOP

Étape 3 : Collecter, Créer

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 ?

Sources : capture d'écran de la boîte à outils Kobotoolbox

Ressources / modèles disponibles

Confidentialité

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

Sécurité

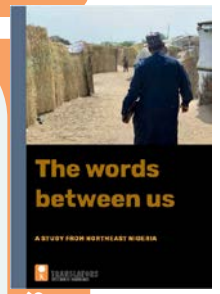
Respecter les procédures opérationnelles standardisées (SOPs) relatives aux logiciels et à l'équipement informatique.

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**

Sécurité des données

- **Formation des** enquêteur.rices



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

cartong

MINISTÈRE DE L'EUROPE ET DES AFFAIRES ÉTRANGÈRES

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 partagées

Qualité

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

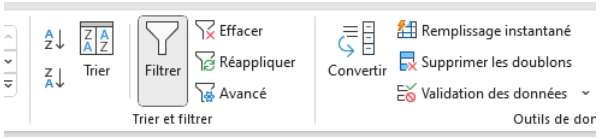
Culture des données

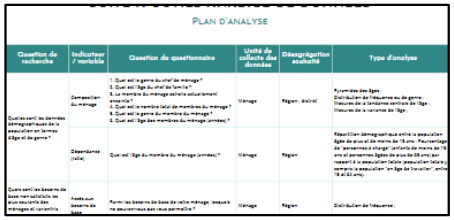
- S'assurer de la bonne compréhension de la qualité des données, des biais, des équipes impliquées dans le nettoyage, ainsi que des limites des données collectées.

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'accèsze à leurs données ? Leurs données sont-elles traitées de manière confidentielle ?
Comment **mettez-vous en œuvre les SOPs** concernant le nettoyage des données ? Comment garantissez-vous **la qualité** de la base de données ?





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** **ernée** (opposi- 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** nettoyage, de valida Sauvegarder les do s'assurer que le logi Interdiction des comptes partagées

Vérifier les mesures de sécurité des données de votre organisation

Qualité

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

Culture des données

- 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.

cartong

MINISTÈRE DE L'EUROPE ET DES AFFAIRES ÉTRANGÈRES

2 Points clés

Collecte sur mobile et protection des données

Quiz

Vous voulez un outil sûr ?

- 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

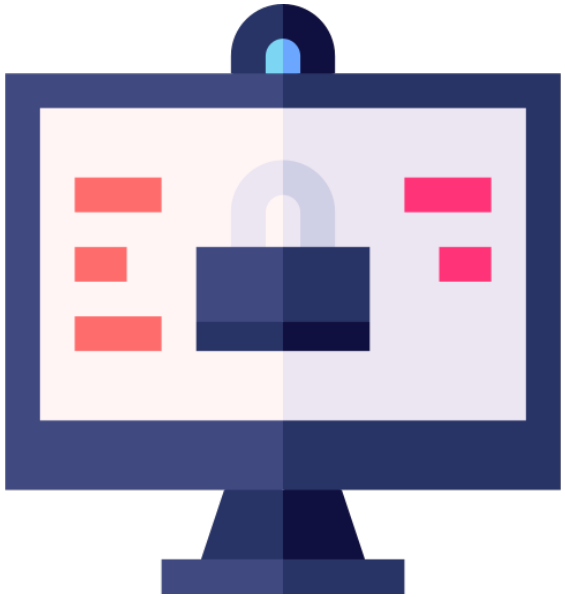
Source: centre for humanitarian data

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 - Evénement à Wilton Park - OCHA

Nota Bene

*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

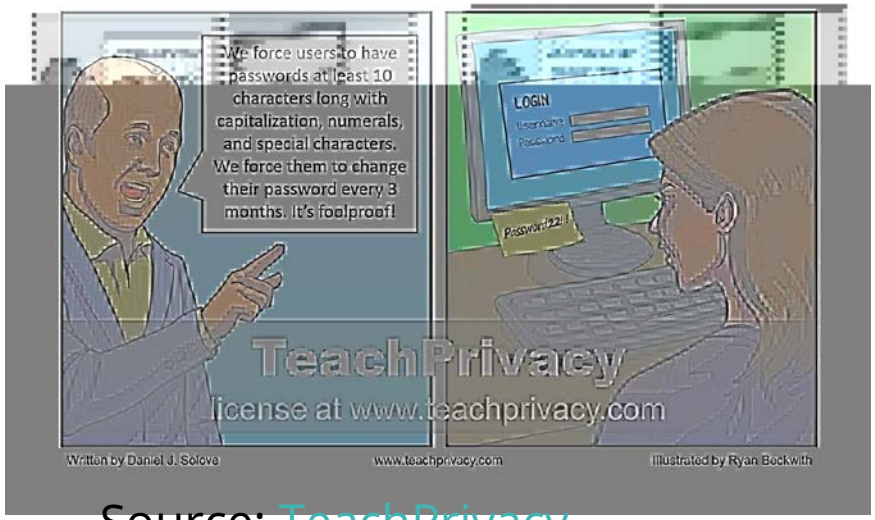
Objectif : Garantir la destruction correcte des données à la fin du cycle de vie du matériel informatique et des logiciels.

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

Questions & réponses

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

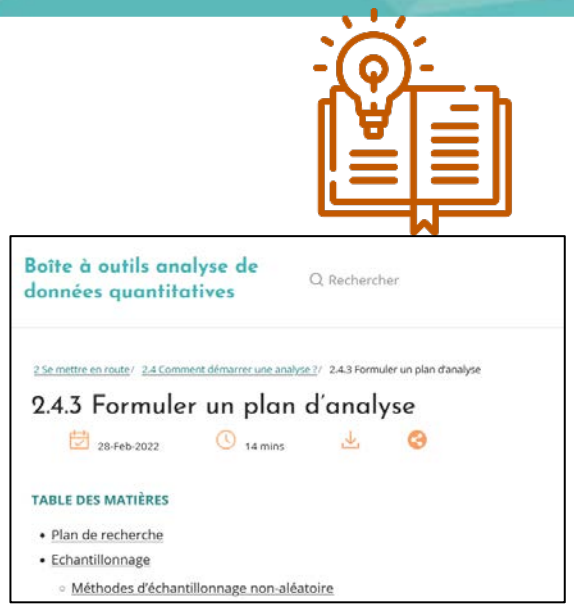
La minimisation des données comme mantra pour avoir moins de données à protéger !

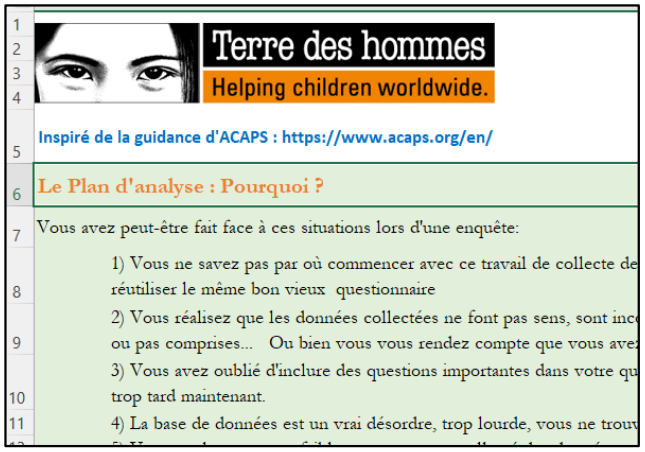
- Faire preuve **de créativité pour minimiser** la collecte et le partage des données
- Par exemple, une fois votre stratégie d'échantillonnage définie, avez-vous vraiment besoin de collecter les noms des enquêtés ?

Sources: Accessnow & Calpnetwork

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 !



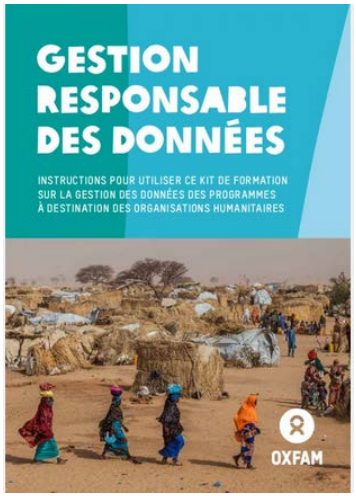


Sources: Tdh & boite à outils analyse quantitative de CartONG

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.

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



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

Identifiants uniques

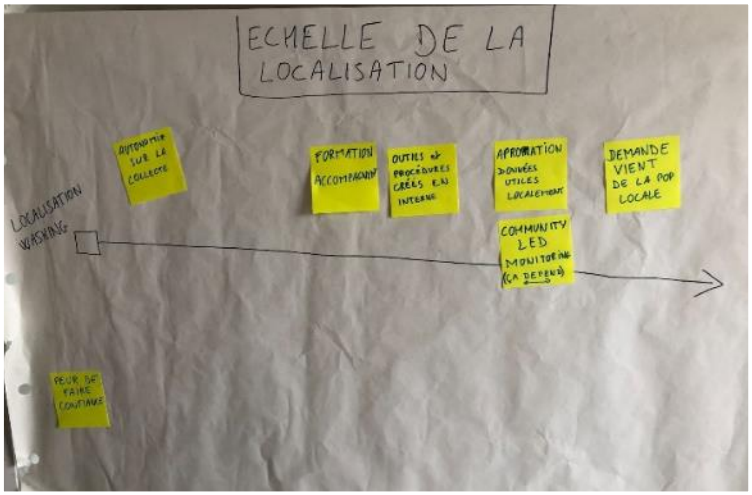
- Construire des identifiants uniques **qui ne permettent pas d'identifier directement les personnes** (ex: éviter « villageParisHHFinas »)
- Suivre une **procédure interne** là-dessus si elle existe pour homogénéiser les pratiques

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.)

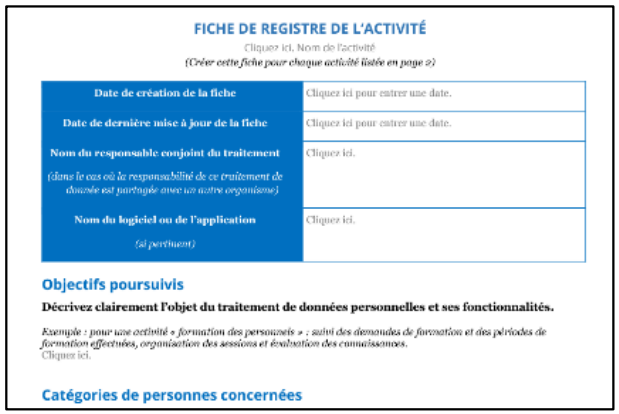
Dans le passé, nous avons organisé un atelier avec une échelle de « *localisation-washing*".



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 *(dans le cas où la responsabilité de ce traitement de données est partagée avec un autre organisme)*	Cliquez ici.
Nom du logiciel ou de l'application *(si pertinent)*	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