Cycle de formation à la gestion responsable des données

cartong

MINISTÈRE DE L'EUROPE ET DES AFFAIRES ÉTRANGÈRES

Session 2 : Focus sur les principes de la protection des données

Introduction à la session 2

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 2

- Introduction à la session d'aujourd'hui
- Comprendre les grands principes de la protection des données
  - Premier aperçu de l'étude de cas
  - Aperçu des grands principes de la protection des données
- 5 sujets d'intérêt
  - Quelle base légale choisir pour la collecte de données ?
  - Et maintenant, qu'en est-il du consentement ?
  - Comment gérer et atténuer les risques ?
  - Comment aborder les différentes législations ?
  - Que faire en cas de violations des données ?
- Conclusion

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.

L'objectif de cette session : démystifier cela !

Transformer cela en quelque chose que vous comprenez et sur lequel vous pouvez agir !

Source: The Guardian

Questions & réponses

Avez-vous des questions concernant le contenu de la 1ère session ?

Quiz

Comprendre les grands principes de la protection des données

Premier aperçu de l'étude de cas

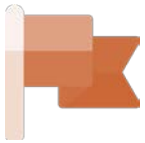
Présentation de l'Akachaland et de la Licorne

Imaginez...

Dans le pays **Akachaland**, une inondation majeure durant la saison des moussons 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 produits non alimentaires (NFI). Ses membres sont pour la plupart originaires de l'Akachaland et une partie du personnel est originaire de Finobaka.

Votre ONG "Licorne" a mis en place différents projets dans d'autres régions de l'Akachaland depuis une dizaine d'années. Elle a collecté et stocké des données personnelles.

Vous vous demandez comment gérer de manière responsable ces données ? Et comment appliquer les **principes de protection des données sur** le terrain ?



Akachaland

Aperçu des grands principes de la protection des données

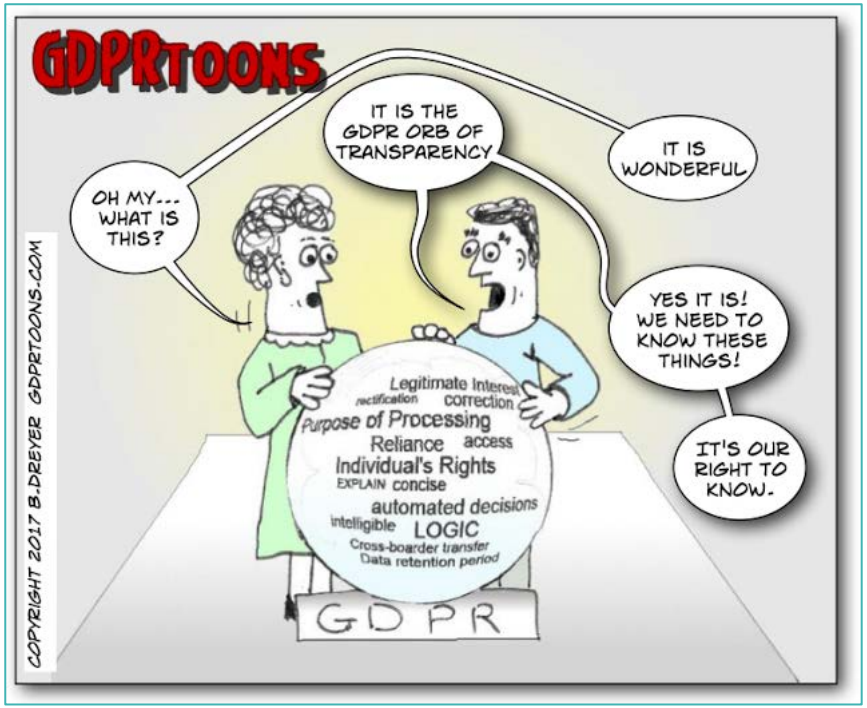
Aperçu des principes du RGPD

En nous "conformant au RGPD", nous ne devons pas perdre de vue **ce qui compte** - veiller à ne jamais utiliser les informations personnelles de quiconque d'une **manière qu'il.elle ne souhaite pas ou d'une manière qui pourrait lui causer un préjudice** (source: OXFAM).

- Légitimité et transparence
- Limitation de la finalité
- Proportionnalité, pertinence et minimisation
- Qualité
- Limitation de la période de conservation des données
- Confidentialité
- Redevabilité et documentation

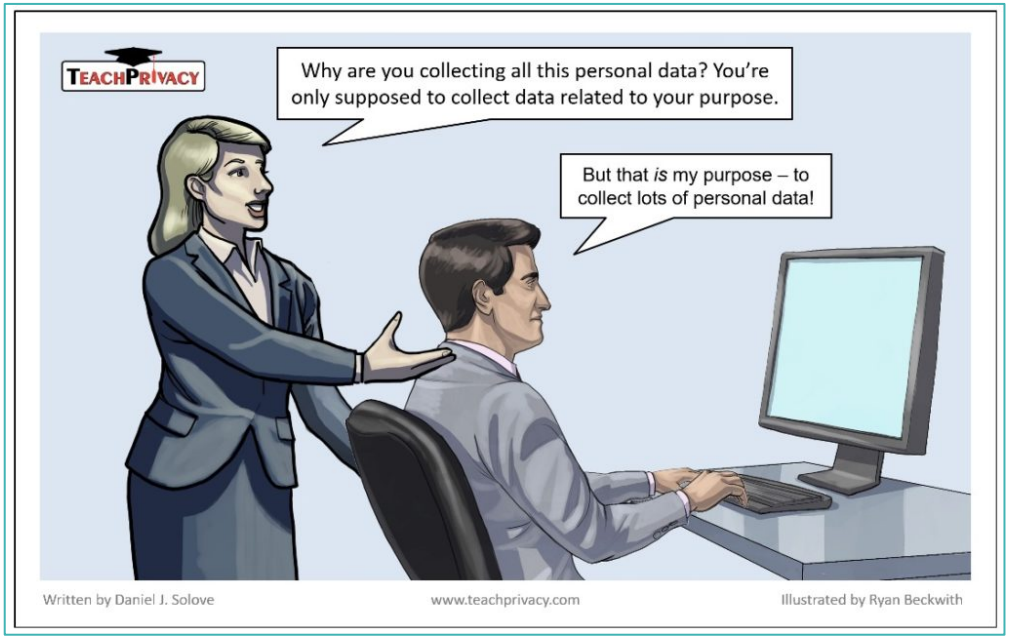
Légitimité et transparence

- S'assurer que les processus de collecte des données **n'enfreignent pas la loi ("base légale")**.
- Soyez **clair, ouvert et honnête** avec les gens sur la **façon dont vous utiliserez leurs données personnelles**.
- Enregistrez les objectifs et **les partager dans les informations** que vous donnez aux personnes



Source: gdprtoons.com

Limitation de la finalité



Source: teachprivacy

- Les données personnelles doivent être collectées pour une **finalité spécifique, légale** et **légitime**
- Précisez **dès le départ** les **finalités du traitement des données**.
- L'objectif de la collecte et de l'utilisation des données **doit être limité**

Proportionnalité, pertinence et minimisation

Source: cartoonstock

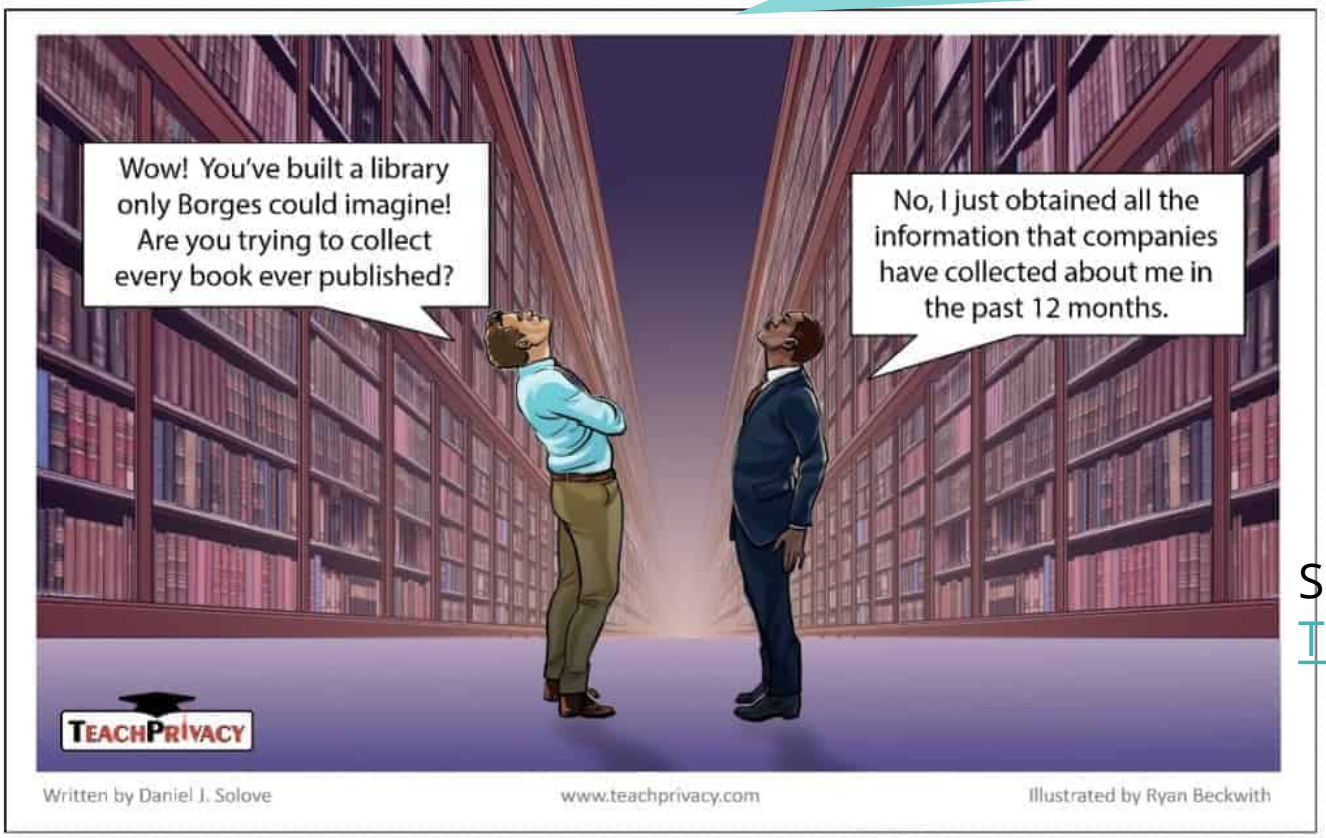
- Les données gérées par les acteurs humanitaires doivent être **adéquates, pertinentes et non excessives** au regard des finalités pour lesquelles elles sont collectées et traitées

- Ce principe s'applique tout au long du cycle de gestion des données.

Focus sur la minimisation des données

"Moins vous traitez de **données**, **moins vous courez le risque de causer des préjudices** avec ces données". **Principe clé** dans le secteur humanitaire

Exemples : supprimer d'une base de données les éléments qui ne sont pas nécessaires



Source: Teachprivacy

Qualité

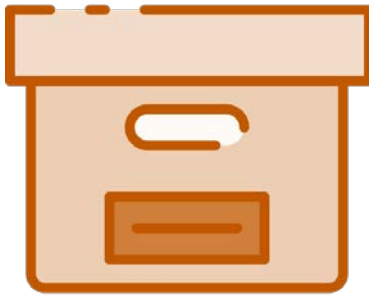
La qualité des données comprend des éléments tels que l'**exactitude, la pertinence, l'accessibilité, la comparabilité et l'actualité, y compris la mise à jour des données.**

Toutes les mesures raisonnables doivent être prises pour minimiser la possibilité de prendre une décision qui pourrait être **préjudiciable** à une personne, comme l'exclusion d'une personne d'un programme humanitaire **sur la base de données potentiellement incorrectes**.

Limitation de la période de conservation des données

La limitation de la période de conservation signifie que **les données sont conservées le moins longtemps possible.**

Assurez-vous de **planifier** et d'**être en mesure de justifier** la durée de conservation des données personnelles (par exemple : pour des audits, des besoins opérationnels, etc.) et veillez à conserver le moins de données possible pendant les phases de conservation (archivage intermédiaire, anonymisation...).



Confidentialité

La confidentialité implique :

- Disposer de **mesures de sécurité appropriées** pour protéger les données personnelles que vous détenez.
- S'assurer que seules les **personnes autorisées** ont accès à ces données et gérer les **droits d'accès**
- Disposer de processus appropriés pour **tester l'efficacité de vos mesures** et entreprendre toute amélioration.
- Permettre la **restauration des données** en cas d'incident physique ou technique.

Redevabilité et documentation

Source: gdprtoons

Assumez la responsabilité de ce que vous faites avec les données personnelles et de la manière dont vous respectez les autres principes :

- Être en mesure de **démontrer votre conformité**.
- Tenir des **registres** (par écrit) sur plusieurs aspects du traitement, tels que les **finalités, le partage et la conservation des données**.

Les responsables du traitement et les sous-traitants
ont tous deux des obligations en matière de documentation.

Difficultés associées

- L'application de ces principes dans certains pays peut s'avérer problématique d'un point de vue juridique lorsque, par exemple, **le chiffrement ou les VPN sont interdits.**

- Cela peut parfois conduire à **ne pas collecter les données** dont vous avez besoin.

Source: All things secured

" Dans les cas les plus graves, si le **niveau de risque est trop élevé** pour collecter toute donnée personnelle, les seules options sont de **collecter des informations limitées et anonymes, ou de s'appuyer sur des sources de données alternatives** " (Oxfam).

Un dernier détail

Tous ces éléments s'appliquent aux deux :

Papier

Numérique

Source de l'image : Tdh

Questions & réponses

Avez-vous des questions?

5 domaines d'intérêt

Quelle base légale choisir pour la collecte des données ?

Akachaland et la Licorne

Retour à Akachaland...

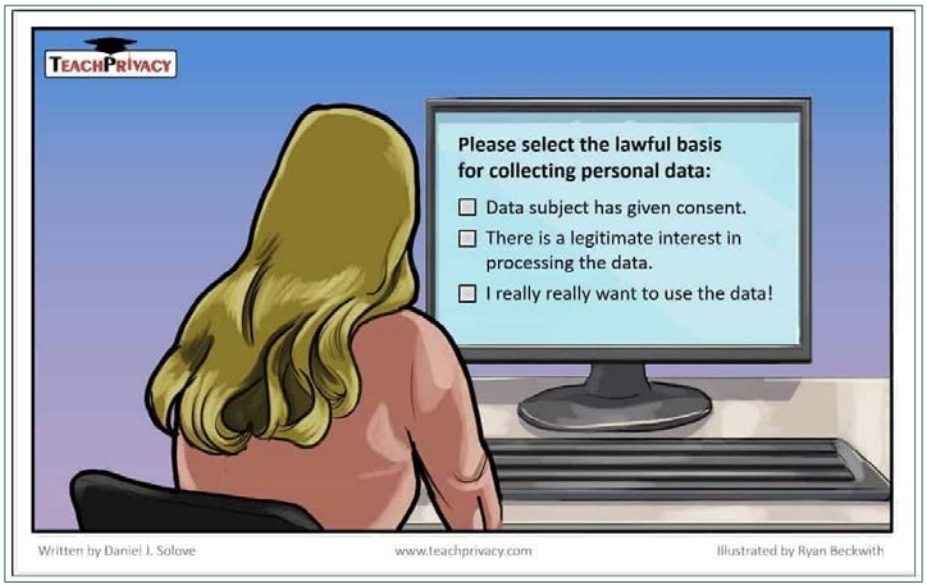
L'accès aux communautés du nord est assez restreint. Vous faites partie du premier convoi avec une équipe d'enquêteurs.rices : parmi les personnes survivantes, vous devez savoir combien il y a d'enfants et de femmes et quels sont leurs besoins urgents en termes de protection, de nourriture et de NFI. Pour ce faire, vous **devrez** probablement **collecter leurs données personnelles** et en déterminer l'usage exact.

Comment pouvez-vous **vous assurer de collecter les données personnelles des enfants et des femmes de manière légitime et transparente** ?

Quiz

Les 6 bases légales du traitement des données

Il existe 6 bases légales différentes pour le traitement des données dans le cadre du RGPD :



Source: Teachprivacy

- Obligation **contractuelle**
- Obligation **légale**
- Intérêt **public**
- Sauvegarde des intérêts **vitaux**
- Intérêts **légitimes**
- Le **consentement**

Obligation contractuelle

Le traitement peut être nécessaire à **l'exécution d'un contrat** que vous avez conclu avec la personne concernée, ou parce qu'il vous a été demandé de prendre des mesures spécifiques avant de conclure un contrat (par exemple, un devis).

Il s'applique aux fins suivantes :

- la gestion des **dossiers de ressources humaines**, y compris le recrutement
- la gestion des relations avec les **fournisseurs de biens/services**
- relations avec les **bailleurs de fonds**

Obligation légale

Le traitement peut être nécessaire pour vous **conformer à la loi** - identifiez les dispositions légales spécifiques ou une source appropriée de conseils ou d'orientations qui énoncent clairement vos obligations.

Exemples courants: **droit du travail**, **droit financier**...

Si cela risque d'exposer les populations à la répression, vous devriez **envisager de ne pas vous engager dans la collecte de données en** premier lieu.

Intérêt public

Le traitement est nécessaire à l'exécution d'une tâche d'**intérêt public** ou à l'exercice de fonctions officielles clairement mentionnées dans la loi.

- L'activité en question doit s'inscrire dans le cadre d'un **mandat humanitaire établi en vertu du droit national ou international.**

- Cela ne s'applique **pas** à la majorité des ONG

Intérêts vitaux

Le traitement est **nécessaire pour protéger la vie d'une personne** (la personne concernée ou une autre personne).

Il s'applique à :

- **la surveillance des épidémies**
- cas des **personnes portées disparues**
- en cas de catastrophe naturelle ou humaine, entraînant une **urgence humanitaire**
- traiter les données personnelles d'un parent pour **protéger la vie d'un enfant**
- pour les **soins médicaux d'urgence**

Restrictions aux "intérêts vitaux"

Toutefois, ils **ne peuvent pas être utilisés** pour des données relatives à la santé ou d'autres données de catégorie spéciale **si la personne est capable de donner son consentement**, même si elle refuse de le faire.
→ le traitement est alors limité aux **phases d'urgence proprement dites** (et limité à cette assistance) et sans traitement ultérieur.

Gardez à l'esprit que cela ne doit pas vous faire oublier les **autres droits** des personnes concernées (tels que l'information ou l'opposition)

Intérêt légitime

Le traitement est **nécessaire pour vos intérêts légitimes,** à moins qu'il n'existe une bonne raison de protéger les données personnelles des populations concernées qui l'emporte sur ces intérêts légitimes.

Il peut s'utiliser quand:

- vous utilisez les données des personnes d'une **manière à laquelle elles peuvent raisonnablement s'attendre**
- le traitement a un **impact minimal sur la vie privée**
- le traitement est **justifié par des raisons impérieuses**

Il s'agit de la base légale la plus souple. L'utilisation de cette base vous fait assumer une **responsabilité supplémentaire** dans la prise en compte et la protection des droits et des intérêts des personnes.

Exemples d'intérêt légitime pour les ONG

- **collecter les données** nécessaires à la réalisation du projet
- **l'analyse de ses systèmes informatiques** à la recherche de virus et à d'autres fins de sécurité informatique ;
- vérifier l'identité de la population concernée à des fins de **lutte contre la fraude ;**
- l'utilisation des données relative aux salariés pour le **suivi du temps de travail ;**
- se **défendre** dans une procédure judiciaire engagée par un ancien employé

Les éléments clés de la base légale

La plupart des bases légales exigent que le traitement soit **"nécessaire" pour une finalité spécifique**. Si vous pouvez raisonnablement atteindre la même finalité sans procéder au traitement, la base légale n'est pas valable.

Veillez à faire les choses correctement dès le départ - vous **ne** devez **pas changer de base légale à une date ultérieure** sans raison valable. En particulier, vous ne pouvez généralement pas passer du **consentement** à une base différente.

Quelle que soit la base légale utilisée pour collecter des données personnelles, la **redevabilité envers la population concernée implique de toujours l'informer**. Elle doit être informée des raisons et de l'utilisation de ses données personnelles avant qu'elles ne soient collectées.

Et maintenant, qu'en est-il du consentement ?

Akachaland et la Licorne

Retour à Akachaland...

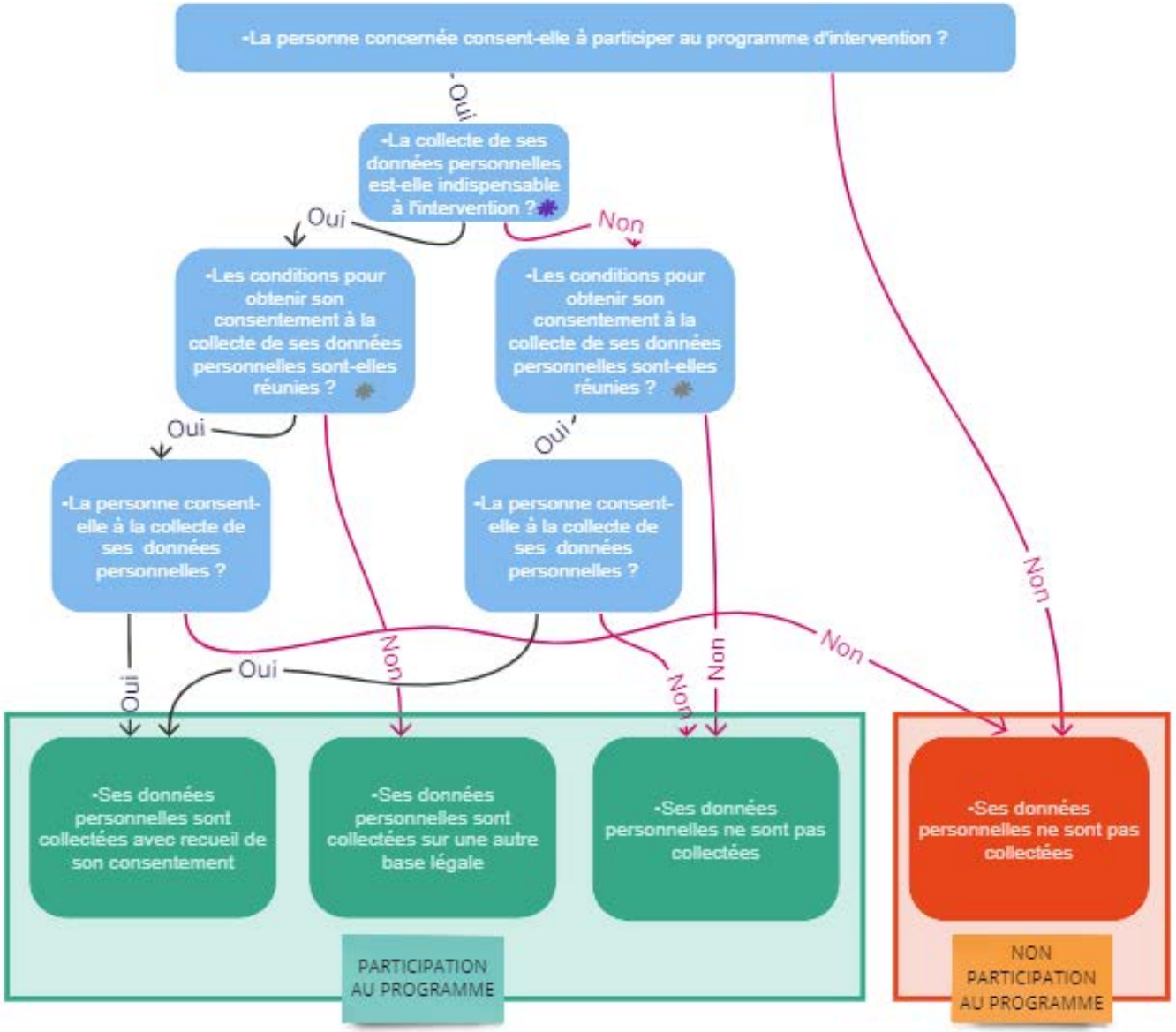
Il y a plus de 300 enfants et 500 femmes parmi les survivant.es. Ils.elles ne connaissent pas l'équipe et les activités de l'ONG. La population est traumatisée par cette catastrophe naturelle et se trouve dans une situation très vulnérable. Certaines personnes ont perdu leur maison et des membres de leur famille et n'ont nulle part où aller.

Pour commencer l'assistance le plus rapidement possible, afin de répondre aux besoins, vous et vos collègues de l'équipe Licorne devez mener la collecte de données sur le terrain avec la population affectée. Vous avez déterminé l'**objectif** et l'utilisation de **la collecte de données personnelles** ainsi que **ses limites.**

Comment **informer la population de** la nécessité de collecter ses données personnelles ? Comment instaurer la confiance au sein de la population ?

Consentement éclairé à la collecte de données

Source:
CartONG

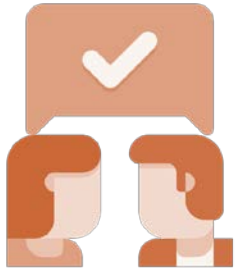


Conditions du consentement éclairé

Consentement = l'acronyme « FRIES »

Freely given (librement consenti- le consentement est clair, il n'y a pas de ruses ou de manipulations !)
Réversible (les personnes doivent pouvoir retirer leurs données à tout moment)
Informé (il vous incombe d'expliquer correctement aux personnes concernées ce qui va être fait avec leurs données, en tenant compte du contexte et des normes socio-culturelles)
Enthousiaste (les gens doivent pouvoir exprimer activement leur consentement !)
Spécifique (le consentement est donné à une fin spécifique et doit clairement être limité à celle-ci)

Source: The Engine room



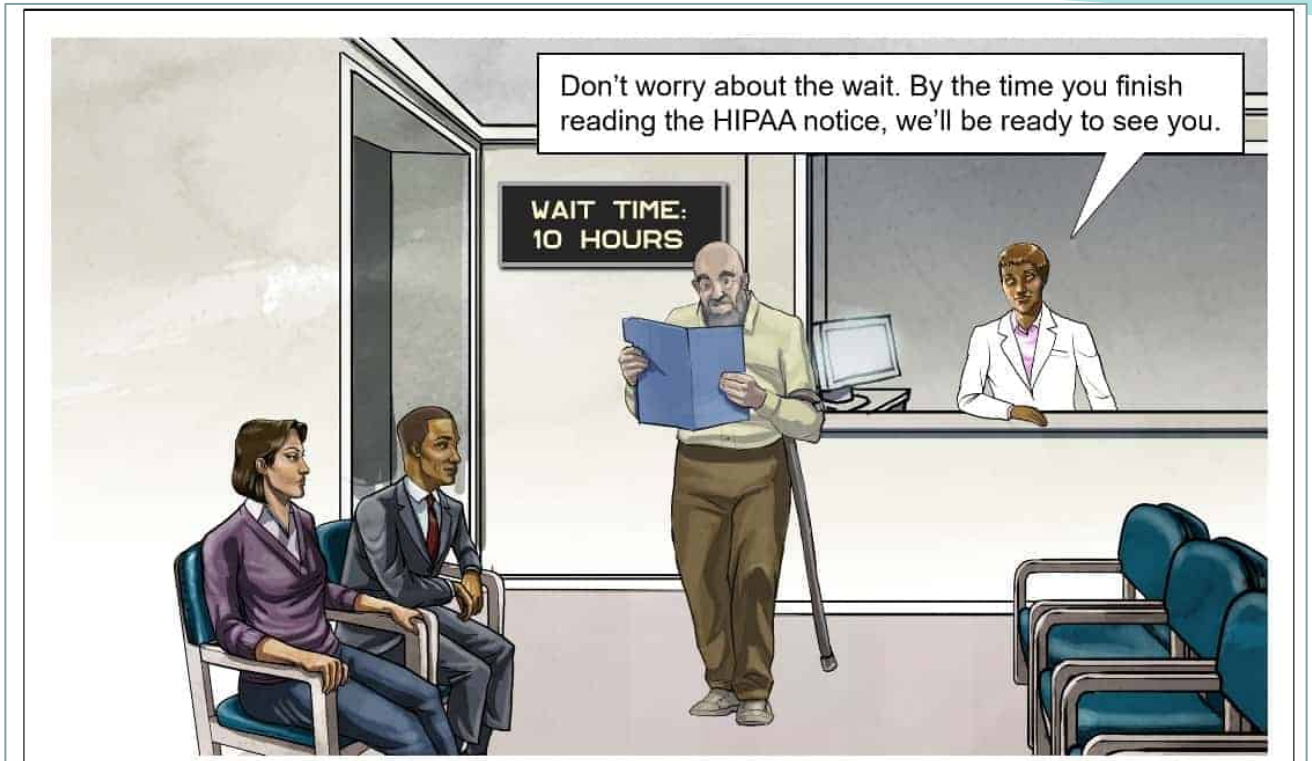
Les enjeux du consentement éclairé

Le consentement est censé **préserver la dignité des personnes et des communautés concernées**, mais il a été prouvé que ce n'est pas le cas :

- les personnes peuvent ne pas donner un consentement véritablement valable en raison de **différences culturelles** ou de lacunes dans les connaissances
- le consentement éclairé n'est pas efficace dans un environnement où les **déséquilibres de pouvoir sont** importants. S'il n'y a aucun moyen de refuser, le consentement n'est pas valable
- de refuser ou de retirer son consentement a souvent un impact sur la **capacité à recevoir de l'aide** et des services
- "les messages de consentement ne sont en fait **régulièrement pas demandés**" (Oxfam)

À garder à l'esprit

Cela signifie que l'organisation humanitaire détient un tel pouvoir sur eux que l'idée d'un consentement éclairé n'a pas de sens : c'**est comme "faire miroiter une friandise**", comme l'a fait remarquer un travailleur humanitaire en Somalie. (Human Rights Watch)



Source: Teachprivacy

Que faire alors ?

Nos recommandations, dans la mesure du possible :

- **Exclure le consentement** utilisé comme base légale pour la collecte de données, **dans la plupart des situations**, car sa validité n'est pas souvent solide

- Utiliser d'autres bases légales pour collecter les données, telles que l'**intérêt légitime** ou les **intérêts vitaux.**

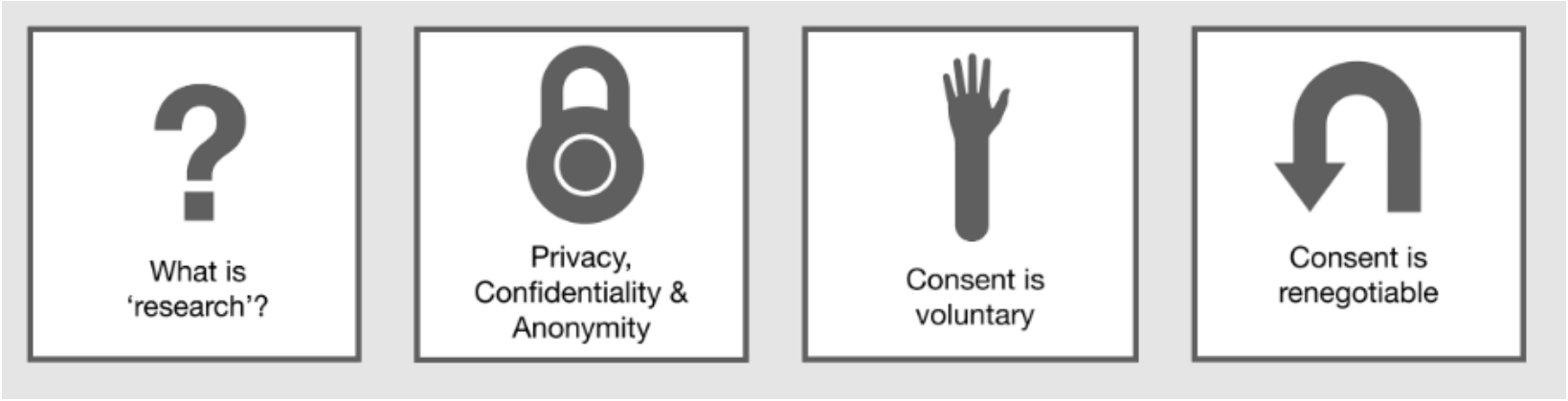
- **Utiliser le consentement lors de la collecte de données sensibles**, par ex. photos, des témoignages ou utilisation de données biométries - il est le mieux adapté car les risques associés sont plus forts.

- Il est impératif d'**informer les populations des raisons qui motivent le traitement de leurs données personnelles**, quelle que soit la base légale utilisée

Témoignage siège et terrain

De Tdh - les conditions spécifiques d'information auprès des enfants

- **CONSENTEMENT ou ASSENTIMENT** des enfants et consentement des personnes qui s'occupent d'eux -> QUELS adultes impliquer ?
- **INFORMATION - méthode** en fonction de la maturité émotionnelle et cognitive,
- Processus de **construction de la confiance** ou événement ponctuel - **ÉTHIQUE ou CONFORMITÉ**



Charte internationale pour une recherche éthique impliquant des enfants

De Tdh - illustration des pratiques et conditions spécifiques d'information des enfants au Burkina Faso

Eléments clés pour obtenir le consentement éclairé des enfants

Obtenir le consentement informé des enfants, une tâche difficile

Il peut s'avérer difficile d'obtenir le consentement informé des enfants, qui repose en partie sur l'âge et la maturité de l'enfant. Il n'existe aucune solution facile et globale pour tous les pays, âges et milieux. Le personnel de Tdh a toutefois l'obligation d'essayer d'obtenir le consentement informé des enfants qui fournissent des renseignements sur leur personne. Par ailleurs, le consentement informé des tuteurs légaux est obligatoire. Voici une liste de suggestions pour aider les enfants à comprendre ce à quoi ils accordent leur consentement.

- Présentez-vous en tant que personne plutôt que selon votre poste.
- Expliquez l'objectif de la collecte de données.
- Expliquez l'importance des données.
- Expliquez aux enfants les modalités et la durée de leur participation, ainsi que la manière dont la confidentialité des renseignements sera assurée.
- Expliquez aux enfants quel type de renseignements seront recueillis, de quelle manière, et comment ils seront utilisés.
- Assurez-vous que les enfants comprennent réellement ce que vous leur avez dit en leur demandant de le répéter.
- Donnez le temps aux enfants de poser des questions ou de soulever des préoccupations.
- Écoutez les enfants.
- Assurez-vous que les enfants savent qu'ils peuvent interrompre le processus à tout moment.
- Assurez-vous que les enfants comprennent que vous ne leur promettez aucunement d'améliorer leurs conditions de vie.
- Ne faites aucune promesse que vous ne pouvez tenir.
- Lorsque des enfants fournissent des dessins ou des rédactions, vous devez leur indiquer que leur œuvre pourrait être utilisée, puis leur demander s'ils désirent être identifiés à titre d'auteur ou d'artiste.

Dans les cas où le personnel rencontre des mineurs non accompagnés qui ne sont pas en présence d'un adulte légalement garant de leurs intérêts, on doit considérer avec soin s'il est dans l'intérêt de l'enfant d'entrer en contact avec Tdh.

Adapté de : Regional Working Group on Child Labour in Asia (RWG-CL), Handbook for action-oriented research on the worst forms of child labour including trafficking in children, p. 115 ff, décembre 2002

Source: Terre des hommes

Quelles sont les données à protéger ?

Akachaland et la Licorne

Retour à Akachaland…

Vous **avez pu recueillir des données sur** les enfants et les femmes parmi les survivants et cibler leurs besoins prioritaires. Vous et vos collègues de Licorne, avez désormais accès à ces données.

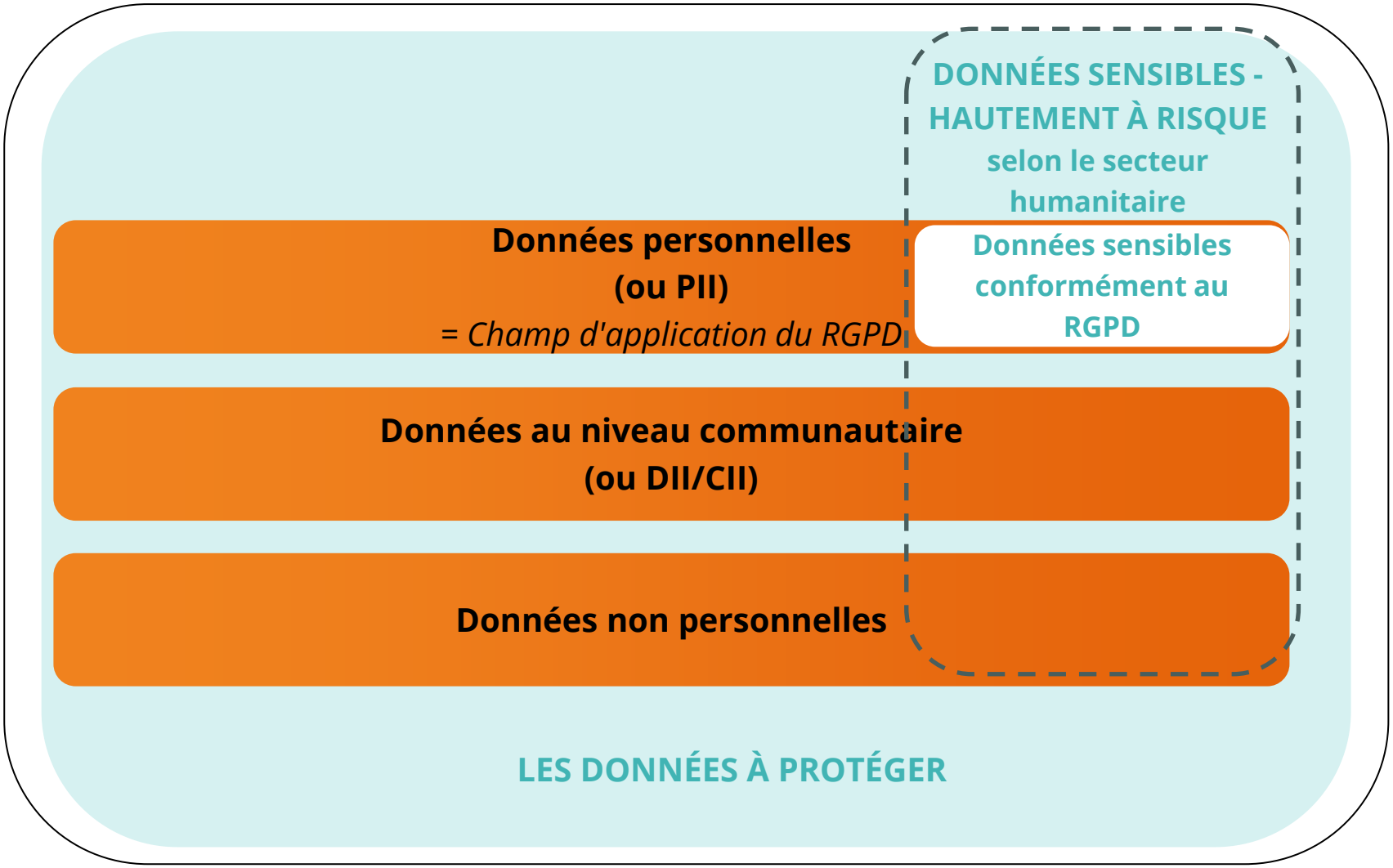
Allez-vous traiter toutes les données de la même manière ? Comment **identifier les données sensibles** parmi toutes les données collectées dans ce contexte ?

Données personnelles sensibles…

Elles nécessitent un **niveau de protection plus élevé** parce que les conséquences de leur utilisation abusive seraient **plus graves, risquant de porter préjudice aux** droits fondamentaux des personnes.

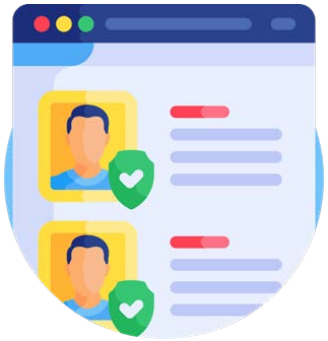
Le CICR déclare :
"La **protection des données personnelles des individus fait partie intégrante de la protection de leur vie**, de leur intégrité et de leur dignité"

… et les données sensibles non personnelles



Source: CartONG

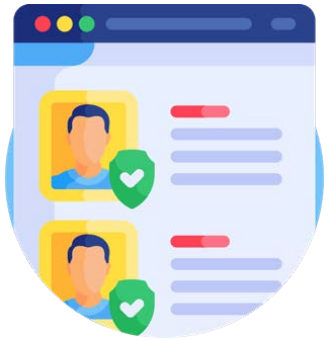
Une autre classification de la sensibilité des données



Information and Data Sensitivity Classification		
Sensitivity	Definition	Information and Data Sensitivity Classification
Low or No	Information or data that, if disclosed or accessed without proper authorization, are unlikely to cause any harm or negative impacts to affected people and/or humanitarian actors.[5]	**Public**
Moderate	Information or data that, if disclosed or accessed without proper authorization, are likely to cause minor harm or negative impacts and/or be disadvantageous for affected people and/or humanitarian actors.	**Restricted**
High	Information or data that, if disclosed or accessed without proper authorization, are likely to cause serious harm or negative impacts to affected people and/or humanitarian actors and/or damage to a response.[6]	**Confidential**
Severe	Information or data that, if disclosed or accessed without proper authorization, are likely to cause severe harm or negative impacts and/or damage to affected people and/or humanitarian actors and/or impede the conduct of the work of a response.[7]	**Strictly Confidential**

Source: Centre des données humanitaires

Une autre classification de la sensibilité des données



Information and Data Sensitivity Classification		
Sensitivity	Definition	Information and Data Sensitivity Classification
Low or No	Information or data that, if disclosed or accessed without proper authorization, are unlikely to cause any harm or negative impacts to affected people and/or humanitarian actors.[5]	Public
Moderate	Information or data that, if disclosed or accessed without proper authorization, are likely to	Restricted
	Information or data that, if disclosed or accessed without proper authorization, are likely to cause severe harm or negative impacts and/or damage to affected people and/or humanitarian actors and/or impede the conduct of the work of a response.[7]	Strictly Confidential

Cependant, il **n'existe pas de classification officielle des données sensibles**, car les données peuvent être sensibles dans un contexte spécifique et ne pas l'être dans un autre, ou peuvent changer au fil du temps. Pour déterminer si des données sont sensibles, il faut procéder à une **évaluation des risques**. (ACF)

Source: Centre des données humanitaires

Discussion en groupe !

En groupe, vous travaillez pour la " Licorne " dans l'Akachaland. Certaines situations issues du terrain impliquent des questions de protection des données.

Prenez le temps d'y réfléchir et de répondre aux questions suivantes

Débriefing de l'exercice

Comment gérer et atténuer les risques ?

Akachaland et la Licorne

Retour à Akachaland...

Il y a quelques années, **le groupe armé " AKaidnappers "** a développé son influence dans les pays de la région. Ce groupe est connu pour se spécialiser dans l'enlèvement d'enfants et utilise des cyber-attaques pour accéder à des données afin de les localiser.
Ils ciblent les communautés du nord, car il s'agissait d'une zone enclavée avant l'inondation et son accès est désormais assez restreint : ils contrôlent une petite partie de la zone. Ils recrutent principalement des enfants au sein de la communauté.

L'accès aux données collectées auprès des 300 enfants et 500 femmes n'est autorisé qu'à certains membres de Licorne.

Quels sont les **principaux risques pour la communauté en ce qui concerne l'accès à la base de données,** y compris les données personnelles ? Quelles mesures pouvez-vous prendre pour prévenir ces risques ?

Quiz

Rappel des définitions indispensables

Qu'est-ce qu'une menace ?

Une menace est tout ce qui peut causer **un préjudice**, **intentionnellement ou non**.

Ex: Utilisation déraisonnable: utilisation de données pour cibler l'assistance en fonction de la situation matrimoniale plutôt que des besoins.

Qu'est-ce qu'un préjudice ?

Tout dommage, préjudice ou **impact négatif -** matériel, immatériel ou économique - subi par une personne ou une organisation et pouvant résulter du traitement des données personnelles. Il s'étend à **tout déni des droits** et libertés **fondamentaux.**

Ex : Préjudices corporels : lésions corporelles, perte de la liberté de mouvement, atteinte à une personne, et autres préjudices matériels ou corporels.

Qu'est-ce qu'un risque ?

Les risques sont l'intersection du préjudice et de la menace et décrivent la **probabilité et l'impact d'**un **événement préjudiciable.**

Ex : Dans le cadre d'une formation sur le VIH, le risque d'inculper les hommes qui y participent sera plus élevé dans un pays hostile à l'homosexualité.

Source: CartONG/Tdh

Comment identifier les risques en matière de protection des données ?

Il est **courant d'effectuer des analyses de risques** dans le secteur humanitaire (par exemple : sécurité).

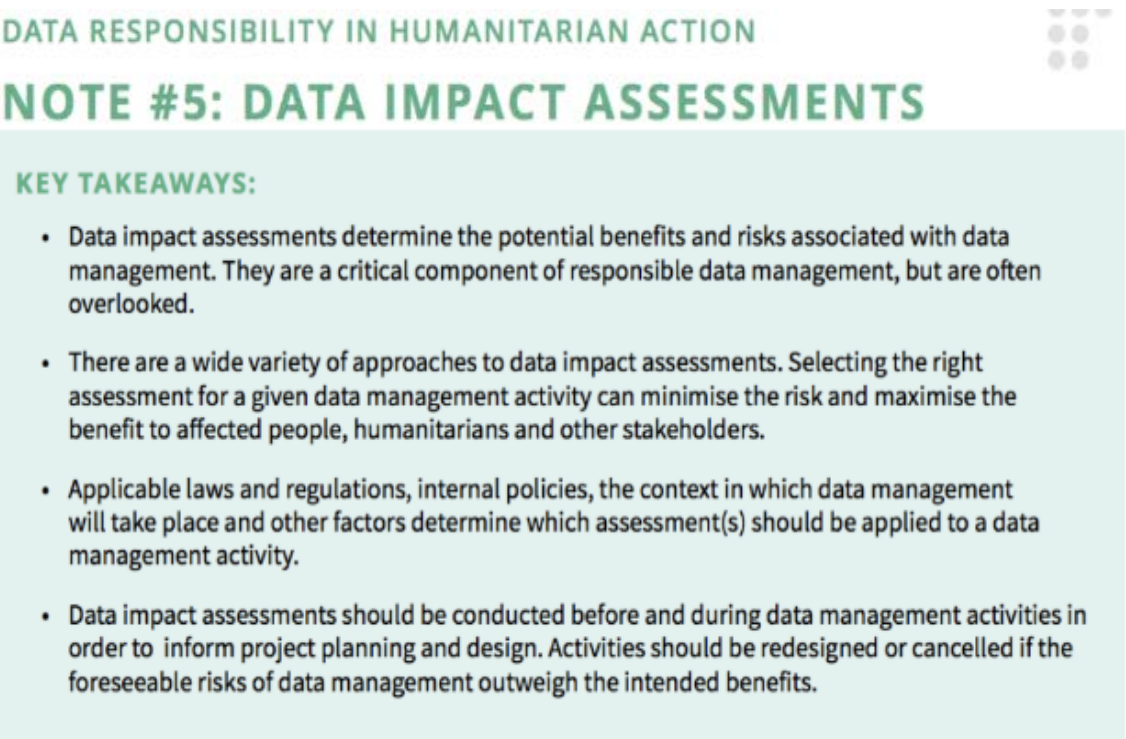
C'est le **même mécanisme** qui devrait être appliqué aux risques liés à la protection des données d'un projet (souvent négligés)

Mieux encore, ils peuvent être **révisés et mis à jour régulièrement.**

Analyse d'impact relative à la protection des données

L'AIPD en français ou le DPIA en anglais- Cet outil aide à :

- **Identifier les risques** et les **mesures d'atténuation** d'un projet ou d'une collecte de données
- **Évaluer la sensibilité des données**



Source: The centre for humanitarian data

Quand faut-il procéder à un DPIA ?

Si un traitement est susceptible d'entraîner un **risque élevé pour les personnes**, en particulier lorsqu'un de ces éléments est présent:

- Données des personnes en **situation de vulnérabilité**
- **Utilisation innovante** des données
- **Données sensibles** ou très personnelles
- Données traitées à **grande échelle**
- Mise en correspondance ou **combinaison d'ensembles de données**
- **Évaluation** ou notation
- **Prise de décision automatisée** avec effet juridique
- Lorsque le traitement des **données** en lui-même "**empêche les personnes concernées d'exercer un droit** ou d'utiliser un service ou un contrat".
- **Suivi systématique**

Quel est le contenu du DPIA ?

Votre DPIA doit

- **décrire la** nature, la portée, le contexte et les finalités du traitement ;
- **évaluer la nécessité**, la **proportionnalité** et les mesures de **conformité ;**
- identifier et évaluer les **risques pour les individus**
- identifier toute mesure supplémentaire visant à **atténuer** ces risques

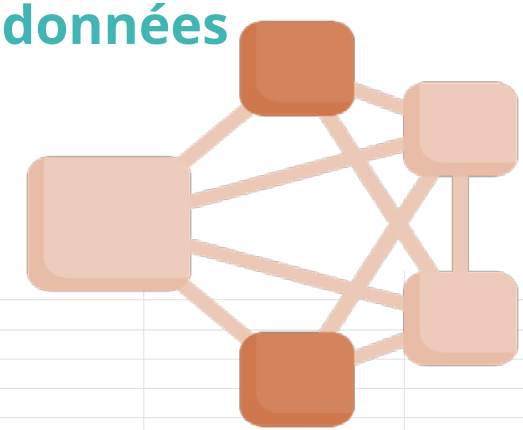
Son **formulaire ou questionnaire peut varier** en fonction de votre organisation

Il s'agit d'une étape clé pour **sensibiliser l'**équipe.

Pour les documenter, un registre de données ?

Le registre des données est un outil qui peut aider votre organisation :

- **documenter les activités de traitement des données**
- de **cartographier les** données personnelles



Voici un exemple (tiré de l'OIC) :

Controller					
Name and contact details		Data Protection Officer (if applicable)		Representative (if applicable)	
Name		Name		Name	
Address		Address		Address	
Email		Email		Email	
Telephone		Telephone		Telephone	

Article 30 Record of Processing Activities									
Business function	Purpose of processing	Name and contact details of joint controller (if applicable)	Categories of individuals	Categories of personal data	Categories of recipients	Link to contract with processor	Names of third countries or international organisations that personal data are transferred to (if applicable)	Safeguards for exceptional transfers of personal data to third countries or international organisations (if applicable)	Retention schedule (i possible)
Finance	payroll	N/A	employees	contact details	HMRC	N/A	N/A	N/A	5 years post employment

Source : The ICO

Témoignage

Comment aborder les différentes législations ?

Akachaland et la Licorne

Retour à Akachaland...

En 2020, **le gouvernement de l'Akachaland** a adopté une loi permettant une **surveillance de masse de** la population, les " Akaidnappers " ayant commencé à recruter parmi les communautés de l'Akachaland. Cette loi impose à toutes les ONG travaillant avec la population, en particulier dans la zone nord, où votre équipe Licorne est active, de partager leurs données.

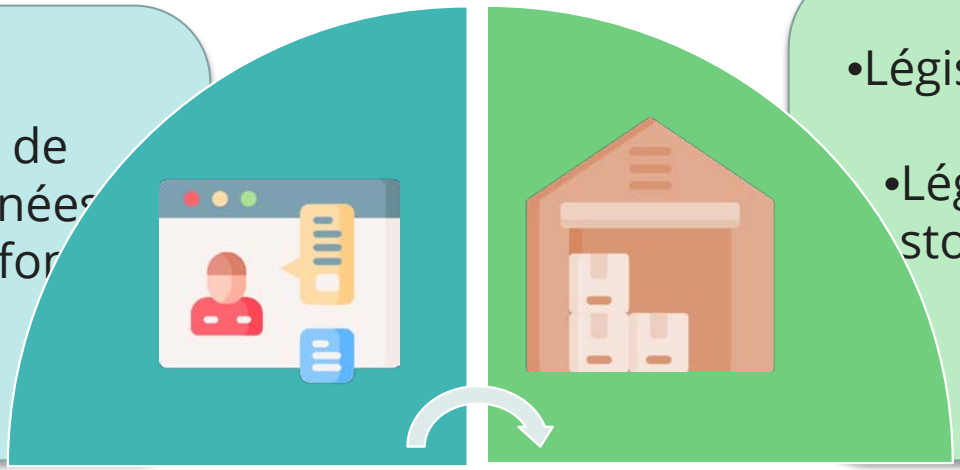
De plus, **votre principal bailleur de fonds de Brajoki** demande toutes les informations détaillées sur les membres de la Licorne, afin de vérifier s'ils.elles figurent sur leur liste de personnes faisant l'objet de sanctions internationales.
Et votre partenaire local spécialisé dans l'assistance médicale, **" Akachaland soins "**, souhaite utiliser votre base de données pour identifier les besoins les plus urgents et fournir une assistance médicale aux communautés.

Comment gérer toutes les demandes, lorsque les données collectées sont personnelles et sensibles ? Comment partager " en toute sécurité " les données ?

Un exemple des différents contextes juridiques et contractuels

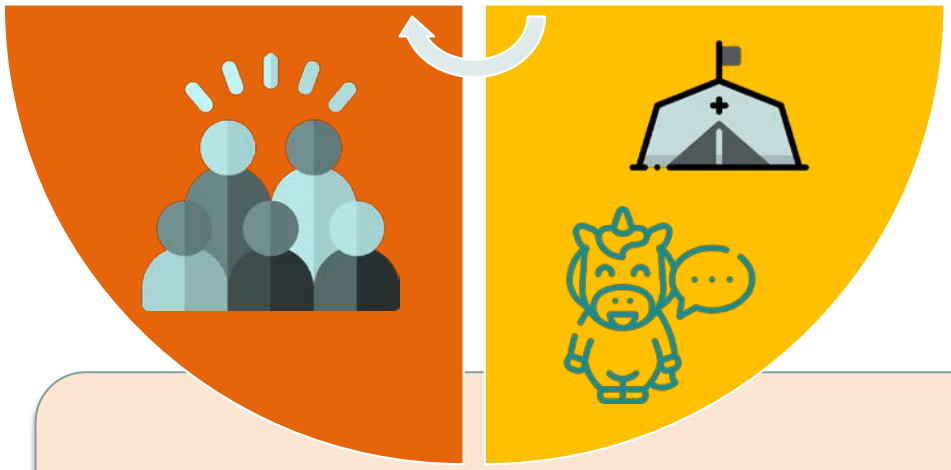
- Mesure complémentaire de transfert de données aux bailleurs de for

Brajoki



•Législation nationale du pays du siège
•Législation du pays de stockage des données

Finobaka

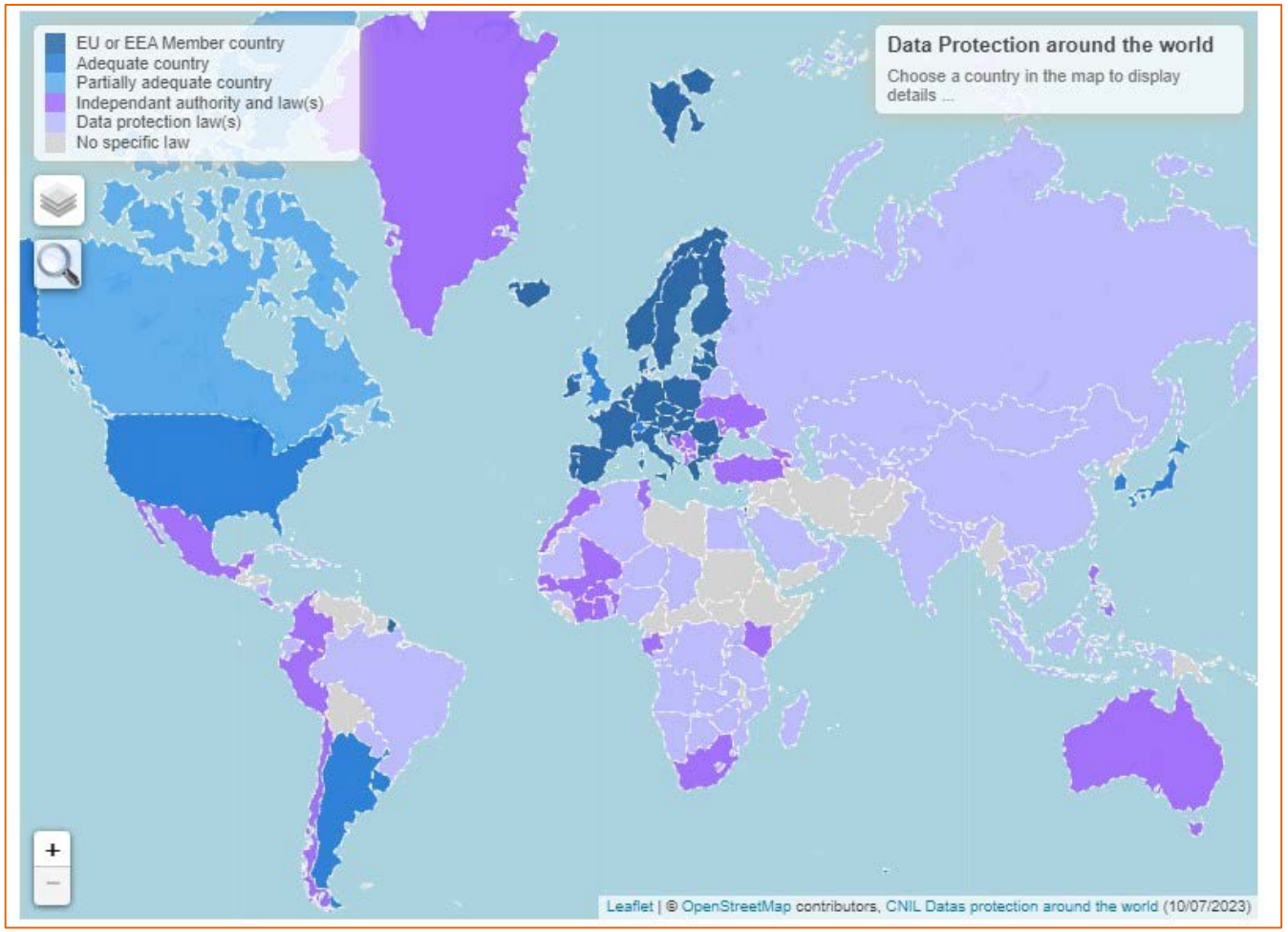


•Législation locale
•Contrats avec les partenaires locaux

Akachaland

Carte mondiale des législations en matière de protection des données

Les législations relatives à la protection des données se développent dans le monde entier, bien que leur contenu et leur **niveau de protection varient**



Source: CNIL

Que faut-il savoir sur le RGPD ?

Les principes et règles du RGPD sont connus comme respectueux de la **législation sur le droit à la vie privée**, dans le secteur humanitaire

En tant qu'organisation, nous croyons fondamentalement au **droit à la vie privée**, indépendamment du texte de la loi. Nous considérons le RGPD comme **complémentaire à notre travail et à nos principes** (OXFAM).

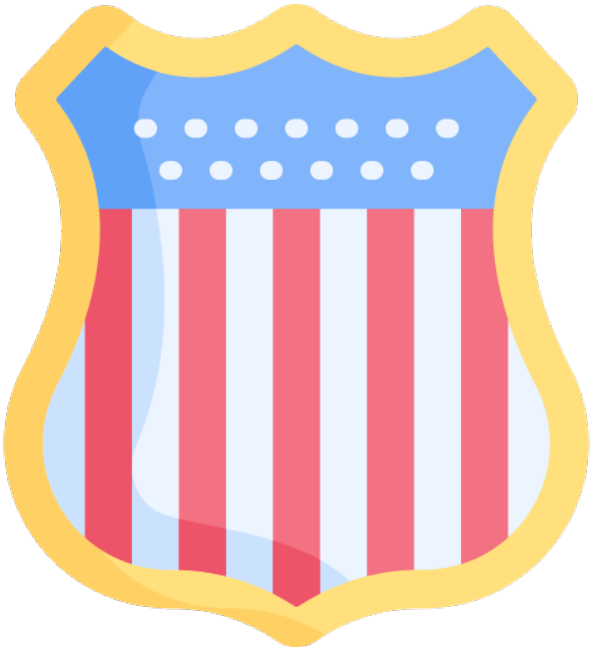
La législation européenne s'applique à :

- **Organisations établies dans l'UE**, quel que soit le lieu du traitement
- Organisations établies en dehors de l'UE qui **ciblent les données des résidents de l'UE**

- " La protection offerte par le **présent règlement devrait s'appliquer aux personnes physiques, quels que soient leur nationalité ou leur lieu de résidence**, en ce qui concerne le traitement de leurs données personnelles " (RGPD).

Que faut-il savoir sur le Cloud Act ?

La législation américaine "Cloud Act" adoptée en 2018 a élargi les conditions permettant au gouvernement américain de **demander des données personnelles, indépendamment de la localisation des données**, par exemple si celles-ci appartiennent à une ONG financée par l'aide américaine



Si une telle demande est faite, vous devez évaluer les conditions du transfert pour juger de sa nécessité et mettre en œuvre des mesures garantissant la protection des données, car le transfert vers les États-Unis n'**est pas conforme aux principes de base de la protection des données.**

Que faut-il savoir sur le Cloud Act ?

La législation américaine "Cloud Act" adoptée en 2018 a élargi les conditions perm
de
pers
loca
si c
fina

Si u
devez évaluer
transfert pour juger de sa nécessité et mettre en œuvre des mesures garantissant la protection des données, car le transfert vers les États-Unis n'**est pas conforme aux principes de base de la protection des données.**

En cas de demande de transfert de données à la Development Data Library de US Aid, il est acceptable d'**anonymiser les données.**

Que faut-il savoir sur le système des Nations unies?

Les Nations unies disposent de **leur propre cadre juridique en matière de protection des données -** il est censé appliquer le même niveau de protection des données que le RGPD

La majorité des agences des Nations unies disposent de lignes directrices et de politiques à l'intention de leurs partenaires chargés de la mise en œuvre, mais **diverses pratiques** sont observées, **parfois de manière** problématique.

Recommandations :

- **Vérifier avec le siège** quelle est la politique de l'organisation
- Soyez attentif,ves aux clauses **avant de signer un contrat**
- Les **renvoyer** à **leur propre politique** si les contrats posent problème.
- Prendre des **mesures de protection supplémentaires** lors du transfert de données

cartong

United Nations

Que faire en cas de violation des données ou de fuite de données ?

Akachaland et Licorne

Retour à Akachaland...

Le groupe armé " AKaidnappers " a pu **pirater votre système** et accéder à certaines données collectées sur le terrain, à partir d'une base de données partagée avec le partenaire local « Akachaland soins ». Ces données contiennent les noms, la localisation, l'âge, les membres de la famille et les dossiers médicaux.

Vous ne découvrez l'attaque que parce qu'un de vos collègues s'est rendu compte il y a deux jours qu'il ne pouvait pas accéder à la base de données concernée. Vous ne connaissez pas encore les circonstances exactes de l'incident, ni le volume et la nature des données piratées.

Quelles sont les **premières mesures que vous prenez dans cette situation** ? Que faites-vous à l'égard de la population ? Comment signaler l'infraction ?

Qu'est-ce qu'une violation ou fuite de données ?

La perte, la destruction, l'altération, l'acquisition ou la divulgation d'informations à des fins accidentelles ou intentionnelles, illégales ou non autorisées, qui **compromettent la confidentialité, l'intégrité et/ou la disponibilité des informations.** (OCHA)

Ex : vous trouvez des informations confidentielles dans un endroit où elles ne sont pas censées être stockées ; votre ordinateur portable, votre téléphone mobile ou un dossier papier contenant des données personnelles a été perdu ou volé (510)

Que faire en cas de violation ou de fuite de données ?

En 2022, une cyberattaque massive contre le CICR - nous pouvons nous inspirer de sa réaction :

- **communiquer sur la violation,** y compris auprès de la population concernée
- évaluer la **gravité de** l'incident, son contexte et sa portée
- **prendre les mesures adéquates** pour atténuer les risques
- **réfléchir aux leçons tirées** pour prendre des mesures préventives

Source: Le CICR

Comment signaler une violation ou fuite de données ?

En cas de violation des données ou de fuite de données, il est éthiquement encouragé (et souvent juridiquement contraignant) de :

- Rapporter l'incident en interne, conformément à vos procédures
- Signaler certains types de **violation des données personnelles à** l'autorité de contrôle compétente dans les **72 heures** après avoir pris connaissance de la violation.
- En cas de risque élevé, informer les **personnes concernées**
- Disposer d'une solide **procédure de détection des violations, d'enquête et de reporting interne.**
- **Conservez un registre de** toute violation des données personnelles, que vous soyez ou non tenu de la notifier.

Questions & réponses

Avez-vous des questions ?

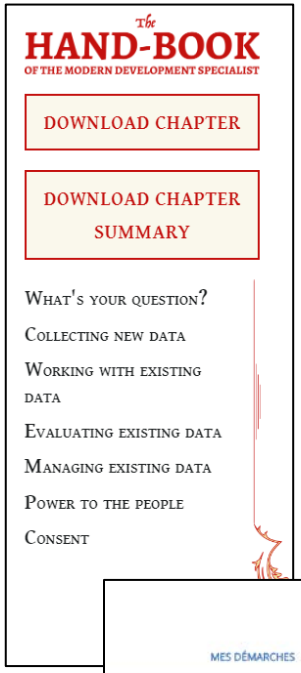
Conclusion

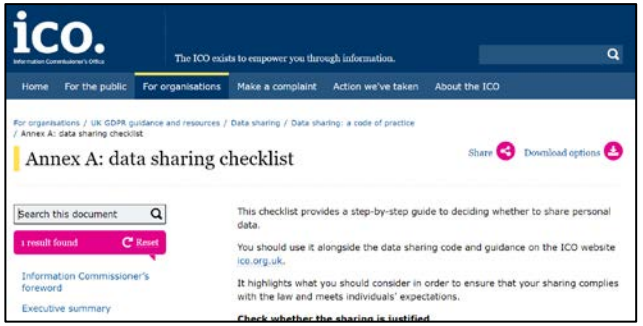
Messages clés

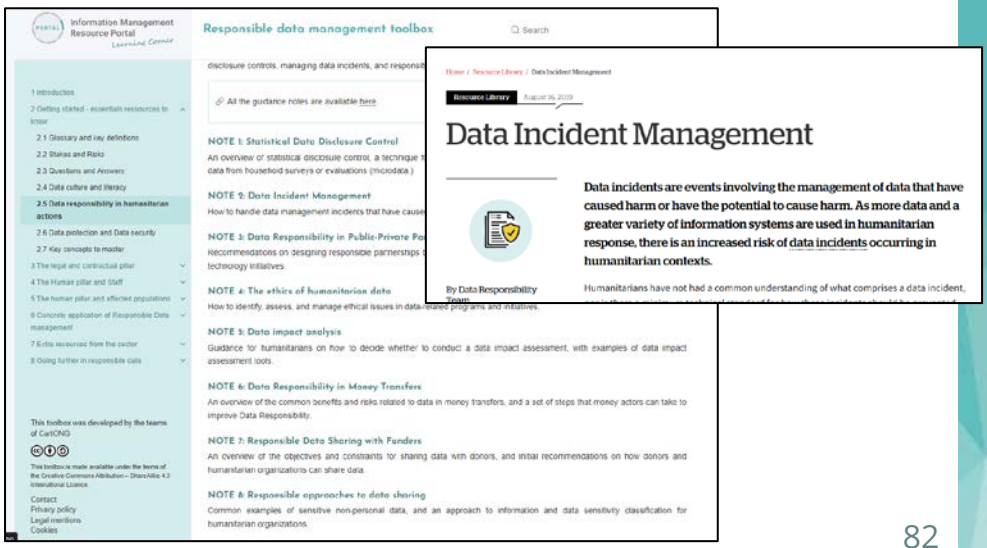
- **La rationalisation de vos besoins en matière de données selon les** principes de "minimisation des données" et de "proportionnalité des données" peut grandement contribuer à simplifier vos pratiques, processus et procédures en matière de données
- **L'évaluation des risques** liés à la collecte de données est essentielle pour respecter pleinement le principe "Ne pas Nuire", afin d'identifier les risques et de prendre des mesures préventives.
- **Interroger votre base légale** pour la collecte des données
- Redevabilité envers les populations concernées : **informer sur les raisons de la collecte de données personnelles**, même lorsque le consentement n'est pas la base légale de la collecte de données (et mieux encore, partager quelques résultats !) .

Les ressources à consulter

Si nous devions sélectionner 5 références clés





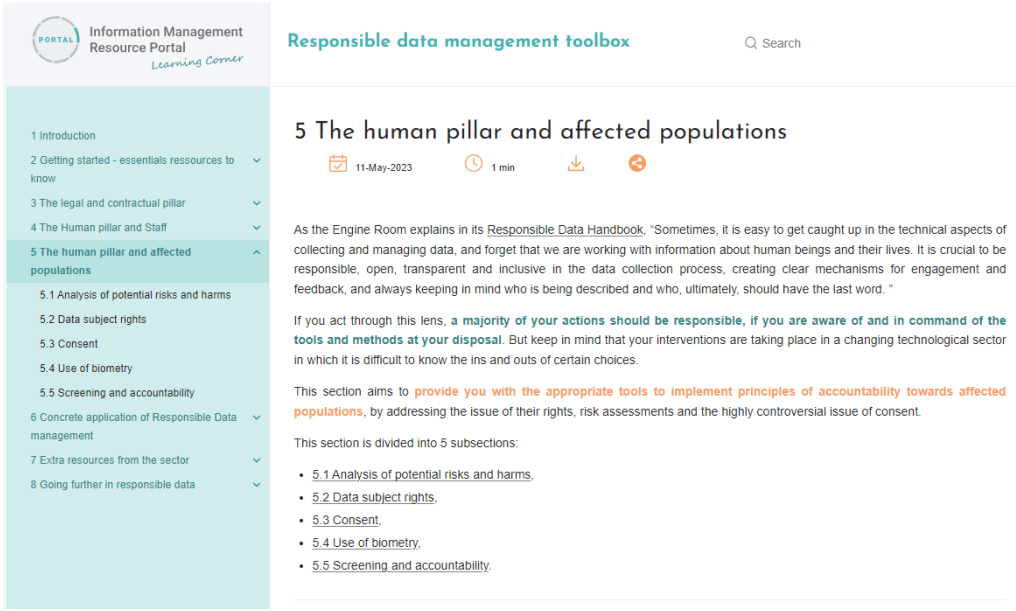


Et la dernière boîte à outils CartONG

Responsible data management

Dive into the responsible data management best practices

Disponible sur https://www.im-portal.org/learning-corner



Les sections 3 & 5 pour la protection des données

Disponible sur https://cartong.pages.gitlab.cartong.org/learning-corner/en/3_legal_contract_RD_page

Devoirs pour la prochaine session

Merci de votre attention !
Des dernières questions?

info@cartong.org

www.cartong.org