# EXPLOITER LE CYCLE DES DONNÉES POUR GÉRER LES DONNÉES DE FAÇON RESPONSABLE

OXFAM

## QU'EST-CE QUE LA GESTION RESPONSABLE DES DONNÉES ?

Ce dépliant oriente quiconque souhaite gérer, partager des données d'un programme ou y accéder afin d'en garantir un traitement responsable tout au long du **cycle de vie des données**.

Il porte principalement sur la gestion responsable des données pendant les crises humanitaires, du point de vue de la collecte des données. Les principes, outils et approches ont toutefois également des applications plus vastes.

La gestion responsable des données exige un traitement respectueux des données collectées et la protection des droits des répondant·e·s (à savoir les personnes dont nous recueillons les données). Par « données », on entend les réponses aux enquêtes, les renseignements fournis à l'inscription, les photos, les témoignages, etc.

La gestion responsable des données n'est pas nécessairement restrictive. Elle peut au contraire renforcer et faciliter la contribution des données pour un travail de grande qualité. Elle doit être envisagée comme un cadre garantissant que les personnes en charge de la collecte des données fassent preuve de sensibilité, rendent des comptes et fassent passer des messages.

Le cadre réglementaire (lois et autres normes) en matière de gestion des données évolue sans cesse, tout comme les technologies de collecte et de gestion des données. Par conséquent, la gestion responsable des données est un processus en constante évolution quant au choix du moment et du mode de collecte des données, ainsi que du mode de gestion des risques.

## 1 PLANIFIER

Définissez clairement l'objectif de la collecte de données.

Les avantages attendus de ces données doivent être proportionnels aux risques. Vous devez être guidé·e par les intérêts et le bien-être de la population affectée.

Évaluez les méthodes et les outils disponibles pour identifier ceux qui sont les mieux adaptés au contexte et à votre objectif.

Limitez le nombre de questions à poser, et déterminez avec soin s'il est indispensable de toutes les poser. Vérifiez que les informations n'ont pas déjà été recueillies par une source fiable.

Avez-vous besoin de protéger les données/**d'évaluer l'impact sur la vie privée** ?

Les **données personnelles** sont très sensibles et requièrent une protection supplémentaire, comme un enregistrement séparé des réponses des répondant·e·s ou l'**anonymisation** de ces données.

Planifiez dès le départ comment garantir un véritable **consentement éclairé**. Expliquez clairement ce que l'on entend par « consentement » et informez les communautés de la finalité des données collectées.

Évaluez le risque de biais lié au ciblage et à la méthodologie. Comment contrôlerez-vous l'exactitude de vos données ?

## 2 ÉVALUER LES RISQUES

Le recueil de données peut exposer certaines personnes à des risques. Évaluez les risques et prenez des mesures pour éviter toute répercussion négative sur les répondant·e·s, par exemple en garantissant la confidentialité et la protection des données.

Faites appel à des experts techniques pour appréhender les risques spécifiques, et élaborez un plan en cas de problème ou d'**atteinte à la protection des données**.

## 3 FORMER LES RECENSEURS/EUSES

Lors de la formation des personnes en charge de la collecte de données :

- Évoquez la gestion responsable des données.
- Passez en revue le processus de consentement. Que devraient savoir les répondant·e·s sur l'exploitation qui sera faite de leurs données ?
- Recourez à des scénarios réalistes pour animer la formation sur les systèmes et les protocoles.

## 4 OBTENIR UN CONSENTEMENT ÉCLAIRÉ

Le consentement ne se résume pas à un formulaire à cocher. Il s'agit de traiter les répondant·e·s avec respect et dignité tout en respectant les exigences légales sur les données personnelles.

Indiquez aux répondant·e·s comment vous allez exploiter leurs données, et dans quel but. Comment seront-elles stockées ? Avec qui seront-elles partagées ? Comment veillerez-vous à ce qu'elles ne soient pas davantage partagées ? Que faire si les répondant·e·s reviennent sur leur consentement ? Comment peuvent-ils vous contacter ?

Demandez aux répondant·e·s s'ils/elles souhaitent recevoir un retour sur votre utilisation de leurs données, et sous quelle forme.

Indiquez aux répondant·e·s qu'ils/elles peuvent se retirer, et élaborez un « plan B » le cas échéant.

## 5 GÉRER LES DONNÉES

### TRANSFERT

Restez vigilant lorsque vous utilisez des appareils portables et des technologies de partage. **Chiffrez** au besoin et paramétrez des systèmes qui permettent d'éliminer à distance toutes les données d'un téléphone.

Pour les processus papier, redoublez de vigilance lorsque vous voyagez sur le terrain avec des documents imprimés. Chiffrez les fichiers numériques dès le point de saisie des données.

### ACCÈS

Concernant les droits d'accès aux sources de données numériques, créez des comptes individuels sécurisés par des mots de passe utilisateur. Dressez la liste des personnes devant accéder aux données et identifiez les données concernées.

Chaque personne recueillant ou utilisant des données doit gérer ces données de façon responsable. Une approche consiste à confier la protection des données à un membre de l'équipe et à s'assurer que tous les autres membres comprennent leur rôle et leurs responsabilités.

## STOCKAGE

Examinez avec soin les caractéristiques du stockage sur le cloud et des options de base de données en matière d'emplacement et de protection des données.

Pour le recueil de données sur papier, réfléchissez à des options de stockage sûres. Si possible, stockez-les dans un coffre ou un placard sous clé.

## PARTAGE

Convenez d'un **accord de partage des données** avec les organisations avec lesquelles vous échangez des données, notamment sur les directives à suivre en matière de traitement des données. Sollicitez des conseils juridiques, au besoin.

Ces principes s'appliquent quel que soit le tiers : État, autre ONG, entreprise privée, banque, etc.

Ne partagez pas les données si vous n'avez pas obtenu le consentement des répondant·e·s.

Certaines organisations diffusent ouvertement les données. Sollicitez des conseils d'experts ou évaluez les risques et les sensibilités avant de communiquer tout **ensemble de données**. Le retrait des noms ne suffit pas à masquer les identités.

## 6 FAIRE BON USAGE DES DONNÉES

Les applications sont variées : lobbying, plaidoyer ou ajustements apportés à des programmes.

Pensez aux personnes représentées dans les données. Avez-vous tenu compte de la parité entre les femmes et les hommes ?

Y a-t-il un biais dans la décision prise, d'après les données recueillies ?

## 7 PROPRIÉTÉ ET RETOUR

Comment promouvoir le fait que les répondant·e·s sont propriétaires de leurs données ?

Échangez avec les répondant·e·s pour valider les résultats et assurez-vous que les données concordent avec leurs points de vue lorsque la situation le permet. Informez-les de ce qu'il est advenu de leurs données.

## 8 CONSERVATION/SUPPRESSION

Statuez systématiquement sur la période de conservation des données. Leur pertinence s'étiole très rapidement.

La suppression d'un document numérique n'a rien à voir avec l'incinération ou le déchiquetage de documents papier, car votre ordinateur conserve des traces numériques de vos documents (par exemple, dossiers de téléchargement, archives, etc. On parle de « rémanence des données »).

## PETIT LEXIQUE

**Anonymisation** En théorie, cela implique de rendre difficile ou impossible toute identification d'une personne à partir d'un ensemble de données. Mais dans la réalité, des fragments de données peuvent souvent être regroupés pour révéler des identités.

**Atteinte à la protection des données** Communication (intentionnelle ou non) d'informations dans un environnement non approuvé.

**Cycle de vie des données** Flux d'informations dans un système, de la création à la suppression, en passant par le stockage.

**Ensemble de données** Recueil de données associées.

**Accord de partage des données** Cadre pour le partage de données qui définit le mode de transmission, de stockage et d'utilisation des données.

**Chiffrement** Conversion des données dans un format empêchant les personnes non autorisées d'en prendre connaissance.

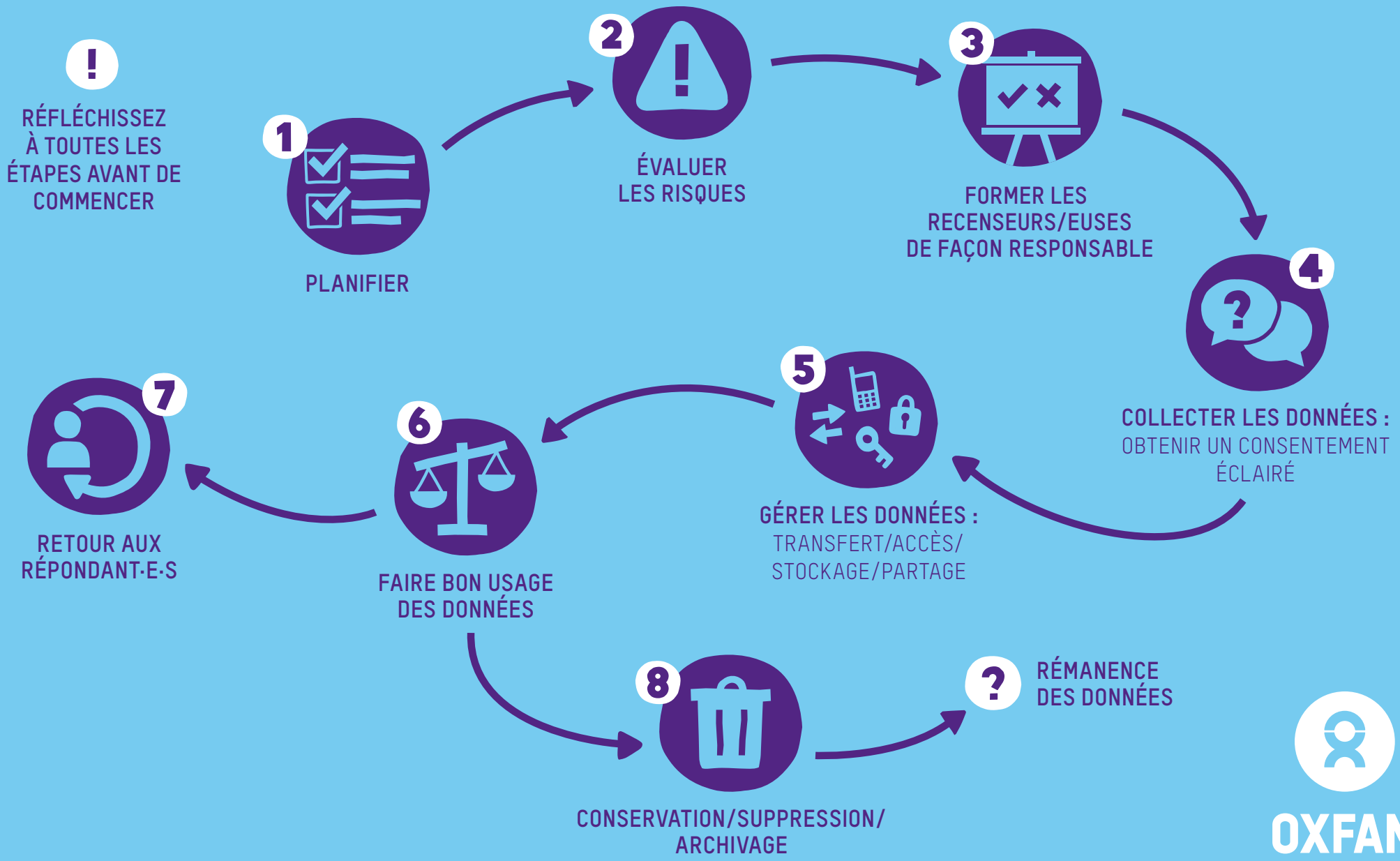
**Consentement éclairé** Accord libre et volontaire se basant sur une appréciation et une compréhension claires des faits, implications et futures conséquences d'une action. Les personnes doivent être informées de leur droit de refuser d'accorder leur consentement, et pouvoir faire valoir ce droit. Dans certains cas, le consentement n'est pas possible, par exemple avec des enfants ou des personnes handicapées.

**Données personnelles** Informations pouvant être utilisées en l'état ou associées à d'autres informations pour identifier une personne.

**Évaluation de l'impact sur la vie privée** Outil permettant d'identifier et de réduire les risques d'atteinte à la vie privée.

Pour plus d'informations…
www.oxfam.org.uk/responsibledata

# LE CYCLE DE DONNÉES RESPONSABLE




OXFAM