Brouillon de travail v2 - mai 2025
Préparé par le Data Responsibility Working Group

Responsabilité des données dans la réduction rapide de la taille ou la fermeture des opérations

La perte et l'exposition des données opérationnelles[1] sont des risques critiques qui ne sont souvent pas pris en compte lors d'une réduction rapide de l'échelle ou de la fermeture des opérations. La perte de données opérationnelles peut avoir un effet néfaste sur la capacité à planifier, prioriser, répondre, suivre et rapporter efficacement, ainsi qu'à mener un plaidoyer éclairé par des preuves et une mobilisation des ressources. L'exposition de données sensibles peut nuire aux personnes concernées, aux communautés d'accueil et au personnel humanitaire, et peut entraver les organisations humanitaires dans leurs activités humanitaires.

Le Groupe de travail sur la responsabilité des données (DRWG) a préparé cette liste pour les situations de réduction rapide ou de fermeture des opérations, basée sur les directives opérationnelles de l'IASC sur la responsabilité des données dans l'action humanitaire. Cette liste vise à aider à éclairer les décisions concernant la conservation interne des données pour une utilisation future, leur publication sur des plateformes externes, leur transfert à un tiers ou leur destruction.

Les organisations qui réduisent ou éliminent progressivement les opérations impliquant la gestion des données humanitaires doivent décider de la manière dont les données opérationnelles seront gérées, y compris les données numériques et analogiques.
Ces décisions doivent éviter de nuire et être fondées sur les politiques organisationnelles, notamment celles concernant la protection des données, la sécurité, la rétention et l'archivage. Les décisions doivent être guidées par les principes de responsabilité des données, en utilisant des approches centrées sur les personnes axées sur la maximisation des bénéfices et la minimisation des risques. Plus précisément, ces décisions doivent viser à :

1. Évitez l'exposition de données personnelles et de données sensibles non personnelles
2. Protéger la disponibilité continue des données, sur la base d'un objectif défini et spécifique
3. Comprendre l'impact sur d'autres opérations ou programmes, notamment si des protocoles de partage d'informations ou des accords de partage de données sont en place
4. Informer les partenaires, autorités et autres utilisateurs de données des évolutions de la qualité, de la disponibilité et de l'accès des données
5. Informer les personnes concernées du transfert, de la conservation ou de la destruction de leurs données personnelles
6. Permettre au personnel restant de maintenir la prestation des services et la continuité des activités, ou de réduire la prestation de services de manière responsable
7. Permettre un éventuel « scale-up » et un réengagement à l'avenir

Les données personnelles doivent toujours être gérées conformément aux politiques et législations organisationnelles applicables. Consultez des points de référence juridiques, de sécurité de l'information ou de protection des données afin d'éclairer les décisions concernant la conservation, le transfert ou la destruction des données et pour naviguer dans les exigences

[1] Données relatives au contexte d'une crise, aux besoins et vulnérabilités des personnes concernées, ainsi qu'aux activités des acteurs humanitaires impliqués dans la réponse.

applicables en matière de localisation et de protection des données.

Utilisez les étapes suivantes pour éclairer la prise de décision concernant la gestion des données lors d'une réduction rapide ou de la fermeture des opérations :

1. **Identifier les données gérées dans l'opération**
   Développez un aperçu des activités de gestion des données dans l'opération, par exemple un registre de gestion des données. Cette présentation doit clairement indiquer les activités pour lesquelles les données personnelles sont traitées.

2. **Évaluer la pertinence opérationnelle**
   Examinez les données gérées dans l'opération et déterminez quelles données sont pertinentes pour le travail de votre organisation et/ou de vos partenaires. Par exemple, les données peuvent être nécessaires en interne pour la continuité opérationnelle ou à des fins d'audit, partagées pour une utilisation par les gouvernements ou partenaires spécifiques, ou publiquement partagées pour un usage général en soutien à la réponse globale.

3. **Évaluer la sensibilité des données**
   Considérez la probabilité et l'impact de préjudice pour les personnes concernées, les communautés d'accueil et le personnel humanitaire en cas d'exposition accidentelle ou intentionnelle des données, ainsi que l'impact potentiel sur l'organisation et ses partenaires. Si disponible, consultez le protocole de partage d'information pour le contexte de réponse afin de déterminer le niveau de sensibilité des différents types de données et de jeux de données.

4. **Évaluer la capacité interne à conserver les données de manière responsable et à garantir la disponibilité continue des données**
   Identifiez la disponibilité de modalités de stockage ou d'archivage sécurisées et durables au sein de votre organisation, en notant que celles-ci doivent être adaptées au niveau de sensibilité des données. Examinez les autorisations d'accès pour empêcher l'accès non autorisé aux données et systèmes, et examinez la possibilité de révoquer l'accès, et assurez-vous que les données soient toujours disponibles pour ceux qui en ont besoin pour une raison précise.

5. **Évaluer la capacité des partenaires ou autres acteurs à recevoir, stocker et gérer les données de manière responsable**
   Déterminez si les partenaires peuvent être en mesure de prendre en charge la gestion de données spécifiques, y compris leur réception, leur stockage et leur destruction sécurisés. Déterminez si les données doivent être partagées en versions brutes ou propres, ou anonymisées avant le transfert.

6. **Sur la base des étapes 1 à 5, décidez pour chaque activité de gestion des données si les données doivent être conservées, publiées, transférées ou détruites.**

a. Conservation

Si les données sont opérationnellement pertinentes et que l'infrastructure appropriée est disponible pour les maintenir en toute sécurité, envisagez la conservation des données. Fixez une période de conservation initiale et déterminez l'emplacement géographique du stockage (selon le cas). Identifiez l'infrastructure de stockage et mettez en place des mesures de sécurité appropriées ainsi que des autorisations d'accès aux données.

b. Publication

Si les données sont opérationnellement pertinentes mais qu'il est difficile de maintenir l'accès, envisagez de les publier sur une plateforme externe. Des données utiles et non sensibles peuvent être publiées via des plateformes telles que HDX ou Reliefweb afin d'assurer leur disponibilité continue.

c. Transfert

Si les données peuvent être utilisées par d'autres à des fins spécifiques, envisagez de les transférer à un ou plusieurs partenaires. Avant de transférer des données sensibles, déterminez si des canaux sécurisés sont disponibles pour partager ces données, si des accords de partage de données existent si nécessaire, et si les partenaires ont la capacité de gérer les données en toute sécurité. Le cas échéant, assurez-vous que les droits d'accès aux systèmes et outils de gestion des données (par exemple, les autorisations de gestion de projet dans les outils de collecte de données) soient transférés, tout en assurant l'accès pour la surveillance et la supervision.

d. Destruction

Si les risques liés à la rétention, à la publication ou au transfert de données l'emportent sur les bénéfices, envisagez la destruction. Avant de détruire des données, consultez les politiques organisationnelles applicables sur l'archivage et la rétention, et envisagez de créer une version agrégée pouvant être conservée, publiée ou transférée. Assurez-vous qu'il existe une justification claire à la destruction des données, documentez-la et utilisez un outil qui rend la recherche des données impossible.

7. **Révision de l'accès et de la gestion des accréditations**

Veillez à ce que l'accès soit examiné et limité au personnel nécessaire. Révisez les identifiants d'accès aux données, restreignez ou supprimez les droits d'accès pour les personnes partant, ou élargissez les droits d'accès à ceux qui devront remplir plusieurs rôles simultanément (« double-hatting ») en raison de cette réduction rapide. Les collègues doivent gérer de manière proactive les changements dans les droits d'accès en:

a. Identifiant les systèmes où les qualifications seront affectées par les changements de présence et de niveau de personnel et/ou de responsabilités;
b. Créant une liste consolidée des changements d'accès nécessaires par système;
c. Identifiant un point focal responsable de la gestion et du suivi des changements de certification, et d'escalader tout problème qui survient.

8. **Mise à jour des systèmes de suivi des activités**
   Mettez à jour les systèmes de suivi des activités pour indiquer quelles activités sont réduites ou arrêtées. Cela influencera la communication avec les personnes affectées qui consomment ces services (voir ci-dessous). Elle aide également à évaluer et à suivre l'impact des coupes budgétaires, fournissant des données sur les lacunes critiques pour le plaidoyer et la mobilisation des ressources.

9. **Communiquez avec les personnes concernées**
   Lorsque vous communiquez sur la réduction ou la fermeture des opérations aux personnes affectées, incluez une information sur ce qui arrivera aux données personnelles lorsque cela est possible. Par exemple, « Les données collectées dans le cadre de ce projet seront conservées pendant 3 ans à compter de la suspension du projet » ou « Les données liées à ce projet seront détruites et ne seront pas partagées en dehors de notre organisation ». Dans la mesure du possible, les personnes affectées doivent avoir la possibilité de demander la suppression de leurs données personnelles, conformément aux politiques organisationnelles ou à la législation applicable.

Contactez le Data Responsibility Working Group pour entrer en contact avec d'autres organisations humanitaires afin de connaître les meilleures pratiques en matière de responsabilité des données dans le contexte d'une réduction rapide ou de fermeture des opérations.