

NOTE D'ORIENTATION: LA RESPONSABILITÉ DES DONNÉES ET LA REDEVABILITÉ AUX PERSONNES AFFECTÉES

POINTS CLÉS :

- La responsabilité des données est la gestion sécurisée, éthique et efficace des données personnelles et non personnelles pour la réponse opérationnelle, et est un élément indispensable de la redevabilité aux personnes affectées (AAP) dans le système humanitaire.
- Les activités de gestion de données relatives à l'AAP incluent, par exemple, la communication avec les communautés, le traitement de plaintes et de feedback, et le suivi des perceptions des communautés.
- La collecte de données auprès des communautés et à leur sujet peut permettre de mieux comprendre les priorités et les préférences des personnes affectées, ainsi que de les faire davantage participer à l'action humanitaire et se l'approprier.
- Toutefois, la gestion des données liées à l'AAP peut engendrer des risques, notamment la divulgation de données sensibles pouvant nuire aux personnes touchées ou aux travailleurs humanitaires, et la perte de confiance entre les personnes touchées, les organisations humanitaires et les acteurs concernés.
- Les acteurs humanitaires doivent mener des analyses de l'impact relative aux données, assurer la responsabilité des données par conception, développer des diagrammes de la gestion des données, entretenir le registre de gestion de données, mettre en place des accords de partage des données, et adopter des procédures de gestion des incidents liés aux données.

INTRODUCTION

La redevabilité envers les personnes affectées ("AAP") est une approche collective qui a pour objectif de garantir que les besoins et les intérêts des personnes sont au centre de l'action humanitaire. Elle se fonde sur l'engagement de prendre en compte, de rendre compte et de se faire tenir pour compte par les personnes que les humanitaires cherchent à aider.¹ Dans le cadre de leurs activités liées à l'AAP, les humanitaires collectent et utilisent de plus en plus de données. La gestion responsable des données est essentielle pour garantir que ces activités ne nuisent pas aux personnes affectées, et fait partie du respect des engagements liés à l'AAP.

Cette note d'orientation examine la responsabilité des données et l'AAP dans le cadre de l'action humanitaire. Elle identifie les avantages et les risques courants liés aux données dans le cadre de ses activités liées à l'AAP, explique comment les humanitaires peuvent mettre en œuvre les actions des directives opérationnelles de l'IASC sur la responsabilité des données dans l'action humanitaire et propose des exemples d'approches conjointes à ce travail.

¹ Pour plus d'informations sur l'AAP, voir: [OCHA: Accountability to affected people](#).

LA GESTION DES DONNÉES RELATIVES À L'AAP

Par le biais de l'AAP, les humanitaires visent à garantir que l'action humanitaire protège et préserve les droits et la dignité des personnes affectées par les crises, qu'elle reste pertinente et efficace, qu'elle ne laisse personne de côté et qu'elle respecte les principes humanitaires.² Reconnaissant que les personnes touchées par une crise vivent l'aide différemment, l'AAP permet aux humanitaires de travailler avec les personnes affectées pour s'assurer que leurs divers besoins, vulnérabilités et capacités sont pris en compte dans la prise de décision et la conception des programmes.

Les humanitaires s'acquittent de cette tâche principalement par le biais des activités suivantes :

- En fournissant systématiquement aux populations et aux communautés des informations opportunes, pertinentes et exploitables sur la réponse humanitaire, ses acteurs et ses activités.
- En soutenant la participation significative et le leadership des personnes affectées dans la prise de décision, indépendamment de leur sexe, de leur âge, de leur statut de handicapé et d'autres diversités.
- En veillant à ce que des mécanismes de feedback communautaire soient en place pour permettre aux personnes affectées d'évaluer et de faire des observations sur la performance de l'action humanitaire, et de déposer des plaintes sur n'importe quel sujet, y compris des sujets sensibles tels que la protection, la violence basée sur le genre, l'exploitation et les abus sexuels, la fraude, la corruption, le racisme et la discrimination, les violations de l'environnement, et d'autres.

Les organisations humanitaires utilisent de plus en plus les canaux numériques pour travailler avec les communautés. Par conséquent, de grandes quantités de données peuvent être collectées et utilisées, ce qui nécessite une gestion appropriée. La responsabilité des données, c'est-à-dire la gestion sécurisée, éthique et efficace des données personnelles et non personnelles pour la réponse opérationnelle, est essentielle à ces efforts.³ Veiller à ce que les activités de gestion des données⁴ ne nuisent pas aux personnes affectées fait partie du respect des engagements liés à l'AAP.

Les activités courantes de gestion des données relatives à l'AAP sont notamment les suivantes :

- La communication avec les communautés qui consiste à fournir des informations opportunes et pertinentes.
- Les mécanismes de collecte, d'analyse, de renvoi et d'action des plaintes et du feedback.
- Les systèmes de suivi des perceptions des communautés, des rumeurs, des informations erronées, de la désinformation et des discours haineux ("MDH").
- Les activités de gestion de l'information pour éclairer la fourniture et la coordination de l'aide, y compris les évaluations et analyses conjointes des besoins, les enquêtes de perception, et la cartographie de la présence et des activités des partenaires dans différents lieux.
- L'analyse de l'écosystème des informations⁵ pour déterminer la relation entre l'offre et la demande d'informations aux communautés et en provenance de celles-ci.

² [Déclaration des Directeurs du Comité permanent inter-organisations \(IASC\) sur la responsabilité à l'égard des populations touchées dans le cadre de l'action humanitaire.](#)

³ [Directives opérationnelles du Comité Permanent Inter-agences \(IASC\) sur la Responsabilité des données dans l'action humanitaire \(2023\).](#)

⁴ Une activité de gestion des données est toute activité impliquant la gestion de données et d'informations dans le cadre d'une réponse humanitaire. Cela comprend la conception de l'activité, ainsi que la collecte, la réception, le stockage, l'assurance qualité, l'analyse, le partage, l'utilisation, la conservation et la destruction des données et des informations par les acteurs humanitaires. [Directives opérationnelles du IASC sur la Responsabilité des données dans l'action humanitaire \(2023\).](#)

⁵ L'analyse de l'écosystème des informations cherche à capturer toutes les dimensions de la relation entre l'offre et la demande d'informations. Pour plus d'informations, voir: [Internews, Information Ecosystem Analysis - A Human-Centered Approach \(2021\).](#)

Une approche responsable de la gestion des données consiste à comprendre comment ces activités sont liées les unes aux autres et comment les données circulent entre les individus, les communautés et les organisations.⁶

AVANTAGES ET RISQUES LIÉS AUX ACTIVITÉS DE GESTION DES DONNÉES RELATIVES À L'AAP

La responsabilité des données repose sur une compréhension et un équilibre des avantages et des risques liés à la gestion des données. Bien qu'ils puissent varier d'un contexte à l'autre, nous présentons ci-dessous plusieurs avantages et risques courants aux activités de gestion des données relatives à l'AAP.

Avantages :

- Une meilleure compréhension des priorités et des préférences des personnes affectées, telles que les canaux qu'elles préfèrent pour recevoir et soumettre des informations.
- Une amélioration de la participation et de l'appropriation de l'action humanitaire par les personnes touchées.
- Une meilleure efficacité de l'action humanitaire grâce à la prise en compte des observations de la communauté.
- Une amélioration de la transparence et de la redevabilité.

Risques :

- L'exposition accidentelle ou intentionnelle de données sensibles, personnelles ou non, qui pourrait entraîner la réidentification, des représailles, la stigmatisation, la violence ou d'autres formes de préjudice pour les personnes affectées.
- L'utilisation potentiellement abusive des données à des fins non humanitaires. C'est le cas, par exemple, lorsqu'un fournisseur de logiciels commerciaux qui propose un canal de communication communautaire utilise l'historique des discussions pour poursuivre ses propres objectifs commerciaux.
- Une analyse biaisée aboutissant à une prise de décision inadéquate. Cela peut se produire lorsque des données non représentatives provenant d'enquêtes de perception sont utilisées pour tirer des conclusions au niveau des réponses.
- Des occasions manquées pour utiliser les données disponibles lorsque les efforts ne sont pas coordonnés, ce qui peut entraîner la fatigue de la collecte de données de la part des communautés et des personnes affectées qui doivent raconter à nouveau les mêmes histoires difficiles.
- La perte de confiance entre les personnes affectées, les organisations humanitaires et les autres acteurs lorsque des données sensibles sont divulguées.

ACTIONS RECOMMANDÉES POUR LA RESPONSABILITÉ DES DONNÉES DANS LE CADRE DE L'AAP

La responsabilité des données nécessite la mise en œuvre d'actions à différents niveaux d'une réponse humanitaire, conformément aux directives opérationnelles du IASC. Le Centre for Humanitarian Data ("le Centre") recommande les actions suivantes pour soutenir la responsabilité des données dans le cadre de l'AAP :

⁶ Pour plus d'informations, voir [Centre for Humanitarian Data's Tip Sheet on Understanding Data Ecosystems](#).

- **Mener des analyses de l'impact relative aux données**
- **Assurer la responsabilité des données par conception**
- **Développer des diagrammes de la gestion des données**
- **Entretenir le registre de gestion de données**
- **Mettre en place des accords de partage des données**
- **Adopter des procédures de gestion des incidents liés aux données**

Mener des analyses de l'impact relative aux données

Une **analyse de l'impact relative aux données**⁷ (AID) vise à déterminer les impacts anticipés d'une activité de gestion des données et aide à identifier les recommandations permettant d'atténuer les impacts négatifs potentiels. De nombreuses activités de gestion des données relatives à l'AAP impliquent la gestion de données sensibles personnelles et non personnelles, ou impliquent l'utilisation de nouveaux outils numériques. C'est pourquoi les organisations doivent effectuer une analyse de l'impact relative aux données avant d'entamer une activité afin de déterminer si celle-ci est réalisable de manière responsable.

Assurer la responsabilité des données dès la conception

La responsabilité des données dès la conception signifie que l'on identifie les moyens de garantir une gestion sécurisée, éthique et efficace des données. Toutes les mesures relatives à la responsabilité des données doivent être énoncées dans une **procédure opérationnelle standard** (POS) claire et reproductible. Cette procédure doit préciser les rôles et les responsabilités des parties prenantes, les outils et les processus de gestion des données, les mesures visant à empêcher l'exposition de données sensibles et les termes clairs relatifs à la conservation et à la destruction des données. En outre, elle doit préciser la finalité de la gestion des données, y compris, mais sans s'y limiter, le consentement éclairé, et spécifier les mesures à prendre pour faire respecter les droits des personnes concernées. Lors de l'élaboration d'une procédure opérationnelle standard, il convient de consulter l'analyse de l'impact relative aux données pour l'activité concernée afin d'élaborer des mesures d'atténuation des risques appropriées, réalisables et solides.

Développer des diagrammes de la gestion des données

Un **diagramme de la gestion des données** permet de comprendre visuellement une activité et peut aider à identifier les lacunes en matière de partage de données, de dispositions légales, d'infrastructures ou d'orientations.

Entretenir le registre de gestion de données

Un **registre de gestion des données** fournit un résumé des principales activités de gestion des données menées par les différents acteurs dans le contexte de la réponse, y compris les données gérées dans le cadre de ces activités. Le registre doit indiquer le niveau de sensibilité de chaque type de données et s'aligner sur les classifications de sensibilité des données et des informations qui existent pour la réponse, le cas échéant.⁸ Il doit être mis à jour de façon continue par le mécanisme interagences concerné (par exemple, le groupe de travail AAP).

⁷ Pour plus d'informations, voir [Note d'orientation sur les analyses de l'impact relatives aux données](#).

⁸ Une classification de la sensibilité des données et des informations fait partie d'un protocole de partage de l'information (PPI), qui constitue le principal document de référence régissant le partage des données et des informations dans le cadre de la réponse. La classification indique le niveau de sensibilité des différents types de données et d'informations dans un contexte donné. Il s'agit d'un élément clé du PPI, qui doit être élaboré collectivement par les différentes parties prenantes afin qu'elles s'accordent sur ce qui constitue des données sensibles dans leur contexte.

Mettre en place des accords de partage des données

Avant de partager des données personnelles ou très sensibles, les organisations doivent établir un **accord de partage des données** ("Data Sharing Agreement", DSA). Cet accord définit les conditions qui régissent le partage de données personnelles et de données non personnelles sensibles entre deux ou plusieurs parties. Vérifiez si le partage des données est soumis à un cadre spécifique en matière de protection des données (par exemple, si l'un des partenaires est soumis à une législation nationale). Dans ce cas, l'accord doit respecter les exigences prévues par le cadre applicable en matière de protection des données, y compris les droits et les demandes des personnes concernées. Un accord n'est parfois pas nécessaire si des clauses spécifiques sur le partage des données sont incluses dans des accords généraux, tels que des protocoles d'accord et des contrats de service.

Adopter des procédures de gestion des incidents liés aux données

Les incidents liés aux activités dans le cadre de l'AAP comprennent l'exposition de données ("violation de données") qui pourrait entraîner des rétorsions, la stigmatisation, la violence ou d'autres formes de nuisance pour les personnes affectées, ainsi que l'utilisation abusive des données des personnes affectées à des fins autres qu'humanitaires. La gestion des incidents liés aux données fait référence aux processus et aux outils permettant d'identifier, de résoudre, de suivre et de communiquer sur les incidents liés aux données.⁹ Il s'agit d'un élément clé de la gestion transparente et responsable des données, qui peut contribuer à prévenir de futurs incidents. Les organisations doivent établir une **procédure opérationnelle standard pour la gestion des incidents liés aux données**, ainsi qu'un registre pour assurer le suivi des incidents liés aux données et de leur traitement. Lorsque l'incident constitue une violation de données à caractère personnel, les organisations doivent s'acquitter des obligations prévues par le règlement sur la protection des données et par les accords de partage de données applicables. Ces obligations peuvent inclure la fourniture d'informations sur la violation aux personnes dont les données personnelles ont été exposées.

Étude de cas en Afghanistan: La responsabilité des données dans l'AAP

Suite au décret des autorités de facto de décembre 2022 interdisant aux femmes afghanes de travailler pour des ONG, le IASC a établi des critères minimaux pour la programmation, y compris des engagements solides en matière de l'AAP. Le groupe de travail AAP (AAP WG) a lancé la plateforme '**Afghanistan Community Voices and Accountability Platform**' afin d'aider les humanitaires à recueillir, analyser et répondre en temps utile aux feedbacks des communautés dans leurs interventions en Afghanistan.

Compte tenu de la sensibilité des données partagées sur la plateforme collective, le groupe de travail AAP a pris des mesures pour garantir la responsabilité des données dès la conception. Il a notamment procédé à une analyse d'impact relative aux données afin d'identifier et d'atténuer les risques liés aux données, et a établi une procédure opérationnelle normalisée ("SOP") pour la gestion des données par tous les partenaires concernés. Cette procédure précise qu'aucune donnée personnelle ne doit être stockée sur la plateforme. Elle prévoit également des mesures visant à garantir que la gestion des données au sein de la plateforme ne nuit pas, et promeut l'égalité et la non-discrimination. À cette fin, une analyse collective des plaintes et du feedback reçus des communautés touchées est effectuée, et les principales conclusions sont présentées de manière neutre et impartiale. Le SOP s'inspire du **protocole de partage d'informations**, en vigueur au niveau du système pour l'Afghanistan, qui a été approuvé par l'équipe humanitaire de pays en mai 2023.

Étude de cas en Syrie : Responsabilité des données dans la gestion du feedback des communautés

Le groupe de travail AAP a élaboré des diagrammes de gestion des données afin de guider l'extension de la ligne verte. Ces diagrammes visualisent le flux de données et d'informations entre les différents acteurs concernés. Cela a permis au groupe de travail AAP d'identifier les points à améliorer dans le traitement des données relatives aux plaintes et au feedback.

⁹ Pour plus d'informations sur la gestion des incidents liés aux données, voir: **Note d'orientation sur la gestion des incidents liés aux données** (2019).

Ces modifications seront intégrées dans un SOP pour la ligne verte commune, qui s'appuiera sur les bonnes pratiques de la ligne verte existante du PSEAH. Les mesures relatives à la responsabilité des données comprendront la restriction de l'accès aux données sensibles, l'obligation d'utiliser des canaux cryptés pour le transfert des données et la définition d'un calendrier de conservation et de destruction des données sensibles une fois qu'elles ne sont plus nécessaires à la réalisation de l'objectif de la ligne verte.

Les organisations sont encouragées à partager leur expérience en matière de promotion de la responsabilité des données dans la conception et l'exécution des activités liées à l'AAP via centrehumdata@un.org.

Le **Centro for Humanitarian Data** (ci-après dénommé le « Centre »), en collaboration avec des partenaires clés, publie une série de notes d'orientation sur la Responsabilité des données dans l'action humanitaire au cours de 2022 et 2023. La série de notes d'orientation fait suite au travail initié en 2019 et 2020. Elle complète aussi les **Directives opérationnelles du IASC sur la Responsabilité des données dans l'action humanitaire** (révisées en 2023) et les **Consignes de OCHA sur la Responsabilité des données** (octobre 2021). Par le biais de cette série, le Centre vise à fournir des orientations supplémentaires sur des questions, des processus et des outils spécifiques pour la Responsabilité des données dans la pratique. Les notes d'orientation et les fiches de conseil publiés en 2022-2023 sont rendus possible grâce au généreux soutien du gouvernement de la Suisse.



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Foreign Affairs FDFA