

SÉRIE DE NOTES D'ORIENTATION

LA RESPONSABILITÉ DES DONNÉES DANS L'ACTION HUMANITAIRE

APPROCHES RESPONSABLES EN MATIÈRE DE PARTAGE DES DONNÉES

POINTS CLÉS :

- Un partage ouvert de données à jour et précises est indispensable à l'efficacité de la réponse humanitaire. La façon dont les organisations humanitaires abordent le partage des données est directement liée à la confiance et à la coopération dans le secteur.
- À mesure que l'écosystème de données humanitaires se développe, les opportunités et les risques liés au partage des données deviennent plus clairs, ce qui incite les entreprises à explorer des approches de partage plus limitées.
- Les organisations humanitaires reconnaissent largement la sensibilité des données personnelles : l'exposition de telles données est fortement susceptible d'entraîner diverses formes de préjudice. La majorité des données non personnelles peuvent être partagées ouvertement en toute sécurité, mais ces dernières peuvent également être sensibles et doivent être traitées avec prudence.
- Les organisations humanitaires doivent prendre en compte quatre facteurs lorsqu'elles décident de partager ou non des données non personnelles : (i) l'utilité ; (ii) la sensibilité ; (iii) la capacité humaine et technique ; et (iv) la gouvernance.
- Les organisations humanitaires doivent identifier et comparer toutes les approches disponibles pour le partage des données, en considérant d'abord l'approche la plus ouverte et en travaillant à des approches plus restrictives si nécessaire.

INTRODUCTION

L'utilisation et l'échange de données sont devenus des fonctions essentielles des organisations humanitaires. Les membres du personnel doivent régulièrement décider de partager ou non les données de leur organisation, même si leur rôle n'est pas principalement axé sur la gestion des données ou de l'information. Au-delà des organisations individuelles, le désir de partager et d'utiliser les données générées dans l'action humanitaire s'est également amplifié. En réponse à cela, le secteur humanitaire a connu une augmentation de la production et du partage des données au cours des dernières années.

« Des données exactes sont la clé de voûte d'une bonne politique et d'un bon processus décisionnel. Obtenir ces données et les répartir entre des centaines d'organisations, au milieu d'une urgence humanitaire, est compliqué et prend du temps - mais c'est absolument crucial. »

- Antonio Guterres, Secrétaire Général des Nations Unies, lors de l'inauguration du Centre for Humanitarian Data à La Haye en décembre 2017

Un partage ouvert de données à jour et précises est indispensable à l'efficacité de la réponse humanitaire et doit rester un objectif clé pour le secteur. Par exemple, les données épidémiologiques sur la COVID-19¹ compilées et partagées quotidiennement par le Johns Hopkins University Center for Systems Science and Engineering ont été intégrées dans un certain nombre de tableaux de bord et de rapports de situation pour les décideurs du secteur humanitaire depuis le début de la pandémie. En décembre 2020, ce jeu de données avait été téléchargé plus de 320 000 fois depuis la plateforme d'échange Humanitarian Data Exchange (HDX) depuis sa première publication en janvier de la même année. L'utilité des données ouvertes pour les praticiens humanitaires est également soulignée par le fait que l'utilisation de HDX dans les pays ayant un Plan de Réponse Humanitaire (« Humanitarian Response Plan » ou « HRP » en anglais) en place a augmenté beaucoup plus rapidement que son utilisation dans d'autres endroits.²

La façon dont les organisations humanitaires abordent le partage des données est directement liée à la confiance et à la coopération dans le secteur. Le maintien de la confiance au sein de l'écosystème des données est essentiel à la durabilité du partage des données, et porte sur des questions telles que la qualité, le niveau auquel les données seront sécurisées après le partage et l'utilisation responsable des données par le destinataire. Comme les données dans le secteur humanitaire concernent souvent les populations les plus exposées au risque, la gestion et le partage de ces données justifient la prudence.

De nombreuses organisations humanitaires ont élaboré ou mis à jour leurs directives, leur gouvernance et leurs pratiques pour soutenir différents aspects de la Responsabilité des données : la gestion sécurisée, éthique et efficace des données. Le secteur a en outre constaté une multiplication des efforts collaboratifs visant à améliorer la Responsabilité des données au-delà des organisations individuelles.³ Néanmoins, à mesure que le système humanitaire apprend davantage sur les risques associés au partage des données, les organisations doivent faire face à des défis plus complexes en partageant ces données de manière responsable.⁴

La présente note d'orientation vise à faciliter la prise de décisions concernant le partage de données non personnelles dans les milieux humanitaires. Elle explique la sensibilité des données, fournit des exemples courants de données sensibles non personnelles, et détaille l'approche adoptée en matière de classification de la sensibilité des informations et des données dans les milieux humanitaires. Elle offre également un cadre que les organisations peuvent utiliser pour peser quatre facteurs qui aident à déterminer si les données peuvent être partagées et explique les approches courantes pour le faire de manière responsable.

Options pour le partage de données sur la plateforme Humanitarian Data Exchange

Lorsque la plateforme Humanitarian Data Exchange (HDX) a été lancée en 2014, elle regroupait près de 900 jeux de données, partagés par une poignée d'organisations « précurseurs ». À la fin de 2020, ce chiffre était passé à plus de 18 000 jeux de données. Seules des organisations approuvées ont la possibilité de partager des données sur la plateforme. Elles peuvent mettre les données à la disposition de toute personne qui visite le site ou en privé uniquement à des membres de leur organisation.

En 2017, l'équipe HDX a ajouté une autre option pour le partage des données : HDX Connect. Cette fonction permet aux organisations de publier uniquement les métadonnées, les données sous-jacentes étant disponibles sur demande. Si l'accès est accordé, les données sont partagées bilatéralement sans passer par la plateforme HDX. Par exemple, Ground Truth Solutions utilise HDX Connect pour fournir un accès aux données COVID-19 recueillies en Irak via l'outil Community Perceptions.

¹ Accédez aux [nouvelles données sur les cas de Coronavirus \(COVID-19\) sur HDX](#).

² « Entre août 2016 et août 2020 (période pour laquelle les données sont disponibles), la croissance des utilisateurs mensuels des pays ayant un Plan de réponse humanitaire (HRP+) a été de 943 %, contre 566 % dans l'ensemble des pays. » De l'[étude de cas HDX](#), septembre 2020.

³ Il s'agit, par exemple, du sous-groupe du Comité permanent interorganisations (IASC) sur la Responsabilité des données dans l'action humanitaire, de l'initiative Protection Information Management et de l'initiative Responsible Data for Children, entre autres.

⁴ Pour une meilleure compréhension du défi auquel sont confrontées les organisations humanitaires lors du partage de données spécifiquement dans les situations d'urgence humanitaires prolongées, voir [ALNAP, Data Collection, Analysis and Use in Protracted Humanitarian Crises](#), juin 2020.

Dans le cadre de son processus d'assurance qualité, l'équipe HDX effectue également une évaluation des risques de divulgation sur toute ressource contenant des microdonnées ajoutée à la plateforme. L'équipe HDX le fait parce qu'il peut être possible de réidentifier des personnes ou d'exposer des informations confidentielles même après que les identifiants directs ont été supprimés des microdonnées.⁵

Certaines des organisations utilisant HDX se sont davantage orientées vers un accès contrôlé à leurs données, soit en raison de la nature sensible des données, de la pression accrue pour suivre et rendre compte de la manière dont les données sont utilisées, soit en raison des contraintes de ressources liées à la soutenabilité opérationnelle. HDX prendra toujours en charge différentes méthodes de partage des données. Cependant, le libre accès reste la meilleure option pour la majorité des données générées en matière de réponse humanitaire.

COMPRENDRE LA SENSIBILITÉ DES DONNÉES

Les organisations humanitaires reconnaissent largement la sensibilité des données personnelles⁶ : l'exposition de telles données est fortement susceptible de nuire et d'entraîner diverses formes de préjudice. Cette compréhension est encore peu répandue au niveau des données non personnelles, qui couvrent généralement les trois catégories suivantes dans les environnements humanitaires :

1. Des données sur le contexte dans lequel une intervention a lieu (par exemple les cadres juridiques, les conditions politiques, sociales et économiques, les infrastructures, etc.) et la situation humanitaire (par exemple, les incidents de sécurité, les risques de protection ou les facteurs à l'origine de la situation ou de la crise).
2. Des données sur les populations affectées par la situation et leurs besoins, les menaces et les vulnérabilités auxquelles elles sont confrontées et leurs capacités.
3. Des données sur les acteurs de l'action humanitaire et leurs activités (par exemple, comme rapporté en 3W/4W/5W).

La plupart de ces données peuvent être partagées ouvertement en toute sécurité. Toutefois, les données non personnelles peuvent également être sensibles. Des exemples de données sensibles non personnelles comprennent des données sur les groupes victimes de violences basées sur le genre ou sur la localisation de minorités ethniques dans des situations des zones de conflit. De telles données sont considérées comme sensibles car elles permettent d'identifier des groupes d'individus via des facteurs déterminants sur le plan démographique, tels que l'origine ethnique, le genre, l'âge, la profession, l'appartenance religieuse ou le lieu d'origine. Les données non personnelles peuvent également être sources de risques d'autres manières, par exemple en exposant l'emplacement des structures médicales dans des zones où elles sont particulièrement susceptibles d'être attaquées. À mesure que la prise de conscience des risques associés au partage de ces données continue de croître, certaines organisations sont en train d'évoluer d'une focalisation sur les données ouvertes vers un partage plus contrôlé.

De nombreuses organisations ont des classifications de la sensibilité des informations et des données (voir la figure 1 ci-dessous) qui définissent quelles données entrent dans quelle catégorie de sensibilité afin de faciliter une gestion responsable des données. Ces classifications peuvent également être élaborées en tant qu'exercice collectif pour aider les organisations à s'aligner sur ce qui constitue des données sensibles dans leur contexte, et à identifier les méthodes appropriées de divulgation ou de diffusion pour différents types de données en fonction de leur sensibilité.

⁵ Pour en savoir plus sur le processus d'atténuation des risques pour les microdonnées du Centre, le « Contrôle de la divulgation statistique » ou CDS, consultez le [Learning Parcours pédagogique sur le sujet](#).

⁶ Les données personnelles ne doivent pas être partagées ouvertement et la gestion de ces données doit toujours être conforme aux lois nationales et régionales sur la protection des données ou aux politiques internes de protection des données dans le cas des organisations qui bénéficient des privilèges et immunités.

Classification de la Sensibilité des Informations et Données		
Niveau de sensibilité	Définition	Classification
Faible	Informations ou données dont la divulgation ou l'accès non-autorisé ne sont pas susceptibles d'engendrer du préjudice ou un impact négatif sur les populations affectées et/ou les acteurs humanitaires.	Publique
Modérée	Informations ou données dont la divulgation ou l'accès non-autorisé sont susceptibles d'engendrer du préjudice ou un impact négatif mineurs sur les populations affectées et/ou les acteurs humanitaires.	Limitée
Elevée	Informations ou données dont la divulgation ou l'accès non-autorisé sont susceptibles d'engendrer du préjudice ou un impacts négatif important sur les populations affectées et/ou les acteurs humanitaires et/ou du dommage à la réponse humanitaire.	Confidentielle
Sévère	Informations ou données dont la divulgation ou l'accès non-autorisé sont susceptibles d'engendrer du préjudice ou un impacts négatif sévères sur les populations affectées et/ou les acteurs humanitaire et d'entraver le bon déroulement de la réponse.	Strictement Confidentielle

Figure 1. Exemple de classification de la sensibilité des informations et des données⁷

Les politiques organisationnelles et les instruments de gouvernance collective tels que les protocoles de partage de l'information (PPI) incluent souvent une classification de la sensibilité, et devraient être les principales références pour déterminer la façon dont gérer les données sensibles. Toutefois, ces documents restent discrets sur l'opportunité et la manière de les partager. Cela signifie que le partage des données peut être influencé par des préférences et des compétences personnelles pouvant varier selon les organisations. En adoptant une approche plus cohérente du partage des données et en mettant en œuvre les protections adéquates pour les données sensibles, les organisations peuvent instaurer la confiance et contribuer à une action humanitaire plus efficace.

QUATRE FACTEURS POUR DÉTERMINER S'IL FAUT PARTAGER DES DONNÉES NON PERSONNELLES

Il y a quatre facteurs que les organisations humanitaires doivent prendre en compte lorsqu'elles décident de partager ou non des données non personnelles.

1. Quelle est l'utilité des données pour les autres parties prenantes ?

L'utilité des données dépend du niveau de détail, du nombre de personnes ou de la zone géographique couverte, de leur actualité et de leur pertinence pour l'analyse et la prise de décisions dans la réponse humanitaire. Réaliser une analyse d'impact relative aux données pour aider à définir l'utilité de données spécifiques.⁸

2. À quel point les données sont-elles sensibles ?

La sensibilité des données est fondée sur le risque associé à leur exposition dans un contexte particulier.⁹ Dans certains contextes de réponse, les organisations, les clusters/secteurs et les structures de coordination à l'échelle du système ont également établi des classifications de sensibilité des données et des informations (voir ci-dessus) qui peuvent éclairer cette qualification.

⁷ Consignes de OCHA sur la Responsabilité des données.

⁸ Voir la note d'orientation sur les analyses d'impact relatives aux données.

⁹ Pour la gestion des données dans le secteur humanitaire, on peut définir le risque par la probabilité et l'impact des préjudices découlant de la gestion des données.

La réalisation d'une analyse d'impact relative aux données peut également aider à déterminer la sensibilité des données. Pour les résultats d'enquêtes et d'autres formes de microdonnées, la sensibilité est étroitement liée au risque de réidentification, qui peut être déterminé en réalisant une évaluation du risque de divulgation.

3. Quelles sont les capacités humaines et techniques des organisations qui partagent et utilisent les données ?

L'organisation qui partage les données et l'organisation qui les reçoit et les utilise doivent avoir une capacité humaine et technique suffisante pour une gestion responsable des données, ce qui signifie : la disponibilité du personnel, la diffusion de la culture des données, l'infrastructure technique et les ressources associées. Dans les environnements à faible connectivité, les méthodes de partage de données nécessitant une forte bande passante peuvent ne pas être appropriées. Pour les contextes présentant des risques de sécurité connus, les données doivent généralement être partagées via des approches plus restreintes.

4. Quels instruments de gouvernance s'appliquent ?

Les instruments courants de gouvernance des données comprennent les PPI, les accords de partage de données pour le partage bilatéral,¹⁰ et les licences ou les conditions d'utilisation pour le partage public de données.¹¹ Ces instruments doivent éclairer la façon dont les données sont partagées de manière sécurisée, éthique et efficace. Dans certains cas, une gouvernance devra être développée spécifiquement pour l'approche choisie. Les instruments de gouvernance peuvent couvrir une large gamme de sujets et de dispositions particulières, mais doivent toujours inclure les éléments suivants : (a) l'objectif et la portée du partage ; (b) les éventuelles limites à la façon dont les données doivent être gérées après le partage ; (c) les rôles et responsabilités tout au long du processus de partage ; et (d) les procédures de gestion des incidents liés aux données.¹²

IDENTIFIER ET COMPARER LES APPROCHES

Les organisations doivent définir la meilleure approche en matière de partage de données en fonction des quatre facteurs ci-dessus. Ces approches vont du partage ouvert pour maximiser les bénéfices des données, à des approches plus limitées comme le partage bilatéral des données ou le seul partage des informations issues des données. Le tableau ci-dessous donne un aperçu des différentes approches du partage de données et offre des exemples de plateformes et d'outils couramment utilisés.

Approches, outils et plateformes pour le partage des données dans l'action humanitaire ¹³				
Approches de partage	Libre accès Partager publiquement des données reste l'approche la plus ouverte, permettant un accès sans médiation à quiconque le souhaite.	Accès limité La limitation de l'accès aux données permet quand même à certains partenaires d'utiliser les données tant qu'ils répondent à certaines exigences.	Partage bilatéral Le partage bilatéral est la façon la plus limitée de partager les données, directement avec un seul partenaire.	Aucun partage de données Les données qui ne doivent pas être partagées peuvent toujours avoir de la valeur pour les partenaires, tant qu'ils sont autorisés à les interroger à distance ou à en bénéficier indirectement.
Outils et plateformes communs	Plateformes de données d'organisations HDX Open Listservs	HDX Private UNHCR Microdata Library ¹⁴ IFRC GO ¹⁵ Cluster/secteur Listes de diffusion fermées	HDX Connect Email ¹⁶ Dropbox	OPAL ¹⁷ Aircloak ¹⁸ Chiffrement homomorphe ¹⁹ Calcul multipartite ²⁰

¹⁰ Le Forum économique mondial, en collaboration avec Washington University Centre for Information Assurance and Cybersecurity, le Sustainable Development Solutions Network TReNDS et le NYU GovLab, ont commencé à créer un dépôt d'accords de partage de données pour soutenir la professionnalisation de cette pratique par le biais de leur projet de contrats de collaboration : [Contracts for Data Collaboration \(C4DC\)](#).

¹¹ Les licences recommandées pour le partage de données via HDX sont répertoriées ici : <https://data.humdata.org/about/license>.

¹² Pour plus d'informations sur la gestion des incidents liés aux données dans le cadre de l'action humanitaire, consultez notre [Note d'orientation sur la gestion des incidents liés aux données](#).

En comparant ces différentes approches, considérez toujours l'approche la plus ouverte en premier et travaillez vers des approches plus limitées si nécessaire. Différents types de données nécessitent différents modes de partage. Par exemple, les fichiers de données volumineux nécessitent une infrastructure spécialisée et les interfaces de programmation d'applications (API) sont adaptées aux données publiées régulièrement dans le même format. Comme les technologies de partage des données continuent d'évoluer, les organisations doivent régulièrement revoir et comparer les approches disponibles.

Rendre disponible la valeur des données sans les partager : L'approche de l'interrogation

Une approche relativement nouvelle de l'utilisation des données sans transférer les données elles-mêmes est « l'interrogation », ou « querying » en anglais. L'interrogation permet à des tiers de formuler des questions spécifiques à poser sur les données sans y accéder directement. Le détenteur des données peut alors vérifier la sensibilité des informations ainsi que tout autre problème potentiel. Cette approche évite les transferts de données qui peuvent poser des problèmes juridiques et éthiques, tout en permettant d'utiliser des informations précieuses pour le bien commun.

Dans la mise en œuvre d'une approche d'interrogation, il est essentiel d'établir une gouvernance sous la forme d'instructions et de limites concernant les requêtes afin d'empêcher la récupération d'informations sensibles en posant une combinaison de questions.²¹ La vérification des utilisateurs ainsi que de leurs questions doit toujours constituer une étape clé dans le processus autour de ce type d'approche.

Parmi les solutions commerciales permettant de mettre en place des approches d'interrogation, citons Aircloak Insights, qui sert de « proxy entre les analystes et les données sensibles avec lesquelles ils doivent travailler ». Un autre outil d'interrogation est la plateforme **Open Algorithms** (OPAL). Cet outil a été spécialement développé pour les secteurs humanitaire et de développement et est actuellement mis à l'essai en Colombie.

Méthodes de partage des données au Joint IDP Profiling Service

En 2019, le **Joint IDP Profiling Service** (JIPS) a reçu une subvention du Fonds d'innovation du HCR pour étudier des méthodes scientifiques pour l'anonymisation des données. Le JIPS a étudié des méthodes telles que le calcul multipartite et le chiffrement homomorphe, et a travaillé avec des experts techniques au Laboratoire de Physique appliquée de l'université John Hopkins, Flowminder et au bureau national des statistiques du gouvernement de Colombie.

En étroite collaboration avec Flowminder et en s'appuyant sur leur **Flowkit**, JIPS a développé une approche d'interrogation prototype pour permettre aux acteurs humanitaires et de développement d'accéder et d'interroger en toute sécurité des données sensibles au niveau individuel sans avoir à les partager. L'équipe a développé un flux de travail technique pour démontrer la viabilité de cette approche avec un seul fournisseur de données et a mis en évidence les problèmes et les limitations dans le cas de plusieurs fournisseurs de données.

Les organisations sont encouragées à partager leur expérience en matière de promotion du partage responsable des données avec le Centre for Humanitarian Data via centrehumdata@un.org.

¹³ Not all tools and platforms in this overview have been vetted by the UN Secretariat. Always consult the relevant Information Technology advisors before using a new tool.

¹⁴ Bibliothèque de microdonnées du HCR.

¹⁵ Plateforme GO de la FICR.

¹⁶ Dans le cadre d'interventions humanitaires, l'un des moyens les plus courants de partager des données est l'envoi de pièces jointes par e-mail. Lorsque vous partagez des données par e-mail, prenez toujours les précautions de sécurité nécessaires. Cette façon de partager est responsable dans certains cas, mais il existe souvent des moyens plus appropriés de partager des données. Pour plus d'informations sur le cryptage des emails, reportez-vous à la section suivante par exemple : <https://www.cloudwards.net/how-to-encrypt-your-emails/>.

¹⁷ The Open Algorithms Project.

¹⁸ Aircloak Insights.

¹⁹ Pour en savoir plus sur le chiffrement homomorphe comme méthode de partage de la valeur des données sensibles, consultez : <https://www.microsoft.com/en-us/research/project/homomorphic-encryption/> and here : <https://www.wired.com/story/google-private-join-compute-database-encryption/>.

²⁰ Pour en savoir plus sur le calcul multipartite, veuillez consulter : <https://www.tno.nl/en/focus-areas/information-communication-technology/roadmaps/data-sharing/secure-multi-party-computation/>.

²¹ Pour une explication de ce risque, voir par exemple : <https://www.usenix.org/conference/usenixsecurity19/presentation/gadotti>.

CONTRIBUTEURS : JOINT IDP PROFILING SERVICE (JIPS).

Le **Centre for Humanitarian Data** (ci-après dénommé le « Centre »), en collaboration avec des partenaires clés, publie une série de huit notes d'orientation sur la Responsabilité des données dans l'action humanitaire au cours de 2019 et 2020. La série de notes d'orientation fait suite à la publication du **project de directives opérationnelles sur la responsabilité des données du Bureau de la coordination des affaires humanitaires des Nations Unies** en mars 2019. 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. Cette série est rendue possible grâce au généreux soutien de la Direction générale de protection civile et opérations d'aide humanitaire européennes (DG ECHO).

La traduction de ces notes a été facilitée par CartONG grâce au soutien du Ministère français de l'Europe et des Affaires Etrangères.