

PARTAGE RESPONSABLE DES DONNÉES AVEC LES BAILLEURS DE FONDS

POINTS CLÉS :

- Le partage des données sensibles, qu'elles soient personnelles ou non personnelles, sans garanties adéquates peut exacerber les risques pour les populations affectées par une crise, les organisations humanitaires et les bailleurs de fonds.
- Les bailleurs de fonds demandent régulièrement des données aux organisations qu'ils financent afin de s'acquitter de leurs obligations et de leurs objectifs. Certaines de ces demandes concernent des informations et des données sensibles qui doivent être protégées afin d'atténuer les risques.
- Parmi les objectifs courants pour le partage des données avec les bailleurs de fonds, on peut citer : (i) l'absence de cadre réglementaire pour la gestion responsable des données sensibles non personnelles ; (ii) les lacunes en matière de capacité ; et (iii) la limitation de la finalité.
- Parmi les contraintes courantes liées au partage des données avec les bailleurs de fonds, on peut citer : for responsibly managing sensitive non-personal data; (ii) capacity gaps; and (iii) purpose limitation.
- Les bailleurs de fonds et les organisations humanitaires peuvent prendre les mesures suivantes pour minimiser les risques tout en maximisant les bénéfices lors du partage de données sensibles : (i) examiner et clarifier les cadres formels ou informels qui régissent la collecte et le partage des données désagrégées ; (ii) officialiser et uniformiser les demandes de données sensibles ; (iii) investir dans les capacités de gestion des données du personnel et des organisations ; et (iv) adopter des principes communs pour la gestion des données des bailleurs.

INTRODUCTION

Les bailleurs ont vocation à jouer un rôle important dans l'écosystème des données humanitaires, à la fois en tant que moteurs de la collecte et de l'analyse accrues des données qu'en tant qu'utilisateurs directs de ces données. Il ne s'agit pas là d'un phénomène nouveau ; la nécessité de rendre des comptes et de faire preuve de transparence dans l'utilisation des ressources financières accordées par les bailleurs de fonds est largement comprise et respectée. Or depuis quelques années, les bailleurs de fonds se sont mis à demander des données à caractère potentiellement sensible. Cela comprend des données personnelles au sujet des bénéficiaires et diverses formes de données désagrégées, telles que les résultats d'une enquête au niveau des ménages et les données sur la distribution de l'aide désagrégées par dimension démographique et/ou de groupe (par exemple, origine ethnique, groupe sur la protection, etc.).¹

¹ Comme il existe des normes et des mécanismes bien établis et acceptés pour le partage d'informations financières avec les bailleurs, y compris un rôle pour les audits externes, les demandes de données financières ne sont pas incluses dans la présente note d'orientation. Cette note d'orientation traite des données personnelles et des données sensibles non personnelles.

Les préoccupations concernant les demandes de données de ce type ont conduit les bailleurs de fonds et les organisations humanitaires à mettre davantage l'accent sur l'identification de stratégies relatives à la Responsabilité des données : la gestion sécurisée, éthique et efficace des données. La Responsabilité des données oblige les bailleurs de fonds et les organisations humanitaires à prendre des mesures qui contribuent à réduire les risques tout en maximisant les bénéfices des données. Cela est particulièrement difficile dans les cas où les bailleurs de fonds demandent des données sensibles. Par exemple, les procédures de criblage des bénéficiaires de l'aide, souvent utilisées pour justifier les demandes de données personnelles, ne sont pas seulement difficiles à mettre en œuvre en pratique, mais sont très problématiques au regard d'une aide humanitaire fondée sur des principes.²

En outre, le partage de données apparemment inoffensives comme les résultats d'enquêtes agrégés peut exposer des personnes et des communautés déjà vulnérables à de plus grands risques. Des données qui initialement pourraient être considérées comme non personnelles³ peuvent permettre la réidentification d'individus, de communautés et de groupes démographiques. La réidentification se produit lorsque des données peuvent être retracées ou reliées à un ou plusieurs individus ou groupe(s) d'individus parce que ces données n'ont pas été suffisamment anonymisées. Cela peut entraîner une violation de la protection des données, de la vie privée et d'autres droits humains et permettre de cibler des personnes ou des groupes victimes de violence ou d'autres formes de préjudice.⁴

De nombreux bailleurs de fonds et acteurs humanitaires reconnaissent les risques et les bénéfices associés au partage de ces données sensibles, mais le secteur doit encore œuvrer ensemble à trouver comment équilibrer efficacement ces risques et bénéfices. Les efforts déployés récemment visant à résoudre ce problème ont permis de clarifier davantage les pratiques actuelles, ainsi que les objectifs et les contraintes du partage de données. En septembre 2020, le Gouvernement suisse, le Comité international de la Croix-Rouge (CICR) et le Centre for Humanitarian Data (le Centre) du Bureau de la coordination des affaires humanitaires des Nations Unies (OCHA) ont organisé une discussion virtuelle Wilton Park pour contribuer à élaborer une conception commune de la question.⁵

Cette note d'orientation présente la synthèse des résultats de cette discussion et d'une revue documentaire associée.⁶ Elle décrit les défis inhérents au partage de données sensibles avec les bailleurs de fonds et propose des recommandations initiales sur la façon dont les bailleurs de fonds et les organisations humanitaires peuvent évoluer plus efficacement dans ce domaine.

DEMANDES DE DONNÉES DES BAILLEURS

Les bailleurs de fonds demandent régulièrement des données à leurs partenaires afin de s'acquitter des différents obligations et objectifs. Ces demandes peuvent être formelles ou informelles.

- Les **demandes formelles** ont tendance à être incluses dans les accords de financement en fonction des critères établis pour les rapports et sont généralement fondées sur des exigences juridiques telles que la conformité aux réglementations de lutte contre le terrorisme. De telles demandes ont tendance à être négociées dès le début d'un partenariat ou d'un accord de financement, et sont habituellement faites par écrit et planifiées à l'avance.

² Roepstorff, K., Faltas, C. and Hövelmann, S., 2020. [Counterterrorism Measures and Sanction Regimes: Shrinking Space for Humanitarian Aid Organisations.](#)

³ On entend par données non personnelles les données qui étaient, à la base, des données à caractère personnel, mais qui ont été rendues anonymes ultérieurement, telles que les données sur les populations affectées par la situation humanitaire et leurs besoins, les risques et vulnérabilités auxquels elles sont exposés, et leurs capacités (adapté du [Règlement \(UE\) 2018/1807 du Parlement européen et du Conseil du 14 novembre 2018 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne](#)).

⁴ Voir le [Consignes de OCHA sur la Responsabilité des données](#) et le [ICRC Handbook on data protection in humanitarian action](#).

⁵ Pour en savoir plus sur le dialogue virtuel, consultez ce [rapport Wilton Park](#).

⁶ Willits-King, B. and Spencer, A., 2020. [Responsible data-sharing with donors: accountability, transparency and data protection in principled humanitarian action.](#)

- Les **demandes informelles** concernent des informations ou des données qui ne relèvent généralement pas du cadre normal des rapports. Ces demandes ad hoc ont souvent une valeur implicite, ce qui signifie que si elles ne sont pas formellement requises, la fourniture de ces données supplémentaires est considérée comme bénéfique pour l'engagement et la relation partenariale en cours d'une organisation avec un bailleur de fonds. Ces demandes représentent un plus grand dilemme pour les acteurs humanitaires.

Peu de bailleurs de fonds disposent de politiques ou de lignes directrices formelles quant au partage des données.⁷ Il y a également une absence de position commune sur la terminologie et les risques et objectifs liés au partage des données. Il existe différentes définitions et conceptions des risques liés aux données, ce qui conduit à des pratiques incohérentes et parfois contradictoires concernant le partage de données potentiellement sensibles avec les bailleurs de fonds dans un contexte particulier.⁸

OBJECTIFS POUR LE PARTAGE DES DONNÉES AVEC LES BAILLEURS DE FONDS

Les objectifs les plus souvent identifiés pour les bailleurs de fonds qui demandent des données sensibles aux partenaires sont la connaissance de la situation et la conception des programmes ; la redevabilité et la transparence ; ainsi que les exigences juridiques, réglementaires et politiques.

Connaissance de la situation et conception des programmes

Les bailleurs de fonds recherchent des informations et des données auprès des organisations humanitaires afin de comprendre et de réagir aux changements dans les contextes humanitaires. Cela permet aux bailleurs de fonds d'améliorer la conception et l'évaluation de leurs propres programmes, d'éviter le double-emploi de l'aide, d'identifier les lacunes en matière d'information, et d'assurer une priorisation appropriée de l'aide.

Redevabilité et transparence

Les bailleurs de fonds et les organisations humanitaires ont un devoir de redevabilité dans la manière dont elles gèrent leurs activités. Les données peuvent permettre aux bailleurs de fonds d'expliquer et de justifier l'allocation de fonds pour l'aide internationale auprès des contribuables.

Exigences juridiques, réglementaires et politiques

Les bailleurs de fonds sont soumis à certaines exigences juridiques nationales et internationales, y compris les exigences politiques, juridiques et légales liées à la lutte contre le terrorisme, aux migrations et à l'application de la loi. Dans de nombreux cas, il se peut que les bailleurs de fonds souhaitent utiliser les données pour vérifier leur conformité à ces différentes exigences. Certains bailleurs incluent des clauses de lutte contre le terrorisme dans leurs accords de financement, qui visent à s'assurer que leurs fonds ne sont pas utilisés au profit de groupes terroristes identifiés.⁹ De même, les bailleurs peuvent inclure des clauses pour couvrir les mesures de lutte contre les pots-de-vin, la fraude et la corruption.¹⁰

⁷ Au moment de la rédaction de la présente note, seuls l'USAID et la GIZ avaient des lignes directrices accessibles au public sur le partage responsable des données. Voir USAID, 2019. *Considerations for using data responsibly at USAID and GIZ*, 2018. *GIZ's Responsible Data Principles*.

⁸ Willits-King, B. and Spencer, A., 2020. *Responsible data-sharing with donors: accountability, transparency and data protection in principled humanitarian action*.

⁹ Voir la boîte à outils de NRC *Toolkit for Principled Humanitarian Action; Managing CT Risks*.

¹⁰ Afin de garantir le respect des exigences, les bailleurs de fonds peuvent demander des données très désagrégées pour corroborer leurs processus de diligence raisonnable, s'assurant ainsi que leurs partenaires ne collaborent pas avec des « personnes ou entités visées par des sanctions ». Voir Walker, J., 2020. *Compliance Dialogue on Syria-Related Humanitarian Payments*. « Personnes sanctionnées » est un terme général qui peut inclure des individus, des groupes terroristes, des gouvernements ainsi que des sociétés et autres entités dotées de la personnalité juridique. L'UE, par exemple, a considérablement renforcé au fil des ans son cadre juridique pour la prévention du blanchiment de capitaux et du financement du terrorisme et le fait appliquer constamment. Voir : NGO Voice. *The Impact of EU Sanctions and Restrictive Measures on Humanitarian Action*.

CONTRAINTES EN MATIÈRE DE PARTAGE DES DONNÉES AVEC LES BAILLEURS DE FONDS

Malgré ces objectifs, le partage des données avec les bailleurs n'est pas sans contraintes, notamment l'absence de cadres réglementaires pour gérer de manière responsable les données sensibles non personnelles, ainsi que des lacunes en matière de capacités et la limitation de la finalité.

Absence de cadres réglementaires pour gérer de manière responsable les données sensibles non personnelles

La sensibilité des données personnelles est généralement bien connue et traitée par une variété de cadres stratégiques et réglementaires, mais on ne peut pas en dire autant pour les données sensibles non personnelles. La protection des groupes et de leurs données demeure difficile en raison des lacunes actuelles en matière de réglementation et d'orientation ; et du manque général de compréhension de la sensibilité des données non personnelles. Ces lacunes qui existent dans les politiques relatives aux données augmentent le risque que les données sensibles ne soient pas stockées ou protégées correctement ou qu'elles soient partagées par inadvertance par des partenaires afin de satisfaire les demandes des bailleurs de fonds.

Lacunes en matière de capacités

Répondre aux demandes ponctuelles de partage des données des bailleurs de fonds peut être perçu comme un fardeau supplémentaire par les intervenants humanitaires, détournant le temps, les ressources et l'attention essentiels d'autres activités mises en œuvre.¹¹ Le financement insuffisant du développement des capacités relatives aux données a limité la faculté de nombreuses organisations à fournir à leur personnel les compétences et les ressources nécessaires pour gérer les données de manière responsable.¹² Les lacunes en matière de capacité de satisfaire aux exigences des bailleurs de fonds pourraient également dissuader les ONG plus petites ou implantées localement de chercher ces types de financement, ce qui pourrait contrecarrer les efforts de localisation de l'aide.¹³

Limitation de finalité

Le principe de la limitation de la finalité exige que les données soient recueillies uniquement à des fins spécifiques, explicites et légitimes, et qu'elles ne soient pas traitées d'une quelconque manière qui serait incompatible avec ces finalités.¹⁴ Même lorsque les bailleurs de fonds fournissent des motifs légitimes pour demander des données conformes aux finalités initiales pour lesquelles les données ont été recueillies (par exemple, la fourniture d'une aide humanitaire), il peut être difficile de s'assurer que les données ne seront pas utilisées à d'autres fins une fois partagées. Les données utilisées hors contexte et à des fins qui ne sont pas connues au moment du partage, ou conservées au-delà de la durée prévue dans un but défini, représentent une violation, même si elle est involontaire, des droits des personnes concernées.

RECOMMANDATIONS

Compte tenu des objectifs et des contraintes décrits ci-dessus, le Centre, le Groupe de politique humanitaire de l'Institut de Développement d'outre-mer (Overseas Development Institute, ODI), le CICR, et la Division Sécurité humaine du Département Fédéral des Affaires étrangères suisse recommandent que les bailleurs de fonds et les organisations humanitaires prennent les mesures suivantes pour minimiser les risques tout en maximisant les bénéfices lors du partage de données sensibles :

¹¹ Inter-Agency Standing Committee (IASC) Humanitarian Financing Task Team (HFTT), 2016. [Donor Conditions and their implications for humanitarian response](#).

¹² Publish What You Fund, 2020. [Data Use Capacity in Protracted Humanitarian Crises](#).

¹³ Ibid.

¹⁴ ICRC, 2020. [Handbook on data protection in humanitarian action](#).

¹⁵ Examples include the [Good Humanitarian Donorship Initiative](#) and the [Grand Bargain](#).

- **Examiner et clarifier les cadres formels ou informels qui régissent la collecte et le partage des données désagrégées**

Les bailleurs de fonds et les partenaires devraient examiner les exigences officielles et formelles, ainsi que les exigences ad hoc et informelles en matière de partage des données, et analyser si le personnel des partenaires et des bailleurs de fonds interprète correctement et de manière cohérente ces exigences. Ils devraient évaluer s'il existe des conditionnalités implicites entre la volonté de partager des données désagrégées et la capacité des différentes organisations à accéder aux financements des bailleurs de fond, et à les conserver.

- **Officialiser et uniformiser les demandes de données sensibles**

Lorsque des données sensibles sont nécessaires pour atteindre un objectif mutuellement convenu, les bailleurs de fonds devraient officialiser et uniformiser leurs demandes de données de ce type. Les demandes doivent être faites par écrit et préciser le genre de données demandées, le format souhaité et l'utilisation prévue de ces dernières. Les bailleurs de fonds ne devraient demander que les informations requises pour satisfaire à l'objectif spécifique, et devraient indiquer un calendrier de destruction des données. Les organisations humanitaires devraient documenter toutes les demandes de données et veiller à y répondre de manière cohérente au fil du temps.

- **Investir dans la montée en compétences du personnel et des organisations en matière de gestion des données**

Les bailleurs de fonds et les organisations humanitaires devraient identifier les possibilités d'investir dans le développement d'une expertise en gestion des données, notamment pour le personnel non technique. La communauté des bailleurs de fonds est particulièrement bien placée pour encourager la Responsabilité des données en fournissant des ressources supplémentaires pour la formation et le renforcement des capacités.

- **Adopter des principes communs pour la gestion des données à destination des bailleurs de fonds**

Il existe déjà dans le secteur une série de principes et d'engagements pour informer les différents aspects des dons à destination humanitaire.¹⁵ Toutefois, ces mesures ne répondent pas suffisamment aux préoccupations liées à la Responsabilité des données. Les bailleurs de fonds et les partenaires devraient s'engager dans l'élaboration de principes et de directives communs pour le partage des données aux bailleurs de fonds afin de combler cette lacune. La [Humanitarian Data and Trust Initiative](#), codirigée par le Gouvernement suisse, le CICR et le Centre, offre une plateforme pour faciliter ce processus dans le cadre de ses travaux en cours visant à instaurer la confiance par le dialogue.

CONTRIBUTEURS : LE GROUPE DE POLITIQUE HUMANITAIRE DE L'INSTITUT DE DÉVELOPPEMENT D'OUTRE-MER (ODI); LE COMITÉ INTERNATIONAL DE LA CROIX-ROUGE; ET LA DIVISION SÉCURITÉ HUMAINE DU DÉPARTEMENT FÉDÉRAL DES AFFAIRES ÉTRANGÈRES SUISSE.

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.

¹⁵ Parmi les exemples, citons les suivants : [Good Humanitarian Donorship Initiative](#) et le [Grand Bargain](#).