IASC Inter-Agency Standing Committee

Directives Opérationnelles

LA RESPONSABILITÉ DES DONNÉES DANS L'ACTION HUMANITAIRE

Groupe de résultats 1 sur la réponse opérationnelle

février 2021

Approuvé par le Comité permanent interorganisations (IASC) sur le groupe de politique opérationnelle et de groupe de défense (OPAG)

Table des matières

Remerciements

Cette traduction a été réalisée conjointement par le Bureau de la coordination des affaires humanitaires des Nations Unies (UNOCHA), CartONG et le Fonds des Nations Unies pour l'enfance (UNICEF) pour le compte du Data Responsibility Working Group (DRWG).

***Note sur la traduction**: Cette traduction n'a pas été créée par le Comité permanent interagences (IASC). L'IASC ne peut être tenu responsable du contenu ou de l'exactitude de cette traduction. L'édition originale en anglais "IASC Operational Guidance on Data Responsibility in Humanitarian Action'' fait foi. Cette traduction utilise les versions anglaises d'une série de mots couramment utilisés dans le secteur, tels que "cluster", "Lead", "Co-Lead", etc.. Bien que cette traduction ne soit peut-être pas la plus fidèle, dans l'esprit opérationnel de ce document, il est estimé que ces termes sont à la fois compréhensibles pour un large éventail de lecteurs, que cette traduction contribue à éviter toute confusion potentielle et qu'elle simplifie la mise en œuvre de ces directives. De même, vous constaterez que le terme "responsabilité des données" prend la majuscule. Nous avons choisi de faire cette distinction afin de mettre l'accent sur la signification conceptuelle et philosophique de ce terme dans le contexte de ces directives, et de le différencier de la signification plus littérale du terme "responsabilité" en français.*

Avant-propos

La Responsabilité des données est incontournable car le secteur humanitaire collecte et partage toujours plus de données. De la même manière que la pandémie de la COVID-19 a aggravé les crises humanitaires actuelles, elle a également fait augmenter notre dépendance aux technologies numériques et l'accès aux données en temps réel.

Lorsque nous nous référons aux données dans les contextes humanitaires, nous faisons référence aux populations les plus vulnérables au monde: 235 millions de personnes, un record, auront besoin d'une assistance et d'une protection humanitaire en 2021. Les nouvelles technologies et les multiples sources de données nous aident à prendre des décisions plus rapides, mieux informées, et nous permettent, chaque année, de fournir une aide à plus de personnes. Toutefois, les manières dont les données sont collectées, partagées et utilisées par les organisations à travers tout le secteur humanitaire peuvent engendrer des problèmes quant à la sécurité et au respect des droits et de la vie privée des populations affectées.

Au cours de ces dernières années, nous avons vu se développer des principes, des politiques et des stratégies pour une gestion responsable des données au sein de l'action humanitaire; cependant, il reste à faire pour combler les manques entre les directives globales et leurs applications concrètes dans les opérations de terrain.

Les Directives opérationnelles du Comité Permanent Inter-agences (IASC) sur la Responsabilité des données dans l'action humanitaire sont une avancée bienvenue et attendue visant à adresser collectivement les problèmes et les opportunités dans ce domaine; ceci, à un moment où l'importance de la Responsabilité des données bénéficie d'une reconnaissance globale croissante.

Ces Directives opérationnelles au niveau de tout le système, ce qui est une nouveauté, vont permettre des avancées concrètes en faveur de la Responsabilité des données dans toutes les étapes de l'action humanitaire. Elles sont le produit d'une démarche inclusive et consultative, regroupant plus de 250 acteurs du secteur humanitaire. Les partenaires à travers tout le système vont mettre en œuvre ces directives dans le respect de leurs mandats respectifs et des décisions de leurs autorités décisionnelles.

J'encourage les membres du IASC et plus largement toute la communauté humanitaire à soutenir l'utilisation responsable des données grâce à la mise en oeuvre de ces Directives opérationnelles.

Mark Lowcock
Secrétaire général adjoint aux affaires humanitaires et Coordonnateur des secours d'urgence

Résumé

La responsabilité des données dans l'action humanitaire est la gestion sécurisée, éthique et efficace des données à caractère personnel et non personnel (ci-après 'les données personnelles et non personnelles') pour la réponse opérationnelle. Il est indispensable que le secteur humanitaire aborde la responsabilité des données, et les enjeux sont grands.

Veiller à "ne pas nuire" (principe du 'Do no harm' en anglais), tout en maximisant les avantages qu'offrent les données, nécessite une action collective à tous les niveaux du système humanitaire. Les acteurs humanitaires doivent être vigilants lorsqu'ils gèrent des données pour éviter de faire courir des risques accrus aux individus et communautés déjà vulnérables. Cette vigilance est particulièrement importante lorsque l'urgence des besoins humanitaires exerce une pression forte pour l'obtention de résultats rapides, parfois non testés et non éprouvés, basés sur des données dont les enjeux politiques peuvent avoir des répercussions encore plus extrêmes pour les populations affectées. Par exemple, entre autres risques potentiels, la divulgation de la localisation ou de l'identité ou de l'affiliation d'un individu ou d'une communauté peut engendrer des attaques ciblées, l'exclusion sociale et/ou la stigmatisation. Au-delà de veiller à ne pas nuire, la gestion sécurisée, éthique et efficace des données présente de nombreux avantages : elle peut aboutir à une prise de décisions plus informée et transparente, une réponse humanitaire plus efficace, et une confiance accrue entre les acteurs humanitaires et les populations qu'ils cherchent à aider.

En pratique, la mise en œuvre de la Responsabilité des données manque souvent de cohérence au sein et au travers des contextes de réponse humanitaire. Cette incohérence persiste malgré les principes, les normes et les standards du secteur relatifs aux droits des populations affectées; la multitude de ressources sur la Responsabilité des données disponibles dans la communauté internationale, ainsi que les efforts importants déployés par de nombreuses organisations humanitaires pour développer et mettre à jour leurs politiques et directives dans ce domaine. Cependant, étant donné que l'écosystème humanitaire des données est interconnecté par nature, aucune organisation individuelle ne peut faire face seule aux défis qui se posent. Alors que chaque organisation demeure responsable de ses propres données, les acteurs humanitaires, membres du Comité permanent interorganisations (IASC/CPI) - qui réunit les entités onusiennes (ONU), les consortiums d'organisations non gouvernementales (ONG) et le Mouvement international de la Croix-Rouge et du Croissant-Rouge - ont besoin d'un cadre de travail, à l'échelle du système, pour guider leurs actions, tant individuelles que collectives, et pour maintenir un standard élevé en matière de Responsabilité des données dans différents environnements opérationnels.
En janvier 2020, le Results Group 1 a donc établi le Sous-Groupe[1] sur la Responsabilité des données, qui a été chargé de développer les présentes **Directives opérationnelles sur la**

[1] Le Sous-groupe a été co-dirigé par l'Organisation Internationale pour les migrations, le Centre for Humanitarian Data de OCHA et le Haut Commissariat des Nations unies pour les réfugiés. Il regroupe également vingt organisations membres qui représentent les différentes parties prenantes du système humanitaire. Le Sous-groupe inclut des représentants de CARE, CRS, DRC, ICRC, IFRC, IRC, IOM, JIPS, Mercy Corps, MSF, NRC, OCHA, OHCHR, Oxfam, Save the Children, UNFPA, UNHCR, UNICEF, WFP and WHO. Veuillez consulter l'annexe D pour plus d'informations sur le processus de développement de ces directives opérationnelles du Sous-groupe.

Responsabilité des données dans l'action humanitaire, communes et à l'échelle du système.

Ces directives opérationnelles sont divisées en quatre sections:

- La première section présente **la logique et l'approche** des directives. Elle offre un **aperçu général de la Responsabilité des données dans l'action humanitaire**, et précise **le champ d'application** des directives, ainsi que le public ciblé.
- La deuxième section présente les **principes pour la Responsabilité des données dans l'action humanitaire.**
- La troisième section décrit **les actions clés** à mettre en œuvre aux différents niveaux de la réponse humanitaire pour garantir la Responsabilité des données, y compris **les rôles et les responsabilités** spécifiques.
- La quatrième section est un ensemble d'**annexes**, proposant des **définitions clés**, des **modèles et outils pour la Responsabilité des données**, **des ressources et références**, ainsi que **l'historique du développement de ces Directives opérationnelles**.

Compte tenu de la nature dynamique et évolutive des défis et opportunités de la Responsabilité des données dans l'action humanitaire, ces directives opérationnelles seront révisées et mises à jour à travers un processus collaboratif et consultatif tous les deux ans.

Définir la Responsabilité des données

La Responsabilité des données dans l'action humanitaire est **la gestion sécurisée, éthique et efficace des données personnelles et non personnelles pour la réponse opérationnelle**, conformément aux cadres réglementaires en vigueur sur la protection des données à caractère personnel.[2]

- **Sécurisée** | Les activités de gestion des données garantissent la sécurité des données à tout moment, respectent les droits humains et autres obligations légales, et sont mises en œuvre de façon à ne pas nuire (principe du 'Do No Harm').

- **Éthique** | Les activités de gestion des données sont conformes aux cadres et aux standards en vigueur concernant l'éthique humanitaire[3] et la gestion éthique des données.

- **Efficace** | Les activités de gestion des données atteignent les objectifs qui ont motivé leur mise en place.

La Responsabilité des données exige la mise en œuvre d'actions fondées sur des principes à tous les niveaux de la réponse humanitaire. Ceci inclut par exemple des actions pour garantir la protection des données et la sécurité des données, ainsi que des stratégies pour atténuer les risques tout en maximisant les bénéfices de la gestion des données opérationnelles à toutes les étapes, tel que défini ci-dessous.

Bien que la Responsabilité des données soit liée à la protection des données et à la sécurité des données, il s'agit de termes différents.
La protection des données fait référence à l'application systématique d'un ensemble de garanties institutionnelles, techniques et physiques qui préservent le droit à la vie privée dans le respect du traitement des données personnelles.
La sécurité des données, applicable à la fois aux données à caractère personnel et non personnel, fait référence aux mesures techniques et organisationnelles visant à préserver la confidentialité, la disponibilité et l'intégrité des données.

Les termes essentiels suivants guideront la lecture de ces directives opérationnelles :

La gestion opérationnelle des données : La conception des activités de gestion des données, incluant la collecte ou la réception de données, le stockage, le traitement, l'analyse, le partage, l'utilisation, la conservation et la destruction des données et des informations par des acteurs humanitaires. Ces activités font (pleinement) partie de l'action humanitaire, tout au long du cycle de planification et de réponse des clusters/secteurs et incluant de façon non exhaustive, les analyses de situation, les évaluations des besoins, la gestion des données démographiques, l'enregistrement et

[2] Aux fins des présentes directives opérationnelles, 'conformément aux cadres réglementaires en vigueur sur la protection des données à caractère personnel' signifie que les activités de gestion des données sont guidées par les lois nationales et régionales en matière de protection des données ou par les politiques organisationnelles de protection des données.

[3] L'éthique humanitaire s'est développée comme une éthique fondée sur les principes d'humanité, d'impartialité, de neutralité et d'indépendance qui guident l'aide et la protection humanitaires. Ces principes et les règles qui s'y rapportent sont inscrits dans divers codes de conduite aujourd'hui largement reconnus comme la base d'une pratique humanitaire éthique, notamment: 'The Humanitarian Charter and Minimum Standards in Humanitarian Response', y compris les 'Core Standards and Protection Principles', le 'Core Humanitarian Standard on Quality and Accountability', et le 'Code of Conduct for the International Red Cross and Red Crescent Movement and Non-Governmental Organizations (NGOs) in Disaster Relief'. Pour des orientations supplémentaires sur l'éthique des données humanitaires, voir The Centre for Humanitarian Data, Guidance Note : Humanitarian Data Ethics (2019), disponible à l'adresse : https://centre.humdata.org/guidance-note-humanitarian-data-ethics/.

l'inscription, la gestion des cas, la communication avec les populations affectées, le suivi des activités de protection, et le suivi et l'évaluation des réponses.

Les données personnelles : Toute information se rapportant à une personne physique identifiée ou identifiable ('la personne concernée'). Une personne physique est identifiable lorsqu'elle peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

Les données non personnelles : Toute information ne se rapportant pas à une personne concernée. Les données non personnelles peuvent être classées en fonction de leur origine, à savoir : les données qui ne se rapportent jamais à une personne concernée, telles que les données sur le contexte dans lequel une réponse humanitaire est en cours, ainsi que les données sur les acteurs humanitaires et leurs activités ; *ou* 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. Les données à caractère non personnel incluent les informations démographiquement identifiables (Demographically Identifiable Information, ou DII en anglais), à savoir les données qui permettent l'identification d'un groupe d'individus par des facteurs démographiques, tels que l'ethnicité, le sexe, l'âge, l'occupation, la religion ou la localisation.

Les données sensibles : Les données classées comme sensibles en fonction de la probabilité et de la sévérité du préjudice qui est susceptible de résulter lorsque celles-ci sont divulguées dans un contexte particulier. Les données, qu'elles soient personnelles ou non, peuvent, toutes deux, être sensibles. Beaucoup d'organisations disposent de systèmes de classification spécifiques quant à ce qui constitue des données sensibles, afin de faciliter les pratiques internes de gestion des données.

NB: Une liste complète de définitions est inclue dans l'annexe A.

Contexte, logique et champ d'application

Ces directives opérationnelles visent à soutenir le personnel et les organisations humanitaires, ainsi que leurs partenaires, à mettre en pratique la Responsabilité des données dans différents contextes. La Responsabilité des données est définie comme la gestion sécurisée, éthique et efficace des données personnelles et non personnelles dans les réponses opérationnelles.

Les directives opérationnelles offrent un ensemble de principes et d'actions que les entités au niveau du système humanitaire, les clusters et les secteurs, et les organisations peuvent adopter dans leurs actions et programmes humanitaires. Elles ne visent en aucune façon à remplacer ou à supplanter les politiques et directives organisationnelles existantes,[4] et ne relèvent ni de mandats organisationnels, ni de lois nationales ou régionales spécifiques.

La Responsabilité des données dans l'action humanitaire

La Responsabilité des données est une question cruciale à laquelle le secteur doit faire face. Pour garantir que nous minimisons les risques, tout en maximisant les bénéfices de la gestion des données dans les milieux humanitaires, il faudra un changement de pratiques en profondeur, des efforts continus dans la durée seront essentiels, ainsi qu'une action collective qui s'étendra à tous les acteurs humanitaires et au-delà.

La mise en œuvre de la Responsabilité des données en pratique manque de cohérence d'un contexte et d'une réponse humanitaire à l'autre. Malgré les principes, les normes et les standards définis et reconnus dans le secteur de l'aide, reconnus à l'égard des droits des populations affectées, et malgré la multitude de ressources disponibles sur la Responsabilité des données disponibles, cette incohérence persiste.

Depuis quelques années, de nombreuses organisations humanitaires ont développé ou mis à jour leurs politiques, directives, et pratiques spécifiques pour faire progresser les différents aspects de la Responsabilité des données. Le secteur a également connu un nombre croissant d'efforts de collaboration visant à dépasser l'échelle d'une seule organisation et améliorer la Responsabilité des données.

Cependant, même au sein d'organisations possédant des cadres réglementaires éprouvés ou des principes solides, des défis liés à la gouvernance et aux capacités et ressources disponibles de façon pérenne peuvent entraîner des situations et pratiques qui sont contradictoires avec la Responsabilité des données. Étant donné que l'écosystème humanitaire des données est interconnecté par nature, aucune organisation ne peut faire face seule aux défis qui se présentent.
Alors que chaque organisation est responsable de ses propres données, les acteurs humanitaires au sein du Comité permanent interorganisations (IASC) - qui réunit les entités

[4] Dans le cas de la protection des données, il s'agit, par exemple, des principes de l'ONU en matière de protection de la vie privée et de protection des données, des politiques et lois sur la protection des données telles qu'elles s'appliquent aux agences de l'ONU et aux ONG, et des cadres de protection des données tels que le Conseil de l'Europe, la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE 108), Strasbourg (1981), le Règlement général sur la protection des données (RGPD), ou des documents équivalents, y compris ceux de nature non contraignante.

onusiennes (ONU), les consortiums d'organisations non gouvernementales (ONG) et le Mouvement international de la Croix-Rouge et du Croissant-Rouge - ont besoin, à l'échelle de l'écosystème humanitaire, de lignes directrices, directives normatives. Ceci permettra de guider l'ensemble des actions, qu'elles soient isolées ou collectives, et pour maintenir des normes élevées en matière de Responsabilité des données dans différents environnements opérationnels. Ces directives opérationnelles complètent et s'appuient sur la documentation existante[5] élaborée par les acteurs du développement et issue de la communauté humanitaire, au sens large.

Défis et opportunités pour la Responsabilité des données dans l'action humanitaire
Les expériences acquises dans des contextes de réponses humanitaires variés ont engendré un ensemble commun de défis et d'opportunités qui constituent la base de l'action collective dans le domaine de la Responsabilité des données.

Ces défis incluent :

- **L'absence de définitions communes et des incohérences dans le vocabulaire spécifique utilisé** ont engendré un manque de compréhension commune entre les organisations humanitaires en matière de Responsabilité des données.
- **Les lacunes en matière de lignes directrices et normes,** notamment sur la gestion responsable des données sensibles, sur l'évaluation des risques associés à différents types de données dans différents contextes, et, sans oublier, les défis spécifiques et complexes de la Responsabilité des données dans l'action humanitaire.
- L'application variable de différents **cadres juridiques et réglementaires** au sein des les organisations internationales (OI), ONG et les entités de l'ONU.
- **L'incertitude et le manque de coordination** en matière de développement de nouvelles technologies, et des normes et pratiques de la gestion des données humanitaires, qui évoluent plus rapidement que les cadres institutionnels et juridiques qui réglementent leur emploi.
- La **priorisation des pratiques de politiques internes en matière de protection de données** plutôt qu'un investissement qui appuierait les travaux dans ce domaine dans le secteur de façon générale.
- **L'absence d'outils et processus communs et approuvés** pour la mise en œuvre de la Responsabilité des données.
- **Le manque de capacité** en matière de Responsabilité des données d'un grand nombre d'organisations et de leur personnel.
- **La sous-représentation** des organisations locales, des organisations de la société civile et des structures communautaires dans les activités de la gestion des données.

Les opportunités incluent :

- **L'investissement accru par les organisations humanitaires et de développement, les bailleurs, et les gouvernements des pays hôtes dans la Responsabilité des données,** dans le cadre d'une stratégie pour l'avancement des droits des populations

[5] Ceci inclut, par exemple, les directives opérationnelles de l'IASC sur les Responsabilités des Leads des Clusters/Secteurs, les Professional Standards for Protection Work, le Protection Information Management (PIM) Framework, l'initiative 'Responsible Data for Children', et le Signal Code: A Human Rights Approach to Information During Crisis, (voir Annexe C).

affectées qui contribue à la réalisation d'objectifs humanitaires et de développement plus globaux.

- **L'amélioration de la capacité institutionnelle** concernant les questions en matière de gestion responsable des données (en particulier en matière de protection de données à caractère personnel).
- **Des possibilités accrues de collaboration en matière de gestion des données, avec les gains d'efficacité qui en découlent,** notamment à travers les évaluations coordonnées, déploiement conjoint de l'aide humanitaire, et d'autres activités similaires.
- **Un intérêt et un soutien plus important pour la constitution d'une base concrète et factuelle de pratiques démontrant** "ce qui fonctionne" et "ce qui ne fonctionne pas" en matière de Responsabilité des données.
- **Une amélioration de la transparence et une redevabilité** des organisations humanitaires dans la manière dont elles gèrent les données en appui des différentes activités d'intervention.
- **Des économies d'échelle** grâce à des efforts conjoints pour produire des lignes directrices et des outils communs visant à la mise en œuvre de mesures spécifiques pour la Responsabilité des données.

Champ d'application et audience

Les directives opérationnelles s'appliquent aux différent types de données opérationnelles (personnelles et non-personnelles) qui sont générées ou utilisées lors des réponses humanitaires, notamment:[6]

- **Les données sur le contexte** dans lequel se déroule une réponse (par exemple les cadres juridiques, les conditions politiques, sociales et économiques, l'infrastructure, etc.) et les éléments de contexte spécifiques à la situation humanitaire (par exemple les incidents de sécurité, les risques de protection, les facteurs et les causes sous-jacentes de la crise).
- **Les données sur les populations affectées par la situation humanitaire**, leurs besoins**,** les menaces et les vulnérabilités auxquelles elles sont confrontées, ainsi que leurs capacités.
- **Les données sur les acteurs de la réponse humanitaire et leurs activités** (par exemple 3W/4W/5W).

Ces directives opérationnelles ne couvrent pas les données liées au fonctionnement interne des organisations, telles que les données relatives à la gestion financière interne, aux ressources humaines et au personnel, à la gestion de la chaîne d'approvisionnement et à la logistique, ainsi qu'à d'autres fonctions supports des organisations humanitaires.

Les directives opérationnelles s'appliquent à toutes les formes de gestion des données opérationnelles qui ont lieu dans tous les contextes de réponse humanitaire. La *gestion des données opérationnelles* désigne la conception des activités de gestion de données dont la réception, le stockage, le traitement, l'analyse, le partage, l'utilisation, la conservation et la destruction des données et des informations par des acteurs humanitaires. Ces activités font partie intégrante de l'action humanitaire tout au long du cycle de planification et de réponse à tous les niveaux des clusters/secteurs, et se manifestent, notamment, dans l'analyse situationnelle, l'évaluation des besoins, la gestion des données démographiques, l'enregistrement et l'inscription, la gestion des cas, la communication avec les populations affectées, le suivi de la protection, et le suivi et l'évaluation de la réponse. Dans la mesure où les organisations humanitaires ont des cycles et des processus variés,[7] ces directives opérationnelles n'ont pas vocation à présenter un ensemble unique ou harmonisé d'étapes pour la gestion des données, mais plutôt à mettre en avant les principes et les actions pertinentes à chaque étape de la gestion des données opérationnelles au bénéfice de l'action humanitaire.

Ces directives apportent un soutien à tous les acteurs humanitaires, y compris les entités onusiennes, les autres organisations internationales, les ONG internationales et nationales, et tout autre acteur engagé dans l'action humanitaire.

---

[6] Il peut s'agir de types de données nouveaux ou non traditionnels, tels que les Call Detail Records (CDR), les données des réseaux sociaux, etc. Les organisations humanitaires doivent appliquer les mêmes normes pour la gestion de ces données que pour les autres formes de données.

[7] Une analyse documentaire de 55 documents a permis de dégager 18 processus et cycles différents, chacun d'entre eux variant en longueur et contenant différentes étapes. La liste des documents examinés est disponible à l'annexe C.

Plus précisément, elles visent les structures de coordination suivantes, qui servent de forums pour la promotion et le suivi de la mise en œuvre de la Responsabilité des données aux différents niveaux d'une réponse : l'équipe humanitaire du pays (EHP), le Groupe de coordination inter-cluster (ICCG), le Mécanisme de coordination inter-cluster (ICCM), le Groupe de travail intersectoriel (ISWG), et/ou le Groupe de travail de la gestion de l'information (IMWG); et les clusters, les domaines de responsabilité (AoR), les groupes de travail, et/ou secteurs.

Elles visent des rôles et fonctions spécifiques au niveau du système, des clusters/secteurs et des organisations, notamment les Coordonnateurs résidents/humanitaires, les Chefs de bureau, les Chefs de missions, les Délégués, les Représentants Pays, les responsables de programmes,[8] les coordinateurs des clusters/secteurs, les comités de pilotage, les groupes d'expertise stratégiques et les référents techniques[9] (liste non exhaustive).

En fin de compte, la Responsabilité des données nécessite l'adhésion et la participation de tous, à tous les niveaux, dans toutes les fonctions de chaque organisation, cluster/secteur et du système humanitaire.

[8] Ceci inclut notamment les Program Officers, Sectoral/Technical Experts, Humanitarian Affairs Officers, et d'autres positions.

[9] Ceci inclut, notamment, les responsables IM, Data Analysts and Scientists, statisticiens, responsables-points focaux de protection des données, personnel IM, responsables d'enregistrement, les opérateurs de Community Feedback & Response Mechanism, les responsables de Monitoring & Evaluation, les Enumerators, et d'autres rôles.

Les Principes pour la Responsabilité des données dans l'action humanitaire

Les Principes suivants pour la Responsabilité des données dans l'action humanitaire (ci-après définis comme les "Principes") sont conçus pour permettre la gestion sécurisée, éthique et efficace des données pour toutes les organisations, les clusters/secteurs, à tous les niveaux de l'écosystème humanitaire. Ils doivent guider les acteurs dans leur mise en application des actions recommandées en matière de Responsabilité des données issues de ces directives opérationnelles. Les Principes ne constituent pas une norme de conformité.

Ces Principes reposent sur une analyse de principes existants relatifs à la gestion des données (y compris la protection des données) à travers le secteur humanitaire et le secteur du développement.[10] Cette analyse a révélé des lacunes quant aux orientations en matière de gestion des données opérationnelles au niveau du système et au niveau des clusters/secteurs, ainsi que, de manière plus large, des lacunes quant aux directives en matière de gestion de données non personnelles à tous les niveaux de la réponse humanitaire. Les Principes énoncés dans ce document servent à combler ces lacunes et à garantir une gestion des données sécurisée, éthique et efficace. En ce sens, ils renforcent l'engagement primordial des humanitaires envers le principe humanitaire cardinal de "Ne pas nuire" (Do No Harm), tout en maximisant les avantages que les données apportent à l'action humanitaire[11]. Les Principes réaffirment également que les populations affectées, leurs droits et leur bien-être sont au cœur de l'action humanitaire.

La gestion de **données personnelles** doit être guidée par le *Principe sur la protection des données personnelles*[12] alors que la gestion des **données non personnelles** doit être guidée par les autres Principes. Les Principes ci-dessous sont présentés par ordre alphabétique sans hiérarchie particulière.

---

[10] Il s'agit notamment des principes humanitaires et des normes largement acceptées énoncés, par exemple, dans Sphere, le Core Humanitarian Standard et le Code of Conduct for the International Red Cross et Red Crescent Movement and Non-Governmental Organizations (NGOs) in Disaster Relief, United Nations Data Strategy, et UN Personal Data Protection and Privacy Principles. En outre, ils comprennent des orientations plus thématiques ou spécifiques à différents aspects de la gestion des données, notamment les Normes professionnelles pour le travail de protection, les Professional Standards for Protection Work, the Protection Information Management (PIM) et le Manuel du CICR sur la protection des données dans l'action humanitaire, entre autres. Enfin, les Principes s'appuient sur les directives existantes de l'IASC, notamment les Directives opérationnelles de l'IASC sur les responsabilités des Leads des clusters/secteurs et de OCHA en matière de gestion de l'information, et les Directives opérationnelles de l'IASC pour les évaluations coordonnées dans les crises humanitaires. Une liste complète des documents analysés par le Sous-groupe sur la responsabilité des données est disponible en Annexe C.

[11] Largement reconnu dans le secteur humanitaire, le concept de 'Do No Harm' trouve ses racines dans la pratique médicale, à partir de laquelle il a été développé en un axiome de la réponse humanitaire dans Mary B. Anderson, Do No Harm : How Aid Can Support Peace - Or War, (1999). Aux fins du présent document, le terme est utilisé comme suit : "Ne pas nuire" signifie que la gestion des données dans le cadre de la réponse humanitaire ne doit pas causer ou exacerber les risques pour les personnes et les communautés affectées, les communautés d'accueil, le personnel humanitaire ou les autres parties prenantes, par des actions ou des omissions. Le préjudice est défini comme les 'implications négatives d'une initiative de traitement des données sur les droits d'une personne ou d'un groupe de personnes concernées, y compris, mais sans s'y limiter, les préjudices physiques et psychologiques, la discrimination et le refus d'accès aux services.' Maximiser les avantages de la gestion des données humanitaires implique que les données soient partagées lorsqu'un objectif l'exige, de manière appropriée et sécurisée, en respectant les exigences nécessaires en matière de protection des données. Cela implique également que les données soient gérées de manière à augmenter la probabilité d'un impact positif pour les personnes affectées.

[12] Ceci inclut les UN Personal Data Protection and Privacy Principles.

Lorsque ces Principes sont en conflit, que ce soit dans leur interprétation ou leur application, ils doivent être mis en balance les uns vis-à-vis des autres sur la base de la dynamique du contexte particulier.[13] En cas de conflit entre ces Principes et les politiques internes ou les obligations légales applicables, ces dernières prévalent.

Les Principes pour la Responsabilité des données

Redevabilité

Conformément aux règles pertinentes applicables, les organisations humanitaires ont une obligation de justifier et d'assumer la pleine responsabilité quant à leurs activités de gestion de données. Les organisations humanitaires sont redevables vis-à-vis des populations affectées par les crises, des structures de gouvernance internes, des partenaires humanitaires nationaux et internationaux, et, le cas échéant, vis-à-vis des gouvernements nationaux et des organismes de réglementation. Pour atteindre leurs engagements en matière de redevabilité, les organisations humanitaires doivent mettre en place toutes les mesures nécessaires pour respecter et suivre la bonne adhésion à ces Principes. Ceci inclut la mise en place de politiques et mécanismes appropriés, et la responsabilité d'assurer la disponibilité de compétences, ressources, et capacités adéquates, en termes de personnel, ressources et infrastructure.[14]

Confidentialité

Les organisations humanitaires doivent mettre en œuvre des garanties et des procédures organisationnelles appropriées pour préserver la confidentialité des données sensibles à tout moment. Les mesures doivent être conformes aux normes générales de confidentialité ainsi qu'aux normes spécifiques au secteur humanitaire[15] et aux politiques organisationnelles et exigences légales applicables, tout en tenant compte du contexte et des risques associés.

Coordination et Collaboration

La gestion coordonnée et collaborative des données implique une inclusion véritable des partenaires humanitaires, des autorités nationales et locales, des populations affectées par les crises, et les autres parties prenantes dans les activités de gestion des données, le cas échéant et sans compromettre les principes humanitaires[16] ou les présents Principes. La coordination et la collaboration doivent également viser à garantir la création de passerelles adéquates entre les activités de gestion des données opérationnelles humanitaires et les processus et investissements en matière de données qui soutiennent le développement. La capacité locale et nationale doit être renforcée dans la mesure du possible, et ne doit, en aucun cas, être affaiblie.

Sécurité des données

---

[13] Veuillez consulter l'annexe B pour des exemples des Principes.

[14] Ceci inclut le respect des engagements énoncés dans : IASC, Commitments on Accountability to Affected People and Protection from Sexual Exploitation and Abuse (2017), disponible à l'adresse : https://interagencystandingcommittee.org/accountability-affected-populations-including-protection-sexual-exploitation-and-abuse/documents-56.

[15] Le Manuel sur la protection des données dans l'action humanitaire du CICR (2020) et la politique de l'IASC sur la Protection dans l'action humanitaire (2016) donnent des conseils sur la confidentialité. Ces normes doivent être interprétées conformément aux politiques organisationnelles et orientations pertinentes.

[16] Pour plus d'informations, veuillez consulter OCHA on Message: Humanitarian Principles, disponible ici : https://reliefweb.int/sites/reliefweb.int/files/resources/oom-humanitarianprinciples- eng-june12.pdf.

Les organisations humanitaires doivent mettre en place des mesures de protection, procédures et systèmes appropriés, tant au niveau organisationnel que technique, afin de prévenir, atténuer, signaler et répondre aux incidents de sécurité. Ces mesures doivent être suffisantes pour assurer la protection contre les attaques externes, ainsi que se prémunir, en interne, contre l'accès ou la manipulation non autorisés ou inappropriés; et contre la divulgation accidentelle, les dommages, les altérations, les pertes et les autres risques liés à la gestion des données. Ces mesures doivent être ajustées en fonction de la sensibilité des données gérées, et mises à jour en fonction de l'évolution des meilleures pratiques en matière de sécurité des données, tant pour les données numériques que pour les données analogiques.

Finalité, nécessité et proportionnalité
La gestion des données humanitaires et les activités associées doivent se définir sur la base d'une finalité précise. La conception des processus et des systèmes de gestion des données doit contribuer à améliorer les résultats des actions humanitaires, être cohérente avec les mandats associés et cohérente avec les droits et libertés concernés, en les considérant en balance avec soin quand cela s'avère nécessaire. Conformément au concept de la minimisation des données, la gestion des données dans le cadre de l'action humanitaire doit être pertinente, limitée et proportionnée - en termes d'investissement requis ainsi qu'en termes de risque identifié - aux finalités déterminées.

Equité et légitimité
Les organisations humanitaires doivent gérer les données de manière équitable et légitime, conformément à leurs mandats respectifs, le contexte de la réponse humanitaire, les instruments de gouvernance, et les normes et standards globaux, tels que les Principes Humanitaires. Les motifs légitimes pour la gestion des données incluent : l'intérêt des personnes affectées par les crises, conformément au mandat de l'organisation, l'intérêt public supérieur allant au-delà du mandat de l'organisation, l'intérêt vital des communautés et des individus qui ne sont pas en mesure de prendre des décisions quant à la gestion des données, et tout autre motif légitime spécifiquement identifié par le cadre réglementaire de l'organisation ou les lois applicables.

Approche basée sur les droits humains
La gestion des données doit être conçue et mise en œuvre de façon à respecter, protéger et promouvoir les droits humains. Cela comprend les libertés fondamentales et les principes d'égalité et de non-discrimination tels que définis dans les cadres traitant des droits humains, et plus particulièrement le droit à la vie privée et d'autres droits liés aux données. Et aussi, les droits spécifiques en matière de protection des données promulgués dans la législation et dans d'autres règlements applicables.

Approche inclusive et axée sur la personne
Les populations affectées doivent avoir la possibilité d'être incluses, représentées et légitimées dans l'exercice de leur autorité tout au long de la gestion des données, lorsque le contexte opérationnel le permet. Conformément aux engagements de ne laisser personne pour compte ('Leave No One Behind' en anglais), des efforts concrets doivent être entrepris pour encourager

la participation et l'engagement des personnes qui ne sont pas bien représentées et qui peuvent être marginalisées lors des activités de gestion des données (en raison de l'âge, du sexe et d'autres facteurs de diversité tels que le handicap, l'origine ethnique, la religion, l'orientation sexuelle ou d'autres caractéristiques), ou qui sont d'une façon ou d'une autre rendues 'invisibles'. En matière de gestion des données, une approche inclusive et axée sur les personnes est particulièrement importante dans le développement de normes et de standards spécifiques au contexte.

Protection des données à caractère personnel

Les organisations humanitaires ont une obligation d'adhérer (i) aux lois nationales et régionales applicables en matière de protection des données, ou (ii), à leurs propres politiques en matière de protection des données, si elles bénéficient de privilèges et d'immunités tels que les lois nationales et régionales ne sont pas applicables.[17] Ces lois et politiques contiennent la liste des bases légitimes pour le traitement des données personnelles, dont le consentement.[18] Lors de la conception des systèmes de gestion des données, les organisations humanitaires doivent respecter les normes de confidentialité et de protection des données dès la conception et par défaut. Les organisations humanitaires doivent également tenir compte de la protection des données personnelles quand elles développent des cadres basés sur des données ouvertes ('open data'). Conformément à leur engagement en faveur de l'inclusion et du respect des droits humains, elles doivent garantir les droits des personnes concernées à être informées du traitement de leurs données personnelles, et à pouvoir accéder, corriger, supprimer ou s'opposer au traitement de leurs données personnelles.

Qualité

La qualité des données doit être maintenue de manière à ce que les utilisateurs et les principales parties prenantes puissent faire confiance à la gestion des données opérationnelles et aux produits qui en résultent. On entend par qualité des données le fait que les données soient pertinentes, exactes, opportunes, complètes, à jour et interprétables, conformément à l'utilisation prévue et selon le contexte. Lorsque cela est possible et approprié, sans compromettre ces principes, les organisations doivent s'efforcer de collecter les données et de les analyser de manière désaggrégée, en fonction de l'âge, du sexe et du handicap, ainsi qu'en fonction de tout autre caractéristique de diversité pour les finalités définies d'une activité.

Conservation et destruction

La conservation des données sensibles doit être limitée au temps nécessaire pour atteindre les finalités pour lesquelles elles sont gérées, ou bien, à défaut, limitée à la durée de conservation qui est stipulée par la loi applicable ou les règles d'audit des donateurs. Lorsque leur conservation est nécessaire, un stockage sécurisé et sûr doit être garanti pour éviter que les données sensibles ne soient mal utilisées ou exposées de manière irresponsable. Toutes les

[17] En ce qui concerne les organisations du système des Nations Unies, le HLCM a adopté les Personal Data Protection and Privacy Principles, qui doivent servir de cadre fondamental pour le traitement des données personnelles par les entités des Nations Unies. Pour les organisations qui ne bénéficient pas de privilèges et d'immunités, il convient de se référer à la législation applicable en matière de protection des données ainsi qu'aux ensembles de principes et autres orientations auxquels ces organisations sont soumises.

[18] Pour plus d'informations sur le traitement des données personnelles et l'usage de 'consentement' en tant que base légitime dans l'action humanitaire, veuillez consulter le Manuel sur la protection des données dans l'action humanitaire du CICR (2020).

autres données peuvent être conservées indéfiniment, à condition que leur niveau de sensibilité soit réévalué à des moments appropriés, que des droits d'accès puissent être définis et mis en oeuvre et - pour les données anonymisées ou agrégées - qu'une évaluation de réidentification soit effectuée. Quel que soit le niveau de sensibilité, un calendrier de conservation doit indiquer quand les données doivent être détruites et comment les détruire de manière à rendre leur récupération impossible. Des durées spécifiques de conservation doivent être définies dans la mesure du possible et, lorsque ce n'est pas le cas, l'examen quant à la nécessité de conserver les données d'une période spécifique doit être déterminé.

Transparence
La gestion des données dans l'action humanitaire doit être effectuée de manière à offrir une transparence significative aux parties prenantes, plus particulièrement aux populations affectées. Cela doit inclure une information pertinente quant à l'activité de gestion des données et ses résultats escomptés, ainsi que le partage des données de manière à promouvoir une véritable compréhension de l'activité de gestion des données, de son objectif, de l'utilisation et du partage ultérieur prévus, ainsi que les éventuelles limites et risques associés.

Les actions recommandées pour la Responsabilité des données dans le contexte de la réponse humanitaire

Cette section présente les actions recommandées pour mettre en œuvre la Responsabilité des données au niveau du système (1), au niveau des clusters/secteurs (2), et au niveau des organisations (3). Ces actions représentent les leviers les plus puissants pour viser un impact collectif et organisationnel en matière de Responsabilité des données. En pratique, il s'agit également d'un ensemble d'actions recommandées que la communauté humanitaire doit s'efforcer de maintenir.

Ces actions s'appliquent à tous les contextes de réponse humanitaire. Comme l'adoption de la Responsabilité des données varie selon les contextes d'intervention, ces actions vont servir de socle commun pour l'adaptation et la mise en œuvre dans le contexte ; en fonction de la nature d'une crise particulière. Si certaines de ces actions peuvent être nouvelles au niveau du système, du cluster/secteur et des organisations dans différents contextes, toutes les actions sont conçues pour s'appuyer sur les pratiques, processus et outils existants et visent à les compléter.

Les actions sont présentées selon une séquence logique à chaque niveau pour guider l'action progressive et l'amélioration constante. Les acteurs humanitaires et leurs partenaires devront identifier comment aborder la mise en œuvre de ces actions en fonction de la prise en compte actuelle de la Responsabilité des données dans le contexte.

Le tableau ci-dessous présente une **description de chaque action** et **son importance pour la Responsabilité des données**. Les sections suivantes sur les niveaux du système, du cluster/secteur, et des organisations décrivent **comment adapter ces actions à chaque niveau** et **qui doit être impliqué** dans ce processus. Ces sections incluent aussi des références à des exemples de modèles et outils (cf. annexe B) pour accompagner la mise en œuvre de ces différentes actions.

Les actions pour la Responsabilité des données dans l'action humanitaire		
Actions	**Description**	**Importance**
Diagnostic de la Responsabilité des données	Un diagnostic de la Responsabilité des données implique l'identification et l'examen des lois, normes, politiques et standards existants dans le contexte spécifique de la réponse, ainsi que des processus et procédures et des outils	Ce diagnostic aide à identifier des opportunités et défis communs pour la gestion responsable des données et informe la priorisation des actions pour la Responsabilité des données à différents niveaux d'une réponse.

	techniques pour la gestion des données.	
Carte de l'écosystème des données et registre des données	La carte de l'écosystème des données présente un résumé des activités de gestion des données, y compris l'échelle, la portée, et les types de données qui sont traitées, les parties prenantes, les flux de données entre les différents acteurs, ainsi que les processus et plateformes utilisés. Un registre de données présente le résumé des jeux de données clés qui sont générés et gérés par différents acteurs dans un contexte donné.	La carte de l'écosystème et le registre des données aident à identifier les lacunes et les duplications potentielles des données, soutiennent la complémentarité et la convergence (y compris avec des processus de développement orientés sur le long-terme), facilitent la collaboration, et permettent la priorisation et la prise de décisions stratégiques en matière de gestion responsable de données.
Analyse de l'impact des données[19]	Conduire une analyse de l'impact des données permet de déterminer les risques, les préjudices et les bénéfices envisagés, ainsi que les impacts d'une activité de gestion des données sur la vie privée, la protection des données, et/ou sur les droits humains.	Une analyse informe la conception et la mise en œuvre des activités de gestion de données de manière à maximiser les bénéfices et à minimiser les risques.
La Responsabilité des données à la conception	La Responsabilité des données dès la conception implique que les Principes pour la Responsabilité des données dans l'action humanitaire sont pris en compte dès le début d'une activité de gestion des données (y compris les phases de conception et de planification) et que l'adhésion à ces Principes peut être vérifiée tout au long du processus.	L'inclusion de la Responsabilité des données dans la conception, la mise en œuvre, le suivi et l'évaluation des activités de gestion des données contribue à atténuer les risques et maximiser les bénéfices.
Protocole de partage des informations & Classification de la sensibilité des données et informations	Un Protocole de partage des informations (PPI) doit inclure une classification de la sensibilité des données et informations pour le contexte spécifique,[20] les actions communes en vue de promouvoir la Responsabilité des données, des clauses quant au respect de la protection des données personnelles au besoin, et aussi inclure des instructions quant au traitement des incidents.	Un PPI établit la base fondatrice pour une approche collective de l'échange responsable de données et d'informations. Bien qu'ils soient généralement établis au niveau du système, les PPI peuvent également être établis au niveau des clusters/secteurs et des organisations, au besoin.

[19] 'Analyse de l'impact des données' est un terme générique qui fait référence à de multiples types d'évaluations, telles que définies dans l'annexe A. Notez qu'une analyse de l'impact sur la protection des données (AIPD) est l'outil et le processus établi dans la législation sur la protection des données qui doit être utilisé (spécifiquement) pour évaluer les risques liés à la protection des données personnelles.

[20] La classification de la sensibilité des données et informations indique le niveau de sensibilité de différents types de données et informations dans un contexte spécifié. Elle doit être développée de manière collective avec les différentes parties prenantes pour s'accorder sur la sensibilité dans leur contexte spécifique.

Accord de partage des données	Un accord de partage des données (APD) établit les modalités qui régissent le partage des données personnelles ou des données sensibles non personnelles. Il est utilisé surtout pour le partage de données bilatéral et est typiquement établi au niveau national. Conformément aux cadres de la protection des données, la signature d'un APD est obligatoire pour le partage de données personnelles.	Ce type d'accord est essentiel pour le respect des obligations juridiques, politiques, et normatives quant au partage des données personnelles et, dans certains cas, des données sensibles non personnelles.
Gestion des incidents liés aux données[21]	Afin de gérer, répertorier et communiquer sur les incidents liés aux données, il faut établir une procédure opérationnelle standard pour la gestion des incidents et un registre central qui reflète les détails clés concernant la nature, la sévérité et la résolution de chaque incident.	La gestion des incidents des données permet de réduire le risque qu'un incident se reproduise, de soutenir le développement d'une base de connaissances communes et de favoriser des approches plus coordonnées en matière de gestion de tels incidents au fil du temps.
Coordination et prise de décisions sur l'action collective pour la Responsabilité des données	Des mécanismes existants peuvent être employés pour coordonner et prendre des décisions sur l'action collective pour la Responsabilité des données aux différents niveaux d'une réponse humanitaire. Ceci inclut, entre autres, l'Équipe humanitaire du pays (EHP, ou HCT en anglais), le mécanisme de coordination inter-clusters, et les clusters/secteurs.	La coordination et l'action collective aident la communauté humanitaire à suivre les progrès et les défis, et à identifier les possibilités d'améliorer la Responsabilité des données. Elles permettent également de favoriser la redevabilité et l'investissement conjoint dans la mise en œuvre des autres actions de ce guide opérationnel.

Niveau 1: Les actions pour la Responsabilité des données au niveau du système

Pour faire progresser la Responsabilité des données au niveau du système, une action collective dans un certain nombre de domaines est nécessaire. Le bureau du Coordonnateur résident/humanitaire, l'équipe humanitaire du pays, OCHA ou HCR,[22] ainsi que d'autres

[21] Pour plus d'informations sur la gestion des incidents liés aux données, veuillez consulter : OCHA Centre for Humanitarian Data, *Guidance Note: Data Incident Management* (2019), disponible à l'adresse : https://centre.humdata.org/wp-content/uploads/2019/08/guidanceNote2_dataincidentmanagement.pdf.

[22] Les Directives opérationnelles proposent des rôles et des responsabilités conformes aux structures de coordination introduites par l'approche des clusters. Il reconnaît la responsabilité globale des autorités nationales, qu'il cherche à soutenir en favorisant une

structures de coordination, telles que l'ICCM/ICCG/ISCG, l'IMWGm et le Forum ONG ont des rôles importants à jouer pour soutenir ces actions.

Étant donné que les niveaux de prise en compte de la Responsabilité des données varient souvent au sein et à travers des contextes de réponse humanitaire, ces actions doivent servir de socle commun pour l'adaptation et la mise en œuvre dans le contexte donné. Si certaines actions peuvent être nouvelles au niveau du système dans certains contextes, toutes les actions sont conçues pour s'appuyer sur et compléter les pratiques, processus et outils qui existent déjà au sein du secteur humanitaire. Des rôles et responsabilités spécifiques sont définis dans le tableau ci-dessous pour appuyer la mise en œuvre de chaque action.

À travers ces actions, les organisations humanitaires doivent s'assurer d'un engagement significatif avec les organisations et les autorités nationales, selon le contexte donné.[23] Un tel engagement va permettre de renforcer la capacité de réponse des acteurs nationaux, instaurer la confiance et créer un espace favorable à la collaboration productive et à la gestion des questions liées aux données.

Actions pour la Responsabilité des données au niveau du système		
Actions	**Approche recommandée**	**Rôles et Responsabilités**
Mener un diagnostic de la Responsabilité des données au niveau du système **[Annexe B : modèle de diagnostic de la prise en compte de la Responsabilité des données]**	Le diagnostic de la Responsabilité des données au niveau du système présente un aperçu des mesures en vigueur en matière de Responsabilité des données entre les agences, les clusters et les secteurs. Le diagnostic facilite la prise de décision conjointe sur la manière de cibler et de prioriser l'action collective en matière de Responsabilité des données. S'il n'existe pas de cartographie de l'écosystème des données au niveau du système, dans l'idéal, cette démarche est à mener ensemble.	Ce diagnostic doit être réalisé annuellement par **le(s) mécanisme(s) inter-agence(s) compétent(s)** (le **ICCM/ICCG/ISCG** et le **IMWG**) avec le soutien de OCHA. Le diagnostic doit être présenté à l'EHP pour référence et comme outil de suivi des progrès quant aux questions clés en matière de renforcement de la Responsabilité des données.
Créer et maintenir à jour une cartographie de l'écosystème de	La cartographie de l'écosystème des données, au niveau du système, présente un résumé des activités de	La cartographie de l'écosystème doit être revue et mise à jour annuellement par **le(s) mécanisme(s) inter-agence(s) compétent(s)** (le

action coordonnée pour la responsabilité des données. Dans les situations concernant les réfugiés et autres personnes relevant de son mandat, le HCR est chargé de coordonner tous les aspects de la réponse humanitaire.

[23] Un tel engagement doit s'aligner aux directives opérationnelles de l'IASC suivantes: IASC *Operational Guidance for Cluster Lead Agencies on Working With National Authorities* (2011), disponibles ici : https://www.alnap.org/help-library/iasc-operational-guidance-for-cluster-lead-agencies-on-working-with-national, en fonction du rôle des autorités nationales dans la réponse, et l'engagement doit être réalisé en coordination avec les mécanismes inter-clusters/inter-secteurs pertinents.

données au niveau du système **[Annexe B : modèle de cartographie de l'écosystème des données]**	gestion des données dans le cadre d'une réponse humanitaire. La création d'une cartographie de l'écosystème nécessite la participation et la contribution des clusters/secteurs et d'autres entités inter-agences, ainsi que des organisations dont les activités ne seraient pas répertoriées autrement.	**ICCM/ICCG/ISCG** et le **IMWG**) et doit être présentée à **l'EHP** pour référence.
Développer et maintenir un Protocole de partage des informations au niveau du système **[Annexe B : modèle de protocole de partage des données]**	Le Protocole de partage des informations (PPI) est le document principal qui détermine l'échange des données et informations dans le cadre d'une réponse humanitaire. Un PPI doit inclure une classification de la sensibilité des données et informations en fonction du contexte spécifique, indiquant le degré de sensibilité et le protocole de divulgation relatifs aux principaux types de données existant dans la réponse.	Le PPI doit être développé de manière collective et sous la direction de(s) **mécanisme(s) inter-agence(s) compétent(s)** (le **ICCM/ICCG/ISCG** et le **IMWG**) avec le soutien de OCHA. Le PPI doit être présenté à l'**EHP** pour revue et approbation. Tous les acteurs impliqués dans la gestion des données doivent être au courant du PPI et des obligations qu'il contient.
Répertorier et communiquer au sujet des incidents liés aux données.	Au niveau du système, le suivi des incidents liés aux données et la communication à leur sujet doivent inclure un registre central qui répertorie les détails clés concernant la nature, la sévérité et les modalités de résolution de chaque incident. Le cas échéant, ce registre peut être relié à d'autres processus et outils de suivi des incidents déjà en place au niveau du système, par exemple les systèmes de surveillance de la sécurité et des accès. Des mesures de confidentialité et de protection des données sensibles doivent être prises lors de la création d'un tel registre.	Le **ICCM** et le **IMWG** sont responsables de la mise en place et le maintien d'un registre central d'incidents et des rapports réguliers à l'EHP. Ce registre doit être alimenté par les contributions des clusters/secteurs, ainsi que des organisations. L'**EHP,** avec le soutien de OCHA, est responsable du suivi des incidents liés aux données au niveau du système.
Soutenir la coordination et la prise de décision quant aux actions collectives liées à la Responsabilité des	Les structures inter-agences et inter-cluster/intersectorielles doivent créer un forum ou une plateforme commune pour la coordination et la prise de décision sur la Responsabilité des données au niveau du système. Ces	L'**EHP** est responsable de suivre les questions relatives à la Responsabilité des données, quand nécessaire. Le **ICCM** et le **IMWG** sont responsables de fournir des rapports réguliers à l'**EHP** sur leurs périmètres

données via les mécanismes inter-agences existants	structures devraient également faire le suivi des progrès collectifs et/ou des défis et opportunités en matière de Responsabilité des données dans le contexte spécifique.	respectifs en matière de Responsabilité des données.

Niveau 2: Les actions pour la Responsabilité des données au niveau des clusters/secteurs

Pour faire progresser la Responsabilité des données au niveau des clusters/secteurs, une action collective dans un nombre de domaines est nécessaire, et complétera les actions au niveau du système et au niveau des organisations. Les actions élaborées ci-dessous doivent être mises en œuvre conformément aux autres lignes directrices de l'IASC et des clusters/secteurs individuels.

Étant donné que les niveaux de prise en compte de la Responsabilité des données varient souvent au sein et à travers des contextes de réponse humanitaire, ces actions doivent servir de socle commun pour l'adaptation et la mise en œuvre dans le contexte donné. Si certaines actions peuvent être nouvelles au niveau des clusters/secteurs dans certains contextes, toutes les actions sont conçues pour s'appuyer sur et compléter les pratiques, processus et outils qui existent déjà au sein du secteur humanitaire. En fonction de la nature de l'environnement d'intervention, ces actions peuvent être mises en œuvre par les Leads et Co-Leads des clusters/secteurs et leurs partenaires tant au niveau national que local.

Les agences impliquées sont responsables de s'assurer que les actions entreprises s'intègrent bien dans le périmètre d'action d'une réponse particulière (c'est-à-dire les actions des agences Lead ou Co-Lead du cluster, et les actions de l'une de leurs organisations partenaires agissant au nom du cluster/secteur). Ces actions incluent notamment des efforts visant à promouvoir l'adhésion aux lois (le cas échéant), normes, politiques et standards mondiaux et nationaux en matière de protection des données.

Dans le cadre de ces actions, les clusters/secteurs doivent s'assurer d'un engagement significatif[24] avec les organisations et les autorités nationales et locales, ainsi qu'avec toute autre partie prenante concernée. Un tel engagement peut renforcer la capacité de réponse des acteurs nationaux, instaurer la confiance et créer un espace pour une collaboration productive et la gestion des questions liées aux données.

Actions pour la Responsabilité des données au niveau des clusters/secteurs		
Actions	**Approche recommandée**	**Rôles et Responsabilités**
Mener un diagnostic de la Responsabilité des données au niveau	Le diagnostic de la Responsabilité des données au niveau des clusters/secteurs présente un aperçu des mesures en matière de Responsabilité des données en vigueur au sein des clusters/secteurs. Le	Ce diagnostic doit être réalisé ou mis à jour annuellement (ou plus fréquemment si nécessaire, notamment en cas de changement significatif dans la

[24] Un tel engagement doit s'aligner aux directives opérationnelles de l'IASC suivantes: IASC Operational Guidance for Cluster Lead Agencies on Working With National Authorities (2011), disponible ici: https://www.alnap.org/help-library/iasc-operational-guidance-for-cluster-lead-agencies-on-working-with-national, en fonction du rôle des autorités nationales dans la réponse, et l'engagement doit être réalisé en coordination avec les mécanismes inter-clusters/inter-secteurs pertinents.

des clusters/secteurs. **[Annexe B : modèle de diagnostic de la prise en compte de la Responsabilité des données]**	diagnostic facilite la prise de décision conjointe sur la manière de cibler et de prioriser l'action collective en matière de Responsabilité des données. Il complète (enrichissant ou s'appuyant sur) le diagnostic au niveau du système.	nature ou la structure de la réponse) par les agences Lead et Co-Lead des clusters/secteurs en collaboration avec leurs partenaires.
Créer et maintenir à jour une cartographie de l'écosystème de données et un registre des sources de données au niveau des clusters/secteurs. **[Annexe B : modèle de cartographie de l'écosystème des données]**	La cartographie de l'écosystème des données, au niveau des clusters/secteurs, répertorie toutes les activités de gestion des données en lien avec les principales interventions de la réponse au sein des clusters/secteurs. Le registre des données au niveau des clusters/secteurs doit répertorier toutes les 'sources' de données liées aux activités identifiées dans la cartographie de l'écosystème. Ensemble, ces deux actions permettent d'éviter la duplication des efforts et de soutenir le partage des données au sein du cluster/secteur et de façon plus large, pour l'ensemble de la réponse. Elles apportent également les contributions du cluster/secteur à l'exercice de cartographie de l'écosystème de données au niveau du système.	L'exercice de cartographie de l'écosystème des données au niveau du cluster/secteur et le registre des sources de données doivent être complétés et mis à jour sur une base annuelle par les **agences Lead et Co-Lead des clusters/secteurs** en collaboration avec leurs **partenaires**.
Développer et maintenir un Protocole de partage des informations au niveau des clusters/secteurs. **[Annexe B : modèle de protocole de partage des données]**	Dans les cas où un cluster/secteur identifie des problèmes communs spécifiques à la gestion des données au sein de leur cluster/secteur et qui ne sont pas suffisamment traités dans le PPI en vigueur au niveau du système, un PPI supplémentaire doit être développé pour répondre à ces besoins et doit être approuvé par tous les membres du cluster/secteur. Le PPI spécifique au cluster/secteur doit être cohérent sur le PPI au niveau du système et le compléter, ainsi que s'aligner sur les lois, normes, politiques et standards pertinents applicables dans le contexte spécifique. *Remarque : si les membres du cluster/secteur prévoient de partager des données personnelles entre eux, ils doivent établir des accords de partage de données*	Le PPI doit être développé de manière collective et sous le direction de(s) **agence(s) Lead et Co-Lead des clusters/secteurs** en collaboration avec leurs partenaires. Le PPI doit être approuvé par tous les partenaires des clusters/secteurs et présenté au mécanisme inter-agence compétent pour référence.

	à cette fin (voir plus loin au Niveau 3 : actions pour la Responsabilité des données au niveau des organisations).	
Proposer un appui technique et consultatif aux membres du cluster/secteur sur le sujet de la Responsabilité des données	Des ressources humaines et financières dédiées à la Responsabilité des données au niveau du cluster/secteur sont essentielles pour renforcer la prise en compte du sujet au sein du cluster/secteur lui-même et parmi ses membres. Ceci est particulièrement important lorsque les membres entreprennent ou participent à des activités conjointes de gestion des données au nom ou pour le bénéfice du cluster/secteur dans son ensemble. Les contenus relatifs à la responsabilité en matière de données (par exemple, comment mener des évaluations d'impact sur les données et transférer en toute sécurité des données sensibles) devraient être intégrés dans les activités de développement des capacités au niveau du cluster/secteur.	Les **agences Lead et Co-Lead des clusters/secteurs** ont la responsabilité de promouvoir les ressources nécessaires et les activités de renforcement des capacités pertinentes.
Définir les activités de gestion des données au niveau des clusters/secteurs de façon à mettre en oeuvre la Responsabilité des données	Afin d'exposer les membres du cluster/secteur à différentes mesures et stratégies pour une gestion sécurisée, éthique et efficace des données, il faut modéliser différentes approches de la gestion responsable des données à travers des activités conjointes ou communes (par exemple, des évaluations conjointes des besoins). Les clusters/secteurs peuvent également souhaiter développer et soutenir l'utilisation de normes et d'outils communs pour les activités de gestion des données menées par les clusters/secteurs afin de favoriser une approche cohérente parmi les membres.	Les **agences Lead et Co-Lead des clusters/secteurs** doivent s'efforcer de concevoir des activités de gestion des données menées par les clusters conformément à ces directives opérationnelles. Cela peut se faire, par exemple, en incluant la Responsabilité des données dans les stratégies des clusters.
Répertorier et communiquer au sujet des incidents liés aux données	Le suivi et la communication des incidents au sein du cluster/secteur contribuent à réduire le risque de répétition des incidents. Un cluster/secteur doit contribuer activement au suivi des incidents liés aux	Les agences Lead et Co-Lead des clusters/secteurs ont la responsabilité d'établir et de maintenir un registre des incidents liés aux données qui se

au sein du cluster/secteur.	données au niveau du système afin de partager les ‘leçons apprises’ et les bonnes pratiques pour atténuer les risques au sein de la communauté au sens large. Au niveau du cluster/secteur, cela peut inclure un registre central qui répertorie les détails clés sur la nature, la gravité et les modalités de résolution des incidents. Un tel registre doit garantir que des mesures adéquates en matière de confidentialité et de protection des données sensibles sont mises en œuvre.	produisent dans le cadre des activités de gestion des données menées par les clusters/secteurs. Ils doivent également veiller à ce que ces incidents et les leçons qui en découlent soient partagés avec les organes et forums compétents au niveau du système.

Niveau 3: Les Actions pour la Responsabilité des données au niveau des organisations

Essentiel au succès des actions de Responsabilité des données au niveau du système et des groupes/secteurs, le sujet doit également progresser au niveau des organisations dans un contexte d'intervention donné. Les actions figurant dans le tableau ci-dessous doivent être mises en œuvre conformément aux politiques et directives organisationnelles associées. En aucune façon, elles n'affectent ni ne remplacent les obligations contenues dans les politiques organisationnelles ou les cadres juridiques et réglementaires déjà en place. Les actions recommandées sont conçues pour être mises en œuvre par les bureaux et/ou équipes des organisations dans un contexte donné (par exemple, les bureaux et équipes de pays ou de zone).

Étant donné que les niveaux de prise en compte de la Responsabilité des données varient souvent au sein et à travers les contextes de réponse humanitaire, ces actions doivent servir de socle commun pour l'adaptation et la mise en œuvre dans le contexte donné. Si certaines actions peuvent être nouvelles au niveau des organisations dans certains contextes, toutes les actions sont conçues pour s'appuyer sur et compléter les pratiques, processus et outils qui existent déjà au sein du secteur humanitaire.

Compte tenu de la diversité des fonctions et des capacités des organisations humanitaires, les présentes Directives opérationnelles n'attribuent pas de rôles et de responsabilités spécifiques en matière de Responsabilité des données au niveau des organisations. Dans la mesure du possible, les organisations doivent intégrer les actions décrites ci-dessous dans les rôles et responsabilités des équipes et fonctions déjà existantes qui sont impliquées dans la gestion des données opérationnelles dans les différents environnements de réponse.

Les actions pour la Responsabilité des données au niveau des organisations	
Actions	**Approche recommandée**
Mener un diagnostic de la Responsabilité des données au niveau des organisations. **[Annexe B : modèle de diagnostic de la prise en compte de la Responsabilité des données]**	Au niveau des organisations, le diagnostic de la Responsabilité des données présente un aperçu des mesures en matière de Responsabilité des données en vigueur au sein d'un bureau d'une organisation dans un contexte humanitaire donné. Le diagnostic facilite la priorisation de l'action collective en matière de Responsabilité des données. Il favorise également l'identification des opportunités de collaboration et d'action collective en matière de Responsabilité des données au sein des groupes/secteurs (et autres forums inter-agences) dont l'organisation est membre. Ce diagnostic doit être réalisé annuellement ou lorsque les circonstances d'une réponse et/ou les politiques et/ou pratiques de gestion des données d'une organisation changent de manière significative.

Créer et maintenir à jour un registre de sources de données et participer aux exercices de cartographie de l'écosystème des données.	Les organisations doivent faire le suivi de toutes les activités de gestion des données (par exemple les évaluations, le suivi des réponses, et l'analyse de situations) qu'elles mènent ou dans lesquelles elles interviennent via un registre central de données. Au niveau des organisations, le registre des données peut également révéler des lacunes dans les données d'une organisation. Les organisations doivent se référer à ce registre lorsqu'elles contribuent aux exercices de cartographie de l'écosystème de données du cluster/secteur et du système, et, le cas échéant, avant d'entreprendre toute nouvelle collecte de données. Le registre doit être mis à jour régulièrement et être largement diffusé au sein de l'organisation en tant que référence institutionnelle.
Mener une analyse de l'impact des données pour les activités de gestion des données gérées par l'organisation. **[Annexe B: Modèle de l'analyse de l'impact des données]**	Des analyses de l'impact des données (AID) doivent être effectuées avant le début et pendant les activités de gestion des données afin d'informer la planification, la conception, la mise en œuvre et les révisions du projet. Les analyses de l'impact des données doivent être menées de manière inclusive, en impliquant les populations concernées dans la mesure du possible. Une activité de gestion des données devrait être remodelée ou annulée si les risques prévisibles dépassent les bénéfices escomptés, et ce, malgré les mesures de prévention et d'atténuation. Les résultats des AID doivent être partagés à l'interne, au sein de l'organisation, et, dans certains cas, à l'externe avec les acteurs clés impliqués dans une activité de gestion des données et/ou dans la planification d'une activité similaire dans le contexte spécifique. Cela favorise la cohérence dans l'évaluation, le suivi et l'atténuation des risques liés aux données au fil du temps. Note : De nombreuses organisations ont des politiques, des exigences et des lignes directrices spécifiques sur la façon dont les AID doivent être menées. Pour celles qui ne le font pas, le modèle présent en Annexe B peut servir de référence utile.
Définir les activités de gestion des données au niveau des organisations de façon à mettre en oeuvre la Responsabilité des données	Les organisations doivent intégrer la Responsabilité des données dans les activités de gestion des données dès leur conception, c'est-à-dire dès l'étape de planification d'un exercice particulier. Cela comprend par exemple les étapes et considérations suivantes : - Résoudre les points identifiés dans l'évaluation de l'impact des données pour une activité donnée par la mise en place de mesures de prévention et d'atténuation appropriées, réalisables et solides pour tous les risques majeurs identifiés. - Lors du choix des outils de gestion des données, favoriser la complémentarité, l'interopérabilité (si pertinent) et l'harmonisation (y compris en ce qui concerne la structure des données).

	- Promouvoir les mesures de gestion sécurisée des données (par exemple, application du contrôle de la divulgation statistique[25] pour les microdonnées provenant d'enquêtes ou d'évaluations, fourniture d'un espace de stockage sécurisé, etc.). - Adhérer aux orientations et protocoles adéquats en matière de Responsabilité des données et aux processus et procédures connexes, y compris les PPI au niveau du système et/ou au niveau des clusters/secteurs concernés. Il s'agit notamment de s'assurer que toutes les données qui doivent être partagées pour une finalité spécifique sont mises à disposition par les canaux appropriés de manière sécurisée, éthique et efficace, avec les garanties de protection nécessaires pour les données personnelles et en conformité avec les cadres de protection des données applicables. - Les organisations doivent établir et communiquer clairement sur la manière dont les personnes peuvent accéder, vérifier, rectifier et/ou supprimer leurs données.
Établir des accords de partage des données afin de réguler le transfert des données et/ou sensibles **[Annexe B: Modèle d'accord de partage des données**	Les organisations doivent conclure des accords de partage des données lorsqu'elles partagent des données personnelles ou des données sensibles non personnelles, conformément aux obligations institutionnelles, juridiques et réglementaires appropriées ; ainsi qu'aux Principes pour la Responsabilité des données dans l'action humanitaire. Note : Bien que les circonstances du partage des données diffèrent trop pour qu'il soit possible de fournir un modèle unique d'accord de partage des données, le modèle figurant à l'annexe B offre un ensemble de points à prendre en compte dans l'élaboration de tels accords, au cas où des modèles n'existeraient pas déjà (dans la pratique ou les politiques) au sein de l'organisation.
Établir une procédure opérationnelle standard pour traiter les incidents liés aux données **[Annexe B: Modèle de procédure opérationnelle standard pour le traitement des incidents liés aux données]**	Les organisations doivent développer et mettre en place des procédures opérationnelles standards pour la gestion des incidents liés aux données. Ces procédures doivent inclure des processus pour la notification, la classification, le traitement et la fermeture des incidents. Elles doivent aussi inclure l'enregistrement des incidents dans la base de connaissances de l'organisation (par exemple en utilisant un registre central qui répertorie les détails clés concernant la nature, la sévérité et la résolution de chaque incident). Ces procédures doivent énoncer les moyens appropriés mis en œuvre pour la correction et la réparation vis-à-vis des individus qui sont touchés par l'incident des données. Les organisations doivent partager leur expérience en matière de gestion et d'atténuation des incidents des données avec d'autres acteurs, c'est-à-dire aux niveaux du groupe/secteur et du système.

[25] Le contrôle de la divulgation statistique (CDS) est une technique utilisée en statistique pour évaluer et réduire le risque qu'une personne ou une organisation soit ré-identifiée à partir des résultats d'une analyse de données d'enquête ou administratives, ou lors de la publication de microdonnées. Pour plus d'informations, veuillez consulter: The Centre for Humanitarian Data, *Guidance Note: Statistical Disclosure Control* (2019), https://centre.humdata.org/guidance-note-statistical-disclosure-control/.

Annexe A: Définitions

Données agrégées : Données accumulées obtenues en combinant des données au niveau individuel. Il s'agit de données qui sont (1) collectées à partir de plusieurs sources et/ou plusieurs mesures, variables ou individus et (2) compilées dans des résumés de données ou des rapports de synthèse, généralement à des fins de rapport public ou d'analyse statistique.

Anonymisation : Processus par lequel des données personnelles sont modifiées de manière irréversible, soit en supprimant, soit en modifiant les variables d'identification, de telle sorte qu'une personne concernée ne puisse plus être identifiée directement ou indirectement.[26]

Consentement : Le consentement est la base juridique la plus fréquemment utilisée et souvent privilégiée pour le traitement des données personnelles. Cependant, étant donné la vulnérabilité de la plupart des bénéficiaires et la nature des urgences humanitaires, de nombreuses organisations humanitaires ne seront pas en mesure de s'appuyer sur le consentement pour la plupart de leurs traitements de données personnelles.[27]

Données : Représentation ré-interprétable de l'information, de manière formalisée qui convient à la communication, l'interprétation ou le traitement.[28]

Sources de données : Sont considérés comme des sources de données l'ensemble de données ou d'informations, défini et géré en tant qu'une entité unique afin que cet ensemble puisse être compris, partagé, protégé et exploité efficacement.[29]

Registre des données : Un registre des sources de données fournit un résumé des principaux jeux de données générés et gérés par différents acteurs dans un contexte donné.

Cartographie de l'écosystème de données : Une cartographie de l'écosystème des données fournit un résumé des principales activités de gestion des données, y compris l'échelle, la portée et les types de données traitées, les parties prenantes impliquées, les flux de données entre les différents acteurs, ainsi que les processus et les plateformes utilisés.

Analyse de l'impact des données : Une analyse de l'impact des données est un terme générique pour une variété d'outils qui sont utilisés pour déterminer les conséquences positives et négatives d'une activité de gestion des données. Il s'agit notamment d'outils couramment utilisés - et parfois légalement requis - tels que les analyses de l'impact sur la protection des données et les analyses de l'impact sur la vie privée.

Incidents liés aux données : Des événements impliquant la gestion des données, tels que la perte, la destruction, l'altération, l'acquisition ou la divulgation de données et d'informations,

---

[26] UN OCHA Centre for Humanitarian Data, *Glossary*: https://centre.humdata.org/glossary/.

[27] UNHCR, *Guidance on the Protection of Personal Data of Persons of Concern to UNHCR* (2018), https://www.refworld.org/docid/5b360f4d4.html.

[28] UN, *Data Strategy of the Secretary-General for Action by Everyone, Everywhere with Insight, Impact and Integrity, 2020-22* (2020), https://www.un.org/en/content/datastrategy/index.shtml.

[29] United Kingdom National Archives, *Information Asset Fact Sheet* (2017), https://www.nationalarchives.gov.uk/documents/information-management/information-assets-factsheet.pdf.

provoqués de façon accidentelle ou au contraire intentionnelle, avec des objectifs, illégaux ou autrement non autorisés, causant des dommages ou en ayant le potentiel.[30]

Minimisation des données : L'objectif de garantir qu'on ne traite que la quantité minimale de données personnelles nécessaire pour atteindre l'objectif et les finalités pour lesquels les données ont été collectées.[31]

Qualité des données : Un ensemble de caractéristiques qui visent à préparer les données pour l'objectif pour lequel elles sont traitées. La qualité des données comprend des éléments tels que l'exactitude, la pertinence, la suffisance, l'intégrité, l'exhaustivité, la facilité d'utilisation, la validité, la cohérence, la ponctualité, l'accessibilité, la comparabilité et la temporalité appropriée.[32]

Protection des données : L'application systématique d'un ensemble de mesures institutionnelles, techniques et physiques qui préservent le droit à la vie privée dans le cadre du traitement des données personnelles.[33]

Analyse de l'impact sur la protection des données : Un outil et processus permettant d'évaluer les impacts sur la protection des personnes concernées par le traitement de leurs données personnelles et d'identifier les actions correctives nécessaires pour éviter ou minimiser ces impacts.[34]

Responsabilité des données : Un ensemble de principes, procédures et outils qui soutiennent la gestion sécurisée, éthique et efficace des données dans l'action humanitaire.[35]

Sécurité des données : Un ensemble de mesures physiques, technologiques et procédurales qui préservent la confidentialité, l'intégrité et la disponibilité des données et empêchent leur perte, destruction, altération, acquisition ou divulgation, accidentelle ou intentionnelle, illégale ou non autorisée.[36]

Sensibilité des données : Classification des données en fonction de la probabilité et de la sévérité des dommages potentiels qui peuvent se matérialiser du fait de leur exposition dans un contexte particulier.[37]

Accord de partage des données : Accord qui établit les modalités régissant le partage des données personnelles ou des données sensibles non personnelles. Il est utilisé surtout pour le partage de données entre deux parties et est typiquement établi au niveau national. Conformément aux cadres de la protection des données, la signature d'un APD est obligatoire

---

[30] The Centre for Humanitarian Data, *Guidance Note: Data Incident Management* (2019), https://centre.humdata.org/wp-content/uploads/2019/08/guidanceNote2_dataincidentmanagement.pdf.

[31] ICRC, *Handbook on Data Protection in Humanitarian Action* (2020), https://www.icrc.org/en/data-protection-humanitarian-action-handbook.

[32] UN OCHA, *OCHA Data Responsibility Guidelines (Working Draft)* (2019), https://centre.humdata.org/wp-content/uploads/2019/03/OCHA-DR-Guidelines-working-draft-032019.pdf.

[33] Définition développée par le UN Privacy Policy Group (2017).

[34] UNHCR, *Policy on the Protection of Personal Data of Persons of Concern to UNHCR* (2015), https://www.refworld.org/pdfid/55643c1d4.pdf.

[35] UN OCHA, *OCHA Data Responsibility Guidelines (Working Draft)* (2019), https://centre.humdata.org/wp-content/uploads/2019/03/OCHA-DR-Guidelines-working-draft-032019.pdf.

[36] The Centre for Humanitarian Data. *Glossary*: https://centre.humdata.org/glossary/.

[37] The Centre for Humanitarian Data. *Glossary*: https://centre.humdata.org/glossary/.

pour le partage de données personnelles.

Personne concernée : Une personne physique (c'est-à-dire un individu) dont les données personnelles font l'objet d'un traitement, et qui peut être identifiée, directement ou indirectement, par référence à ces données et à des mesures raisonnablement probables. La nomination en tant que personne concernée est liée à un ensemble de droits spécifiques auxquels elle a droit en ce qui concerne ses données personnelles, y compris lorsque ces données sont recueillies, collectées ou autrement traitées par d'autres.[38]

Risque/Préjudice : Implications négatives d'une initiative de traitement des données sur les droits d'une personne ou d'un groupe de personnes concernées, y compris, mais sans s'y limiter, les préjudices physiques et psychologiques, la discrimination et le refus d'accès aux services.[39]

Produit d'information : Produit basé sur des données brutes qui a pour but de transmettre l'information voulue aux utilisateurs (par exemple, infographies, graphiques, cartes, rapports de situation, etc.).

Microdonnées : Données d'observation sur les caractéristiques des unités statistiques d'une population - telles que les individus, les ménages ou les établissements - recueillies dans le cadre d'exercices tels que les enquêtes sur les ménages, l'évaluation des besoins ou les activités de suivi.[40]

Données à caractère non personnel : Toute information ne se rapportant pas à une personne concernée. Les données non personnelles peuvent être classées en fonction de leur origine, à savoir : les données qui ne se rapportent jamais à une personne concernée, telles que les données sur le contexte dans lequel une réponse humanitaire est en cours, ainsi que les données sur les acteurs humanitaires et leurs activités ; *ou* 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 exposées, et leurs capacités. Les données à caractère non personnel incluent les informations démographiquement identifiables (Demographically Identifiable Information, ou DII en anglais), à savoir les données qui permettent l'identification d'un groupe d'individus par des facteurs géographiques définis, tels que l'ethnicité, le sexe, l'âge, l'occupation, la religion ou la localisation.

Gestion opérationnelle des données : La conception des activités de gestion des données, incluant la collecte ou la réception de données, le stockage, le traitement, l'analyse, le partage, l'utilisation, la conservation et la destruction des données et des informations par des acteurs humanitaires. Ces activités font (pleinement) partie de l'action humanitaire, tout au long du cycle de planification et de réponse des clusters/secteurs et incluant de façon non exhaustive, les analyses de situation, les évaluations des besoins, la gestion des données démographiques,

---

[38] UN OCHA, *OCHA Data Responsibility Guidelines (Working Draft)* (2019), https://centre.humdata.org/wp-content/uploads/2019/03/OCHA-DR-Guidelines-working-draft-032019.pdf.

[39] ibid.

[40] The Centre for Humanitarian Data, *Guidance Note: Statistical Disclosure Control* (2019), https://centre.humdata.org/guidance-note-statistical-disclosure-control/.

l'enregistrement et l'inscription des bénéficiaires aux programmes d'aide, la gestion des cas, la communication avec les populations affectées, suivi des activités de protection, et le suivi et l'évaluation des réponses.

Données à caractère personnel : Toute information se rapportant à une personne physique identifiée ou identifiable ('la personne concernée'). Une personne physique est identifiable lorsqu'elle peut être identifiée, directement ou indirectement, notamment en faisant référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant numérique, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.[41]

Données primaires : Données qui ont été générées par le chercheur lui-même, à travers des enquêtes, entretiens, expériences, spécialement conçus pour comprendre et résoudre le problème de recherche en question.[42]

Vie privée : Nul ne sera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes illégales à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes.[43]

Ré-identification : Processus par lequel des données désidentifiées (anonymisées) peuvent être retracées ou reliées à un ou plusieurs individus ou groupe(s) d'individus par des moyens raisonnablement disponibles au moment de la réidentification des données.[44]

Données secondaires : Données recueillies à l'origine dans un but de recherche spécifique ou non (par exemple, un recensement national), et qui sont maintenant utilisées par d'autres chercheurs pour un objectif différent.

Les données sensibles : Les données classées comme sensibles en fonction de la probabilité et de la sévérité du préjudice qui est susceptible de résulter / se concrétiser / se matérialiser si elles sont divulguées dans un contexte particulier. Les données, qu'elles soient personnelles ou non, peuvent, toutes deux, être sensibles. Beaucoup d'organisations disposent de systèmes de classifications spécifiques quant à ce qui constitue des données sensibles, afin de faciliter les pratiques de gestion des données.[45]

Contrôle de la divulgation statistique : Technique utilisée en statistique pour évaluer et réduire le risque qu'une personne ou une organisation soit ré-identifiée à partir des résultats d'une analyse de données d'enquête ou administratives, ou lors de la diffusion de microdonnées.[46]

---

[41] UN OCHA, *OCHA Data Responsibility Guidelines (Working Draft)* (2019), https://centre.humdata.org/wp-content/uploads/2019/03/OCHA-DR-Guidelines-working-draft-032019.pdf.

[42] Public Health Research Guide, *Primary & Secondary Data Definitions:* https://researchguides.ben.edu/c.php?g=282050&p=4036581.

[43] UN General Assembly, *International Covenant on Civil and Political Right*s (1976), https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx.

[44] UN OCHA, *OCHA Data Responsibility Guidelines (Working Draft)* (2019), https://centre.humdata.org/wp-content/uploads/2019/03/OCHA-DR-Guidelines-working-draft-032019.pdf.

[45] The Centre for Humanitarian Data, *Glossary*, https://centre.humdata.org/glossary/.

[46] The Centre for Humanitarian Data, *Guidance Note on Statistical Disclosure Control* (2019), https://centre.humdata.org/guidance-note-statistical-disclosure-control/.

Annexe B: Modèles et outils pour promouvoir la responsabilité des données

Les modèles et outils suivants sont conçus pour soutenir la mise en œuvre des actions recommandées pour la Responsabilité des données présentées dans ce guide opérationnel.

Ces modèles et outils ne sont pas obligatoires. Ils sont plutôt fournis à titre d'exemples pour aider les organisations à mettre en pratique les actions présentées dans ces directives opérationnelles. Ils ne remplacent pas les modèles ou outils existants lorsque ceux-ci existent déjà dans une organisation, que ce soit par la pratique ou via des politiques internes.

Ces modèles et outils seront mis à jour en fonction des réactions reçues et des enseignements tirés de leur utilisation au fil du temps. Chaque modèle et outil comprend une section d'introduction décrivant l'objectif de l'outil, sa ou ses sources et son utilisation à ce jour (le cas échéant), ainsi que des instructions pour son adaptation et son utilisation.

- **Examples of Principles in Practice**
  - **Exemples des principes mis en pratique**
- **Data Responsibility Diagnostic Tool**
  - **Outil pour le diagnostic de la Responsabilité des données**
- **Data Ecosystem Map and Asset Registry Template**
  - **Carte de l'écosystème des données et registre de données**
- **Information Sharing Protocol Template (including a Data Sensitivity Classification)**
  - **Protocole de partage de l'information (et classification de la sensibilité)**
- **Data Sharing Agreement Builder**
  - **Modèle d'accord de partage des données**
- **Data Impact Assessment Template**
  - **Modèle d'évaluation de l'impact des données**
- **Standard Operating Procedure for Data Incident Management**
  - **Procédure opérationnelle standard (SOPs) pour la gestion d'incidents concernant les données**

Annexe C : Ressources et Références

Les documents suivants ont été inclus dans l'analyse documentaire qui a précédé le développement de ces Directives opérationnelles.

(Some of these resources do exist in French. Follow the below links and select the language option when available).

Brussels Privacy Hub (VUB) and International Committee of the Red Cross (ICRC), 2020. Handbook on Data Protection in Humanitarian Action (2nd edition): https://www.icrc.org/en/data-protection-humanitarian-action-handbook.

CARE (Kelly Church) and Linda Raftree, 2019. Responsible Data Maturity Model: https://careinternational.sharepoint.com/:b:/t/Digital/EeATyuHMQSFIoiBzgKHVFKwBuRgwhvQ8mHgTfloFglS1WQ?e=x0yEvz.

Catholic Relief Services, 2019. Responsible Data Values & Principles: https://www.crs.org/about/compliance/crs-responsible-data-values-principles.

CHS Alliance, Group URD and the Sphere Project, 2014. The Core Humanitarian Standard on Quality and Accountability: https://corehumanitarianstandard.org/files/files/Core%20Humanitarian%20Standard%20-%20English.pdf.

Commission Nationale Informatique & Libertés (CNIL). DPIA/PIA Guides and open source PIA software: https://www.cnil.fr/en/privacy-impact-assessment-pia.

DLA Piper, 2020. Data Protection Laws of the World: https://www.dlapiperdataprotection.com/.

ELAN/Cash Learning Partnership, 2018. Data Starter Kit for Humanitarian Field Staff: https://elan.cashlearning.org/.

European Union, 2018. General Data Protection Regulation (GDPR): https://ec.europa.eu/info/law/law-topic/data-protection_en and https://gdpr-info.eu/.

Foreign, Commonwealth & Development Office (FCDO). Personal Information Charter: https://www.gov.uk/government/organisations/foreign-commonwealth-development-office/about/personal-information-charter.

Grand Bargain Working Group on Workstream 5, co-convened by ECHO and OCHA, 2019: https://interagencystandingcommittee.org/grand-bargain/workstream-5-improve-joint-and-impartial-needs-assessments-january-2020-update.

Grand Bargain, 2019. Principles for Coordinated Needs Assessment Ethos: https://interagencystandingcommittee.org/system/files/ws5_-_collaborative_needs_assessment_ethos.pd.

Harvard Humanitarian Initiative (HHI), 2017. The Signal Code: A Human Rights Approach to Information During Crisis: https://hhi.harvard.edu/publications/signal-code-human-rights-approach-information-during-crisis.

Harvard Humanitarian Initiative (HHI), 2018. Signal Code: Ethical Obligations for Humanitarian Information Activities: https://hhi.harvard.edu/publications/signal-code-ethical-obligations-humanitarian-information-activities.

ICRC-led Advisory Group incl. DRC on "Professional Standards", 2018. Professional Standards for Protection Work; Chapter 6: Managing Data and Information for Protection Outcomes: https://www.icrc.org/en/publication/0999-professional-standards-protection-work-carried-out-humanitarian-and-human-rights.

Inter-Agency Standing Committee (IASC), 2008. Operational Guidance On Responsibilities Of Cluster/Sector Leads & OCHA In Information Management: https://www.humanitarianresponse.info/sites/www.humanitarianresponse.info/files/documents/files/IASC_operational_guidance_on_information_management.pdf.

Inter-Agency Standing Committee (IASC), 2016. Policy on Protection in Humanitarian Action: https://interagencystandingcommittee.org/protection-priority-global-protection-cluster/documents/iasc-policy-protection-humanitarian-action.

International Conference on Data Protection and Privacy Commissioners, 2009. Madrid Resolution: International Standards on the Protection of Personal Data and Privacy: http://privacyconference2011.org/htmls/adoptedResolutions/2009_Madrid/2009_M1.pdf.

International Organization for Migration (IOM), 2010. Data Protection Manual: https://publications.iom.int/books/iom-data-protection-manual.

International Organization for Migration (IOM), 2018. DTM & Partners Toolkit: Do No Harm Checklist and Guiding Questions for DTM and Partners: https://displacement.iom.int/dtm-partners-toolkit/field-companion-sectoral-questions-location-assessment.

International Organization for Migration (IOM), 2018. DTM & Partners Toolkit: Enhancing Responsible Data Sharing: https://displacement.iom.int/dtm-partners-toolkit/enhancing-responsible-data-sharing.

International Organization for Migration (IOM), 2018. DTM & Partners Toolkit: DTM Data Sharing Forms: https://displacement.iom.int/dtm-partners-toolkit/dtm-data-sharing-forms.

International Red Cross and Red Crescent Movement, 1994. Code of Conduct for the International Red Cross and Red Crescent Movement and Non-Governmental Organizations (NGOs) in Disaster Relief: https://www.icrc.org/en/doc/resources/documents/publication/p1067.htm.

International Rescue Committee (IRC), 2018. Obtaining meaningful informed consent: https://www.rescue.org/resource/obtaining-meaningful-informed-consent.

Médecins Sans Frontières, 2013. Data Sharing Policy: https://fieldresearch.msf.org/bitstream/handle/10144/306501/MSF+data+sharing+policy+final+061213.pdf;jsessionid=E85DF92F1427CE9A46DA5A06D8D6AED5?sequence=1.

MERL Tech/various. Responsible Data Hackpad: https://paper.dropbox.com/doc/Responsible-Data-Hackpad-SA6kouQ4PL3SOVa8GnMEY.

Office of the Australian Information Commissioner. Undertaking a Privacy Impact Assessment (Training): https://www.oaic.gov.au/s/elearning/pia/welcome.html.

Oxfam, 2015. Responsible Data Program Policy: https://policy-practice.oxfam.org.uk/publications/oxfam-responsible-program-data-policy-575950.

Oxfam, 2017. Responsible Data Management Training Pack: https://policy-practice.oxfam.org.uk/our-approach/toolkits-and-guidelines/responsible-data-management.

Principles for Digital Development, 2017: https://digitalprinciples.org.

Protection Information Management (PIM) Initiative, 2015. PIM Principles: http://pim.guide/guidance-and-products/product/principles-protection-information-management-may-2015/.

Protection Information Management (PIM) Initiative, 2017. PIM Quick Reference Flyer (PIM Process, Matrix & Principles): http://pim.guide/essential/principles-matrix-process-quick-reference-flyer/.

Protection Information Management (PIM) Initiative, 2017. PIM Principles in Action: http://pim.guide/guidance-and-products/product/pim-principles-action/.

Protection Information Management (PIM) Initiative, 2018. PIM Framework for Data Sharing in Practice: http://pim.guide/essential/a-framework-for-data-sharing-in-practice/.

Terre des Hommes and CartONG, 2017. Data Protection Starter Kit: https://www.mdc-toolkit.org/data-protection-starter-kit/.

The Engine Room: Responsible Data Program, 2016. Responsible Data in Development Toolkit: https://responsibledata.io/resources/handbook/.

The Sphere Project, 2018. The Humanitarian Charter and Minimum Standards in Humanitarian Response (Sphere): https://handbook.spherestandards.org/en/sphere/#ch001.

UN, 2020. Data Strategy of the Secretary-General for Action by Everyone, Everywhere with Insight, Impact and Integrity, 2020-22: https://www.un.org/en/content/datastrategy/images/pdf/UN_SG_Data-Strategy.pdf.

UN Global Pulse, 2020. Risks, Harms and Benefits Assessment: https://www.unglobalpulse.org/policy/risk-assessment/.

UN Office for the Coordination of Humanitarian Affairs (UN OCHA), 2021. Data Responsibility Guidelines: https://data.humdata.org/dataset/2048a947-5714-4220-905b-e662cbcd14c8/resource/60050608-0095-4c11-86cd-0a1fc5c29fd9/download/ocha-data-responsibility-guidelines_2021.pdf.

UN Office of Human Rights (OHCHR), 2010. Manual on Human Rights Monitoring (with updated chapters): http://www.ohchr.org/EN/PublicationsResources/Pages/MethodologicalMaterials.aspx.

UN Office of Human Rights (OHCHR), 2018. A Human-Rights Based Approach to Data: Leaving No One Behind in the 2030 Agenda for Sustainable Development: https://www.ohchr.org/Documents/Issues/HRIndicators/GuidanceNoteonApproachtoData.pdf.

UNICEF, 2015. Procedures for Ethical Standards in Research, Evaluation, Data Collection and Analysis: https://www.unicef.org/media/54796/file.

UNICEF, 2018. Industry Toolkit: Children's Online Privacy and Freedom of Expression: https://www.unicef.org/csr/files/UNICEF_Childrens_Online_Privacy_and_Freedom_of_Expression(1).pdf.

UNICEF/GovLab, 2019. Responsible Data for Children Synthesis report: https://rd4c.org/files/rd4c-report-final.pdf.

UNHCR, 2015. Policy on the Protection of Personal Data of Persons of Concern to UNHCR: https://www.refworld.org/pdfid/55643c1d4.pdf.

UNHCR, 2018. Guidance on the Protection of Personal Data of Persons of Concern to UNHCR: https://www.refworld.org/docid/5b360f4d4.html.

UN Conference on Trade and Development (UNCTAD), 2020. Data Protection and Privacy Legislation Worldwide: https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx.

UN Development Group (UNDG). Data Privacy, Ethics and Protection: Guidance Note on Big Data for Achievement of the 2030 Agenda: https://unsdg.un.org/resources/data-privacy-ethics-and-protection-guidance-note-big-data-achievement-2030-agenda.

UN General Assembly, 1945. Charter of the United Nations: https://www.un.org/en/charter-united-nations/.

UN General Assembly, 1948. Universal Declaration of Human Rights: https://www.un.org/en/universal-declaration-human-rights/.

UN General Assembly, 1990. General Assembly Resolution on Guidelines for the Regulation of Personalized Data Files, A/RES/45/95: http://www.refworld.org/pdfid/3ddcafaac.pdf.

UN General Assembly, 1991. General Assembly Resolution 46/182 December 19, 1991: https://www.humanitarianresponse.info/sites/www.humanitarianresponse.info/files/documents/files/GA%20Resolution%2046-182.pdf.

UN High-Level Committee on Management (HLCM), 2018. Privacy and Data Protection Principles: https://www.unsystem.org/personal-data-protection-and-privacy-principles.

UN International Civil Service Commission, 2013. Standards of Conduct for the International Civil Service: https://icsc.un.org/Resources/General/Publications/standardsE.pdf.

UN Secretariat, 2004. Secretary-General's Bulletin on the Use of Information and Communications Technology Resources and Data, ST/SGB/2004/15: https://popp.undp.org/UNDP_POPP_DOCUMENT_LIBRARY/Public/United%20Nations%20Secretary-Generals%20Bulletin%20on%20Use%20of%20ICT%20Resources%20and%20Data%20ST_SGB_2004_15%20%E2%80%93%20Amended.docx.

UN Secretariat, 2010. UN Information Sensitivity Toolkit: https://archives.un.org/sites/archives.un.org/files/RM-Guidelines/information_sensitivity_toolkit_2010.pdf.

UN Secretariat, 2017. Secretary-General's Bulletin on Information Sensitivity, Classification and Handling, ST/SGB/2007/6: http://undocs.org/ST/SGB/2007/6.

UN Secretariat, 2007. Secretary-General's Bulletin on Record-Keeping and the Management of United Nations Archives, ST/SGB/2007/5: http://www.wgarm.net/ccarm/docs-repository/doc/doc462548.PDF.

USAID, 2019. Considerations for Using Data Responsibly at USAID: https://www.usaid.gov/responsibledata.

World Health Organization (WHO), 2007. WHO Ethical and safety recommendations for researching, documenting and monitoring sexual violence in emergencies: https://www.who.int/gender/documents/OMS_Ethics&Safety10Aug07.pdf.

Annexe D : Contexte du développement des Directives Opérationnelles

En janvier 2020, le Results Group 1 du IASC a établi le Sous-groupe sur la Responsabilité des données pour mener le développement de directives opérationnelles communes et à l'échelle du système sur la Responsabilité des données dans l'action humanitaire. Le Sous-groupe a été co-dirigé par l'Organisation Internationale pour les migrations, le Centre for Humanitarian Data de OCHA et le Haut Commissariat des Nations unies pour les réfugiés. Il regroupe également vingt organisations membres[47] qui représentent les différentes parties prenantes du système humanitaire.

Le Sous-groupe a élaboré ces Directives opérationnelles dans le cadre d'un processus de collaboration et de consultation avec les membres de l'IASC et la communauté humanitaire au sens large, les ONG, les agences des Nations Unies, les autres organisations internationales et les donateurs aux niveaux mondial, régional et national. Un certain nombre d'activités ont contribué à l'élaboration de ces directives opérationnelles, notamment :

- Une analyse documentaire[48]
- Une consultation publique[49]
- Une série de consultations ciblées avec différentes parties prenantes de l'ensemble du système humanitaire, y compris les organisations, les clusters/secteurs et les structures à l'échelle du système.
- Une période de retours (feedback loop) au cours de laquelle 150 collègues de 30 organisations différentes ont partagé des contributions et des commentaires sur le projet de directives opérationnelles, et
- Trois phases d'examen structuré et organisationnel du projet de directives opérationnelles à différents stades de développement.

Ces directives opérationnelles complètent et s'inspirent des directives existantes sur la Responsabilité des données, émanant à la fois des acteurs du développement et de la communauté humanitaire au sens large. Elles sont conçues pour tirer parti de l'expertise existante sur la Responsabilité des données, renforcer les efforts et les initiatives, et contribuer à la généralisation des meilleures pratiques. Elles sont alignées sur d'autres orientations et initiatives sectorielles clés sur différents sujets liés à la gestion responsable des données. Une liste complète des ressources examinées dans le cadre du processus de rédaction du guide opérationnel figure à l'annexe C.

[47] Le Sous-groupe inclut des représentants de : CARE, CRS, DRC, CICR, FICR, IRC, OIM, JIPS, Mercy Corps, MSF, NRC, OCHA, OHCHR, Oxfam, Save the Children, UNFPA, HCR, UNICEF, PAM et OMS.

[48] Le Sous-groupe a conduit l'analyse documentaire des orientations existantes en matière de responsabilité des données avec le soutien de Technical University of Delft. Veuillez trouver la liste des documents analysés dans l'annexe C.

[49] La consultation publique a été menée en ligne du 27 février au 18 mars 2020. Les résultats de l'enquête sont disponibles ici : https://centre.humdata.org/survey-results-on-priorities-for-data-responsibility-in-humanitarian-action/.

Compte tenu de la nature dynamique et évolutive des défis et des opportunités en matière de Responsabilité des données dans l'action humanitaire, ces directives opérationnelles seront révisées et mises à jour[50] de manière collaborative et consultative tous les deux ans.

[50] OCHA sera chargé d'initier le processus de révision et de mise à jour de ces directives opérationnelles.