IASC Inter-Agency Standing Committee

Directives Opérationnelles

LA RESPONSABILITÉ DES DONNÉES DANS L'ACTION HUMANITAIRE

Comité Permanent Interorganisations (IASC)

Avril 2023

IASC Inter-Agency Standing Committee

Directives Opérationnelles

LA RESPONSABILITÉ DES DONNÉES DANS L'ACTION HUMANITAIRE

TABLE DES MATIÈRES

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 (2023)'' fait foi.

ACRONYMES

3W	QUI FAIT QUOI OÙ ?
AAP	Redevabilité envers les populations affectées
AoR	Domaine de responsabilité
AGI	Agent de gestion de l'information
AIPD	Analyse d'impact sur la protection des données
APD	Accord de partage des données
CHG	Comité de haute gestion
DII	Renseignements identifiables sur le plan démographique
DRWG	Groupe de travail sur la Responsabilité des données
EHP	Équipe Humanitaire Pays
GTGI	Groupe de travail Gestion de l'Information
IASC	Comité permanent interorganisations
ICCG	Groupe de coordination inter-clusters
ICCM	Mécanisme de coordination inter-clusters
IM	Gestion de l'information (Information Management)
ISCG	Groupe de coordination intersectorielle
OCHA	Bureau des Nations Unies pour la coordination des affaires humanitaires
OI	Organisation internationale
PPI	Protocole de partage de l'information

AVANT-PROPOS

Le Comité permanent interorganisations (IASC) a approuvé la première version de ces Directives opérationnelles sur la Responsabilité des données dans l'action humanitaire en février 2021. Au cours des deux dernières années, les Directives opérationnelles ont été utilisées par les praticiens humanitaires pour orienter les mesures de la Responsabilité des données et renforcer leur application dans au moins vingt contextes d'intervention.

Compte tenu de la nature dynamique et évolutive des difficultés et des opportunités en matière de Responsabilité des données dans l'action humanitaire, l'IASC s'est engagé à réviser et à actualiser les Directives opérationnelles tous les deux ans. En juin 2022, l'IASC a officiellement demandé au Groupe de travail sur la Responsabilité des données (DRWG) de diriger ce processus.

Le DRWG est un organisme de coordination mondial qui s'emploie à promouvoir la Responsabilité des données dans l'ensemble du système humanitaire. Il rassemble un groupe diversifié d'intervenants, y compris des entités des Nations Unies, d'autres organisations internationales, des organisations non gouvernementales et d'autres acteurs engagés dans la mise en œuvre et la coordination de l'action humanitaire. Le DRWG est coprésidé par le Conseil danois pour les réfugiés (DRC), l'OIM, l'OCHA et le HCR.

Entre juin 2022 et avril 2023, le DRWG a mené un processus de collaboration et de consultation qui servit à l'élaboration de cette deuxième édition de Directives opérationnelles. Cela comprend :

- Une analyse documentaire des politiques, des orientations et des cadres pertinents;
- Une étude mondiale qui a obtenu des réponses de 125 acteurs humanitaires de plus de 50 pays;
- Une série de consultations avec des intervenants de l'ensemble du système humanitaire, y compris des organisations, des clusters et des structures à l'échelle du système;
- Une période de rétroaction ouverte au cours de laquelle 100 collègues de 25 organisations différentes ont formulé des observations sur la version révisée;
- Trois séries d'examen formels et structurés du projet de Directives opérationnelles par les organisations membres du DRWG, et ce à différentes étapes de sa révision.

Les révisions majeures présentées dans cette édition de Directives opérationnelles comprennent :

- L'ajout des leçons tirées des deux premières années de mise en œuvre des Directives;
- Une évaluation et un aperçu actualisés des défis et des opportunités liés à la Responsabilité des données dans l'action humanitaire;
- Mise à jour du contenu pour encadrer les Principes relatifs à la Responsabilité des données et les modifications mineures afin de préciser le libellé de chaque Principe et de citer ou de refléter autrement de nouveaux cadres pertinents.
- Mise à jour du cadre et du texte descriptif sur les mesures pour la Responsabilité des données, y compris les modifications apportées aux mesures spécifiques pour les rendre plus faciles à gérer et plus pertinentes sur le plan opérationnel.

- L'ajout d'exemples de la Responsabilité des données dans la pratique en annexe aux Directives.
- Des mises à jour importantes des modèles pour appuyer la mise en œuvre efficace des mesures.

Les progrès en matière de la Responsabilité des données dépendent de notre aptitude à travailler ensemble, anticiper, évaluer et atténuer les risques liés aux données, ainsi qu'à concevoir et à mettre en œuvre des activités qui maximisent les avantages et l'utilisation des données, et qui permettent la protection et les droits des populations affectées. Nous espérons que cette deuxième édition des Directives opérationnelles de l'IASC sur la Responsabilité des données dans l'action humanitaire sevira de cadre commun aux efforts conjoints visant à faire progresser ce travail, qui est de plus en plus essentiel dans la manière dont nous protégeons et servons les populations affectées par les crises.

Coprésidents du Groupe de travail sur la Responsabilité des données :

Kathrine Starup
Responsable de l'Unité de Protection Globale
Conseil danois pour les réfugiés (DRC)

Rachelle Cloutier
Responsable de la politique des données, Service de données global
HCR

Robert Trigwell
Responsable des données et de l'éthique
IOM

Stuart Campo
Chef d'équipe, Responsabilité des données
Centre for Humanitarian Data de OCHA

RÉSUMÉ

La Responsabilité des données dans l'action humanitaire est la gestion sécurisée, éthique et efficace des données à caractère personnel et non personnel pour la réponse opérationnelle, conformément aux cadres établis pour la protection des données personnelles. Il s'agit d'une question cruciale pour le secteur humanitaire, et les enjeux sont de taille.

En pratique, la mise en œuvre de la Responsabilité des données manque souvent de cohérence au sein et au travers les contextes de réponse humanitaire. Cette incohérence persiste, et ce en dépit des principes, des normes et des standards professionnels relatifs aux droits des populations affectées, de l'éventail de ressources sur la Responsabilité des données disponibles dans la communauté internationale des données, ainsi que des efforts significatifs déployés par de nombreuses organisations humanitaires pour élaborer et mettre à jour leurs politiques et directives dans ce domaine. Bien que chaque organisation soit responsable de sa propre gestion des données, les humanitaires ont besoin d'un cadre de travail commun pour guider leurs actions, tant individuelles que collectives, et maintenir un standard élevé en matière de Responsabilité des données dans divers environnements opérationnels.

Les présentes Directives opérationnelles sur la Responsabilité des données dans l'action humanitaire répondent à ce besoin. Les Directives sont le résultat d'un processus inclusif et consultatif mené sous les auspices du Comité permanent interorganisations (IASC) et sont conçues pour garantir des mesures concrètes pour la Responsabilité des données dans toutes les phases de l'action humanitaire. Les Directives ont été approuvées pour la première fois en février 2021. La présente version des Directives a été élaborée dans le cadre d'un processus de révision mené par le Groupe de travail sur la Responsabilité des données (DRWG) et approuvée par le IASC en mars 2023 (voir **l'annexe E** pour plus de détails sur le processus d'élaboration et de révision).

Enseignements tirés de la mise en pratique de la Responsabilité des données

Au cours des deux années qui ont suivi la première approbation de ces Directives opérationnelles en février 2021, des entités, des clusters/secteurs et des organisations à l'échelle du système ont mis en œuvre des mesures pour la Responsabilité des données à l'aide de ces directives.[1] Les enseignements tirés de cette expérience (résumés ci-dessous) ont servi de base à la révision de ces directives et contribueront à promouvoir leur adoption ultérieure.

Au niveau de l'ensemble du système :

- Prioriser l'élaboration d'un protocole de partage d'informations (ISP)[2] en début d'une situation d'urgence contribue à sensibiliser à la Responsabilité des données et à établir des bases d'actions supplémentaires à tous les niveaux d'intervention.
- Assurer la sensibilisation et l'adhésion de l'Équipe humanitaire pays (HCT) aux questions liées à la Responsabilité des données permet de dégager un espace pour des investissements supplémentaires dans ce domaine.
- Intégrer les actions relatives à la Responsabilité des données dans les termes de référence et les plans de travail des structures à l'échelle du système telles que l'IMWG, l'ICCG/ISCG et le CWG favorise une action plus collective dans les domaines d'intérêt commun.

1. Les 15 exemples sont disponibles **ici**, ainsi qu'une liste d'exemples supplémentaires mise à jour par le DRWG.
2. Le modèle ISP est disponible **ici**, et est inclus dans **l'annexe B**.

- Fournir un soutien consultatif aux clusters/secteurs sur la mise en œuvre d'actions pour la Responsabilité des données favorise une approche plus cohérente et permet une coordination plus efficace des actions à travers l'intervention de l'ICCG/ISCG et l'IMWG.

Au niveau du cluster/secteur :

- Dans les cas où les ressources à l'échelle du système (c'est-à-dire un PPI et/ou une classification de la sensibilité des données et des informations) ne fournissent pas suffisamment de détails ou de nuances pour explorer les questions spécifiques au cluster/secteur, l'élaboration d'orientations supplémentaires sur la sensibilité des données et les techniques connexes de traitement des données sensibles pour les membres du cluster/secteur soutient une approche plus cohérente de la gestion responsable des données.

- L'élaboration d'outils et d'approches communs pour la gestion responsable des données améliore le partage et l'utilisation des données au sein du cluster/secteur.

Au niveau des organisations :

- Une organisation qui met en œuvre des actions pour la Responsabilité des données est en mesure d'utiliser les modèles de **l'annexe B** ou adapter ses processus, modèles et outils organisationnels existants pour les rendre plus conformes à ces Directives opérationnelles.

- La Responsabilité des données nécessite une collaboration interfonctionnelle. Définir clairement les rôles et les responsabilités pour la mise en œuvre des différentes actions de ces Directives opérationnelles permet au personnel de comprendre comment l'appliquer à ses activités respectives.

- L'identification d'une activité de gestion des données au sein de laquelle différentes actions peuvent être mises à l'essai permet de démontrer la valeur de ce travail, de favoriser une compréhension commune des concepts et de susciter l'adhésion et l'appropriation avec le personnel et les partenaires.

Structure des Directives opérationnelles

Les Directives opérationnelles sont divisées en quatre sections :

1. La première section présente le contexte de la Responsabilité des données dans l'action humanitaire, précise le public cible ainsi que le champ d'application du document, et donne des instructions sur la manière d'utiliser les Directives opérationnelles dans différentes situations.

2. La deuxième section présente les principes pour la Responsabilité des données dans l'action humanitaire.

3. La troisième section décrit les actions clés à mettre en œuvre aux différents niveaux de la réponse humanitaire, et ce afin de garantir la Responsabilité des données, y compris les rôles et les responsabilités spécifiques pour la réalisation de ces actions.

4. La quatrième section décrit une approche de suivi, d'évaluation et d'apprentissage de la Responsabilité des données et la mise en œuvre de ces directives dans la pratique.

Les annexes proposent des termes clés et des définitions (**Annexe A**), des modèles suggérés pour la Responsabilité des données (**Annexe B**), des exemples de Responsabilité des données dans la pratique (**Annexe C**), des ressources et des références (**Annexe D**), ainsi que des informations générales sur l'élaboration des Directives opérationnelles (**Annexe E**).

Compte tenu de la nature dynamique et évolutive des défis et des opportunités liés de la Responsabilité des données dans l'action humanitaire, ces Directives opérationnelles seront révisées et mises à jour dans le cadre d'un processus collaboratif et consultatif tous les deux ans, ou plus si l'IASC le juge nécessaire.

DÉFINIR LA RESPONSABILITÉ DES DONNÉES

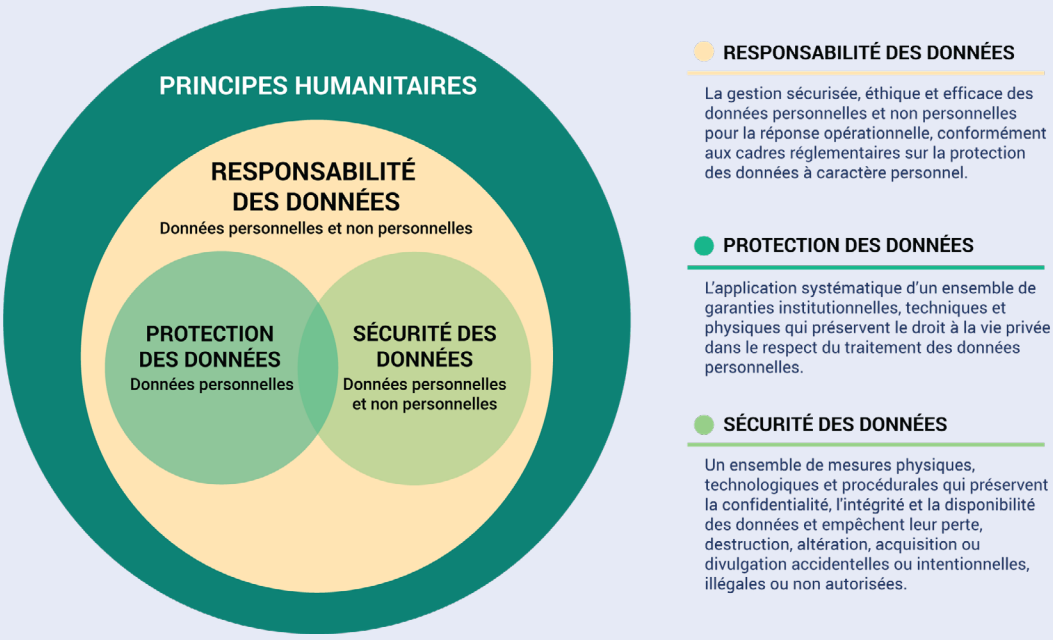
Une liste complète de définitions est incluse dans l'annexe A.

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 règlementaires sur la protection des données à caractère personnel.[3]

- **Sécurisée** | Les activités de gestion des données garantissent la sécurité des données à tout moment, respectent les droits humains et d'autres obligations légales, et ne causent pas de préjudice.
- **Éthique** | Les activités de gestion des données sont conformes aux cadres et aux standards établis en matière d'éthique humanitaire[4] et d'éthique des données[5].
- **Efficace** | Les activités de gestion des données sont bien coordonnées et permettent d'atteindre les objectifs qui ont motivé leur mise en place.

La Responsabilité des données exige une mise en œuvre d'actions fondées sur des principes à tous les niveaux de la réponse humanitaire. Cela inclut par exemple des actions pour garantir la protection des données et la sécurité des données, ainsi que des stratégies pour minimiser les risques tout en maximisant les bénéfices de la gestion des données opérationnelles.

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 » désigne 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 et garantissent les droits des personnes concernées. La « sécurité des données », applicable à la fois aux données à caractère personnel et non personnel, désigne les mesures physiques, techniques et procédurales qui visent à protéger la confidentialité, la disponibilité et l'intégrité des données. Le graphique ci-dessous illustre la relation entre ces concepts clés et les principes humanitaires.



Description : Relation entre les principes humanitaires, la sécurité des données, la protection des données et la Responsabilité des données.

3. Aux fins des présentes Directives opérationnelles, « conformément aux cadres établis pour la protection des données personnelles » signifie que les activités de gestion des données sont guidées par les lois nationales et régionales sur la protection des données ou les politiques organisationnelles de protection des données.

4. L'éthique humanitaire s'est développée comme une éthique fondée sur des principes d'humanité, d'impartialité, de neutralité et d'indépendance qui guident la fourniture de l'assistance et de 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 : La Charte humanitaire et les normes minimales relatives aux interventions humanitaires, notamment les normes fondamentales et les principes de protection, la norme humanitaire fondamentale relative à la qualité et à la redevabilité, et le Code de conduite pour le Mouvement international de la Croix-Rouge et du Croissant-Rouge et pour les organisations non gouvernementales (ONG) lors des opérations de secours en cas de catastrophe.

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

La gestion opérationnelle des données : L'ensemble des activités de gestion des données pour la réponse opérationnelle, incluant la conception des activités et leur exécution ultérieure, notamment la collecte ou la réception, le stockage, l'assurance qualité, l'analyse, le partage, l'utilisation, la conservation et la destruction des données et des informations par les acteurs humanitaires. La gestion des données s'inscrit dans le cadre de l'action humanitaire tout au long du cycle de planification et de réponse dans les différents clusters/secteurs et incluant de manière non exhaustive les analyses de la situation, les évaluations des besoins, la gestion des données démographiques, l'enregistrement et l'inscription, la gestion des cas, la communication avec les populations affectées, le suivi des activités de protection, ainsi que le suivi et l'évaluation de la réponse.

Les données personnelles : Toute information se rapportant à une personne physique identifiée ou identifiable ("la personne concernée.[6] "). Une personne physique identifiable est une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant tel qu'un nom, un numéro d'identification, des données de localisation, une image, 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 qui ne se rapporte pas à une personne concernée.[7] 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 (c'est-à-dire qui ont toujours été des données non personnelles), 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 initialement des données personnelles, mais qui ont été rendues anonymes ultérieurement, telles que les données sur les personnes affectées par la situation humanitaire et leurs besoins, les risques et les vulnérabilités auxquels elles sont exposées, ainsi que leurs capacités. Les données non personnelles incluent les informations démographiquement identifiables (Demographically Identifiable Information, ou DII en anglais), c'est-à-dire les données qui permettent d'identifier des groupes d'individus en fonction de facteurs démographiques tels que l'ethnicité, le sexe, l'âge, la profession, la religion ou la localisation.

Les données sensibles : Données qui, si elles sont divulguées ou consultées sans autorisation préalable, sont susceptibles de causer ce qui suit :

- Un préjudice (tels que des sanctions, la discrimination) à toute personne, y compris la source d'information ou d'autres personnes ou groupes identifiables.
- Un impact négatif sur la capacité d'une organisation à mener à bien ses activités ou sur la perception de cette organisation par le public.[8]

Les données, qu'elles soient personnelles ou non personnelles, peuvent, toutes deux, être sensibles. La sensibilité des données est définie en fonction du contexte de la réponse. Les mêmes types de données peuvent avoir différents niveaux de sensibilité dans différents contextes et la sensibilité peut changer avec le temps. De nombreuses organisations disposent de systèmes de classification et d'outils spécifiques pour évaluer la sensibilité des données afin de faciliter les pratiques de gestion responsable des données.

5. Le Centre de données humanitaires d'OCHA, Guidance Note : Humanitarian Data Ethics (2019) fournit de plus amples informations sur la relation entre l'éthique humanitaire et l'éthique des données, disponible à l'adresse suivante :: https://centre.humdata.org/guidance-note-humanitarian-data-ethics/.

6. ICRC, Manuel sur la protection des données dans l'action humanitaire (2020), https://www.icrc.org/en/data-protection-humanitarian-action-handbook.

7. D'après la définition de « données personnelles » dans le Manuel sur la protection des données dans l'action humanitaire (2020) du ICRC, https://www.icrc.org/en/data-protection-humanitarian-action-handbook.

8. D'après la définition du Groupe consultatif sur les "normes professionnelles" dirigé par le CICR, 2018, 3e édition. Normes professionnelles pour le travail de protection; Chapitre 6 : Gestion des données et de l'information pour les résultats en matière de protection, https://www.icrc.org/en/publication/0999-professional-standards-protection-work-carried-out-humanitarian-and-human-rights.

DÉFIS ET OPPORTUNITÉS POUR LA RESPONSABILITÉ DES DONNÉES DANS L'ACTION HUMANITAIRE

Les organisations humanitaires sont confrontées à un certain nombre de défis et d'opportunités qui constituent la base de l'action collective et de l'action des organisations individuelles dans le domaine de la Responsabilité des données.

Ces défis incluent :

- **L'augmentation de l'ampleur et du nombre d'activités de gestion des données dans le secteur**, souvent mises en œuvre sans égard à la Responsabilité des données.
- **Une prise de conscience limitée des risques, des préjudices et des autres impacts négatifs potentiels** d'une mauvaise gestion des données pour les populations affectées, les organisations humanitaires et leur personnel.
- Une **sous-représentation** des organisations locales, des organisations de la société civile, des structures communautaires et des personnes concernées dans la prise de décision concernant les activités de gestion des données.
- **L'absence de mesures d'atténuation des risques et de mécanismes de responsabilisation** pour la gestion des données dans l'action humanitaire.
- L'absence de **définitions communes** des concepts clés de la Responsabilité des données et les **incohérences qui en découlent dans la compréhension et l'utilisation de la terminologie** au sein des organisations humanitaires.
- Les **lacunes en matière de lignes directrices et normes existantes**, notamment sur la gestion des données sensibles, l'évaluation des risques liés 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.
- Les **écarts entre les directives existantes et leur mise en œuvre** à la fois en termes de différences majeures entre les capacités des organisations à mettre en œuvre les directives et de différences internes entre les sièges et les bureaux locaux.
- L'application variable de **différents cadres juridiques et réglementaires**, en particulier pour la gestion des données personnelles, au sein des organisations internationales (OI), y compris les entités de l'ONU, les ONG internationales, les ONG locales et d'autres acteurs.
- **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 qui réglementent leur emploi.
- La **priorisation des pratiques et des 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 dans la pratique.
- Le **manque de capacité** en matière de Responsabilité des données au sein de nombreuses organisations humanitaires et de leur personnel, notamment en termes de compétences techniques, de contraintes temporelles et d'infrastructure technique.

Opportunités :

- **L'investissement accru par les organisations humanitaires et de développement, les bailleurs et les gouvernements** dans la Responsabilité des données en tant que stratégie visant à faire progresser les droits des populations affectées et à contribuer à la réalisation d'objectifs humanitaires et de développement plus globaux.
- Un **intérêt et une demande accrus de la part des bailleurs et des gouvernements** pour les données et les approches fondées sur des données probantes en matière de planification et d'établissement de rapports humanitaires.
- Le **renforcement de la collaboration** sur la Responsabilité des données entre les organisations, y compris le partage des ressources et des apprentissages.
- Une **amélioration des capacités institutionnelles et collectives** concernant les questions liées à la gestion responsable des données et à la mise en œuvre des normes et recommandations internationales, notamment en matière de protection des données à caractère personnel.
- Des **possibilités accrues de collaboration en matière de gestion des données, avec les gains d'efficacité qui en résultent**, notamment par le biais d'évaluations coordonnées, de déploiement conjoint d'assistance, d'analyses conjointes (y compris avec les populations affectées) et d'autres activités similaires.
- Un **intérêt et un soutien plus important pour l'élaboration d'une base de données concrète** sur "ce qui fonctionne" et "ce qui ne fonctionne pas" en matière de Responsabilité des données dans les contextes humanitaires, notamment par une plus grande prise en compte des connaissances locales.
- **Davantage de transparence** dans la manière dont les organisations humanitaires gèrent les données en appui des différentes activités d'intervention, avec un renforcement associé de la **redevabilité envers les populations affectées**.
- 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.

APERÇU DES DIRECTIVES OPÉRATIONNELLES

Contexte

La Responsabilité des données est un enjeu crucial pour le secteur humanitaire. Veiller à ne pas nuire tout en tirant le meilleur parti des données exige une action collective à tous les niveaux du système humanitaire. Les acteurs humanitaires doivent faire preuve de vigilance dans la gestion des données afin d'éviter de faire courir des risques accrus aux individus ainsi qu'aux communautés déjà vulnérables et de préserver la confiance qui règne entre les populations affectées et les organisations humanitaires.

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, et ce en dépit des principes, des normes et des standards professionnels relatifs aux droits des populations affectées, de l'éventail de ressources sur la Responsabilité des données disponibles dans la communauté internationale des données, ainsi que des efforts significatifs déployés par de nombreuses organisations humanitaires pour élaborer et mettre à jour leurs politiques et directives dans ce domaine. Étant donné que l'écosystème des données humanitaires est interconnecté par nature, aucune organisation individuelle ne peut s'attaquer seule à de tels défis.

Alors que chaque organisation demeure responsable de ses propres données, les acteurs humanitaires 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. Ces directives opérationnelles complètent et s'inspirent des directives existantes[9] sur la Responsabilité des données, émanant à la fois des acteurs du développement et de la communauté humanitaire. Il a été élaboré sous les auspices du Comité permanent interorganisations et approuvé pour la première fois en février 2021. La version actuelle a été préparée dans le cadre d'un processus de révision collaboratif dirigé par le Groupe de travail sur la Responsabilité des données (**DRWG**) et approuvée en mars 2023 (voir **l'annexe E** pour plus de détails sur le processus d'élaboration et de révision).

Champ d'application

Les directives opérationnelles s'appliquent aux données opérationnelles à caractère personnel et non personnel qui sont générées et/ou utilisées dans le cadre des réponses humanitaires, notamment :

- **Les données sur le contexte** dans lequel se déroule une réponse (p. ex., les conditions politiques, sociales et économiques, les données géospatiales, l'infrastructure, etc.) et la situation humanitaire en question (p. ex., les incidents de sécurité, risques en matière de protection, les tendances et prévisions en matière de déplacement, les facteurs et les causes/facteurs sous-jacents de la situation ou 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** (p. ex., telles qu'elles sont rapportées dans « Qui Fait Quoi Où » (3W), Présence opérationnelle et autres outils de suivi des réponses similaires).

9. Il s'agit, par exemple, des directives opérationnelles du IASC sur les responsabilités des chefs de file des clusters/secteurs, des normes professionnelles pour le travail de protection, du cadre de gestion de l'information sur la protection (PIM), de l'initiative "Des données responsables pour les enfants" et du code Signal : Une approche de l'information en temps de crise fondée sur les droits humains (voir **l'annexe D** pour des références et des ressources supplémentaires).

Compte tenu de l'accent mis sur les données opérationnelles, 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.

Ces directives opérationnelles s'appliquent à toutes les formes de gestion des données opérationnelles qui ont lieu dans tous les contextes de réponse humanitaire. Étant donné que les organisations humanitaires disposent d'une grande variété de processus pour la gestion des données et le cycle de vie des données,[10] ces directives opérationnelles ne présentent pas un ensemble standard ou harmonisé d'étapes pour la gestion des données. Au contraire, les principes et les actions de ces directives opérationnelles sont pertinents pour toutes les étapes de la gestion opérationnelle des données dans le cadre de l'action humanitaire, et ce quels que soient les modèles spécifiques élaborés ou utilisés par les organisations et les entités individuelles.

Audience cible

Ces directives opérationnelles doivent guider la gestion des données opérationnelles de tous les acteurs humanitaires, y compris les entités onusiennes, les autres organisations internationales (OI), les ONG internationales et nationales, les organisations de la société civile, les gouvernements et autres autorités étatiques, les prestataires de services du secteur privé et les autres parties prenantes engagées dans l'action humanitaire.

Les Directives opérationnelles ciblent spécifiquement les structures de coordination suivantes, qui servent de forums pour la promotion, le soutien et le suivi de la mise en œuvre de la Responsabilité des données aux différents niveaux d'une réponse : l'équipe humanitaire pays (EHP/HCT), le groupe de coordination inter-cluster/secteurs (ICCG ou ISCG), le groupe de travail sur l'évaluation (et l'analyse) (AAWG ou AWG), le groupe de travail de la gestion de l'information (IMWG), le groupe de travail sur les espèces (CWG), le groupe de travail sur l'accès (AWG) et/ou d'autres groupes de travail à l'échelle du système, et les groupes sectoriels (Clusters), les domaines de responsabilité (AoRs), les secteurs, les comités directeurs (CD), et/ou les groupes consultatifs stratégiques (GCS).

L'ensemble du personnel des organisations humanitaires et des acteurs humanitaires, ainsi que les individus (par exemple, les entrepreneurs, les employés des partenaires en stand-by et le personnel détaché) doivent consulter les Directives opérationnelles lors de la gestion des données. Les Directives opérationnelles ciblent différents rôles et fonctions au niveau de l'ensemble du système, du cluster/secteur et de l'organisation. Il s'agit notamment des coordinateurs résidents/coordonnateurs humanitaires (RC/HC), des chefs de bureau et des représentants nationaux, des gestionnaires de programme et des responsables (par exemple, les responsables de programme, les experts sectoriels/techniques, les responsables des affaires humanitaires et autres rôles similaires), des coordinateurs et coresponsables cluster/secteur, et du personnel technique (par exemple, les responsables de la gestion de l'information, analystes de données, spécialistes des données, statisticiens, responsables de la protection des données ou points focaux, personnel des technologies de l'information, responsables de l'enregistrement, opérateurs de mécanismes de retour d'information et de réponse communautaires, responsables du suivi et de l'évaluation, agents recenseurs et autres fonctions similaires).

10. Une analyse documentaire de 55 documents a permis d'identifier 18 processus et cycles de gestion des données différents, chacun variant en termes de complexité, de champ d'application et d'actions. La liste des documents examinés est disponible à l'annexe D.

Comment utiliser les présentes directives opérationnelles

Ces directives opérationnelles visent à soutenir le personnel humanitaire, les organisations et leurs partenaires à mettre en pratique la Responsabilité des données. Elles offrent un ensemble de principes pour guider la gestion des données dans les contextes humanitaires et un ensemble d'actions recommandées que les entités à l'échelle du système, les clusters et les secteurs, et les organisations peuvent mettre en œuvre pour faire progresser la Responsabilité des données dans leur travail. Elles ne visent en aucune façon à remplacer ou à porter atteinte aux politiques et les directives organisationnelles existantes,[11] et ne relèvent ni de mandats organisationnels, ni de lois nationales ou régionales spécifiques.

Étant donné que la Responsabilité des données varie selon les fonctions du personnel et les contextes d'intervention, l'utilisation des présentes directives opérationnelles prendra différentes formes. Le tableau ci-dessous présente également la manière dont les directives peuvent être utilisées dans différents cas de figure.

11. 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.

Cas de figure	Utilisation des directives opérationnelles
Nouvelle intervention	Dans un nouveau contexte d'intervention, le personnel doit se concentrer sur les actions à l'échelle du système décrites dans la **section 3** des Directives : • L'élaboration et la tenue d'un registre de gestion des données permettront de garder une trace des activités de gestion des données entreprises par les différents acteurs dans le contexte d'intervention, ce qui favorisera la transparence ainsi que la coordination et la collaboration. • L'approbation d'un protocole de partage d'informations au début de l'intervention aide les acteurs humanitaires à s'aligner sur la sensibilité des types de données, ainsi que sur les manières de partager les données avec les différents intervenants. Cela permet de promouvoir la responsabilité dans la gestion des données au fur et à mesure que l'intervention se développe. La mise en œuvre de ces actions au début d'une intervention permettra d'établir un niveau élevé de gestion des données et de favoriser l'harmonisation des processus avec les principes.
Intervention existante sans mesures établies pour la Responsabilité des données	Dans les contextes d'intervention où aucune mesure n'a encore été prise pour la Responsabilité des données, le personnel dispose de deux options pour commencer à utiliser les directives opérationnelles : • Commencer par les actions à l'échelle du système (niveau 1) comme un protocole de partage d'information, puis appuyer les mesures au niveau des clusters/secteurs (niveau 2) et des organisations (niveau 3) pour favoriser l'harmonisation et la cohérence entre les intervenants et les activités de gestion des données. • Concevoir la Responsabilité des données en introduisant des actions pour la Responsabilité des données dans le cadre d'une activité spécifique de gestion des données (telle qu'une évaluation des besoins) afin de démontrer la valeur de ce travail, puis lancer d'autres actions à l'échelle du système. Le personnel peut décider de commencer à mettre en œuvre des mesures à l'échelle du système ou du cluster/secteur et d'introduire simultanément des mesures pour une activité spécifique de gestion des données. Il est important d'harmoniser et de séquencer les actions afin d'éviter les mesures contradictoires, et ce à différents niveaux.
Intervention existante avec quelques mesures établies pour la Responsabilité des données	La plupart des interventions prolongées comporteront au moins quelques mesures relatives à la Responsabilité des données. Par exemple, les organisations humanitaires peuvent disposer d'un registre des activités de gestion des données en cours, ou d'une politique d'accès aux données stockées par l'organisation. Dans de tels contextes, le personnel doit effectuer un diagnostic de la Responsabilité des données à l'échelle du système afin de déterminer les mesures manquantes ou insuffisamment mises en œuvre, et qui pourraient être prioritaires.

LES PRINCIPES POUR LA RESPONSABILITÉ DES DONNÉES DANS L'ACTION HUMANITAIRE

Les Principes pour la Responsabilité des données reflètent l'engagement collectif des acteurs humanitaires en faveur de la Responsabilité des données à l'échelle du système, du cluster/secteur et de l'organisation. Ils se fondent sur un examen des principes existants en matière de gestion des données dans les secteurs de l'humanitaire et du développement.[12]

Les Principes guident les acteurs dans leurs activités de gestion des données et éclairent leur mise en œuvre des actions recommandées en matière de Responsabilité des données issues de ces directives opérationnelles. Ils renforcent l'engagement primordial des humanitaires de "Ne pas nuire" (Do No Harm) et réaffirment le rôle central des populations affectées, de leurs droits et de leur bien-être en vue de maximiser les avantages et de minimiser les risques de la gestion des données dans l'action humanitaire.[13] Les organisations doivent respecter les principes conformément à leur mandat, au contexte de la réponse, aux instruments directeurs, et aux normes et standards mondiaux, y compris les principes humanitaires.[14] Comme les autres directives de l'IASC, les principes établis dans ces directives opérationnelles ne constituent pas une norme de conformité.

Les Principes sont présentés par ordre alphabétique. Lorsqu'ils sont en conflit, que ce soit dans leur interprétation ou leur application, il convient de les interpréter, de les appliquer et de les mettre en balance de manière à obtenir l'impact le plus positif possible pour les populations affectées.[15] En cas de conflit entre les Principes et les politiques internes de l'organisation ou les obligations légales applicables, ces politiques ou obligations légales prévalent.

Bien que les Principes présentés ci-dessous s'appliquent à la fois aux données personnelles et non personnelles, les organisations humanitaires doivent toujours adhérer aux exigences et obligations spécifiques liées au traitement des données personnelles telles que décrites dans le Principe de protection des données personnelles. Bien que certains des Principes utilisent un langage identique ou similaire à celui des principes établis pour la protection des données personnelles (par exemple, la sécurité des données, la proportionnalité, l'équité, la légitimité), ils ne sont pas identiques. La similitude des termes utilisés dans la Responsabilité et la protection des données montre que la gestion responsable des données reflète un ensemble de normes fondamentales communes à toutes les données, indépendamment de leur type et de la mesure dans laquelle ces normes sont codifiées dans la législation.

12. Une liste complète des documents compilés et analysés par le sous-groupe de l'IASC sur la responsabilité des données en 2020 pour éclairer la rédaction des principes est disponible à **l'Annexe D**. Bien qu'aucun principe n'ait été ajouté ou supprimé dans la révision de 2023 de ces Directives, les principes ont été édités dans un souci de clarté et de cohérence.

13. Aux fins du présent document, l'expression "ne pas nuire" est utilisée comme suit : 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 d'autres parties prenantes, que ce soit par des actions ou des omissions. Maximiser les avantages de la gestion des données humanitaires signifie que les données sont partagées lorsqu'un objectif l'exige, de manière appropriée et sûre, en respectant les exigences nécessaires en matière de protection et de sécurité des données. Cela signifie également que les données sont gérées de manière à permettre et à augmenter la probabilité d'un impact positif pour les populations affectées.

14. Pour plus d'informations sur les principes humanitaires, voir OCHA on Message : Principes humanitaires, disponible à l'adresse suivante : **https://www.unocha.org/sites/unocha/files/OOM_Humanitarian%20Principles_Eng.pdf**.

15. Consulter **l'annexe C** pour des exemples des Principes en pratique.

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

Redevabilité
Conformément aux règles pertinentes applicables, les organisations humanitaires ont l'obligation de justifier et d'assumer la pleine responsabilité de leurs activités de gestion des données. Les organisations humanitaires sont redevables vis-à-vis des populations affectées par les crises, des structures de gouvernance internes et aux partenaires humanitaires nationaux, régionaux et internationaux. Les organisations humanitaires doivent mettre en place toutes les mesures nécessaires pour respecter leurs engagements en matière de responsabilité, conformément aux présents Principes. Ceci inclut la mise en place de politiques, de directives et de processus adéquats, et la garantie de la disponibilité de compétences et de capacités suffisantes et appropriées, y compris, et sans s'y limiter, de ressources financières, humaines et technologiques.[16] La mise en place de compétences et de capacités devrait inclure l'offre de formations et d'opportunités d'apprentissage afin de s'assurer que le personnel possède l'expertise, les aptitudes, les connaissances ainsi que les attitudes nécessaires pour gérer les données de manière responsable.

Confidentialité
Les organisations humanitaires doivent mettre en œuvre des garanties et des procédures organisationnelles appropriées afin de préserver la confidentialité des données sensibles à tout moment, notamment en imposant des restrictions d'accès claires et cohérentes. Les mesures doivent être conformes aux politiques organisationnelles et aux exigences légales applicables, tout en tenant compte du ou des systèmes de classification de la sensibilité des données dans le contexte de l'intervention.

Coordination et Collaboration
La gestion coordonnée et collaborative des données implique l'inclusion significative des partenaires humanitaires, des autorités nationales et locales, des populations affectées par les crises et d'autres parties prenantes dans les activités de gestion des données, le cas échéant et sans compromettre les principes humanitaires[17] ou les présentes Directives opérationnelles. Les organisations humanitaires doivent se coordonner et collaborer afin de 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 à plus long terme. La capacité locale et nationale doit être renforcée dans la mesure du possible, et ne doit, en aucun cas, être affaiblie.

Sécurité des données
Les organisations humanitaires doivent mettre en place des mesures de protection, des procédures et des systèmes appropriés, tant au niveau organisationnel que technique, et ce afin de prévenir, d'atténuer et de signaler les atteintes à la sécurité des données numériques et non numériques, et d'y réagir.[18] Ces mesures doivent être conçues pour protéger les données contre les attaques externes, et se prémunir, en interne, contre l'accès ou la manipulation non autorisée ou inappropriée; et la divulgation accidentelle, les dommages, l'altération, les pertes et autres risques de sécurité liés à la gestion des données. Ces mesures doivent être basées sur la sensibilité des données et mises à jour en fonction de l'évolution des normes et des meilleures pratiques en matière de sécurité des données.

16. 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 suivante : https://interagencystandingcommittee.org/accountability-affected-populations-including-protection-sexual-exploitation-and-abuse/doc uments-56.

17. Pour obtenir plus d'informations sur les principes humanitaires, voir OCHA on Message : Principes humanitaires (2022) disponible à l'adresse suivante : https://www.unocha.org/sites/unocha/files/OOM_Humanitarian%20Principles_Eng.pdf.

18. Les organisations humanitaires ont développé des approches distinctes pour les incidents liés à la gestion des données, qu'il convient de suivre en conséquence. Voir la Note d'orientation sur la gestion des incidents liés aux données (2019) du Centre des données humanitaires d'OCHA pour plus d'informations sur la gestion des incidents liés aux données, disponible à l'adresse suivante: https://centre.humdata.org/guidance-note-data-incident-management/.

Finalité, nécessité et proportionnalité
La gestion des données humanitaires et les activités associées doivent se définir sur la base d'une finalité bien 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, respecter et promouvoir les droits et libertés pertinents et, le cas échéant, les équilibrer avec soin. Conformément au concept de minimisation des données, la gestion des données dans le cadre de l'action humanitaire doit être pertinente, limitée et proportionnée aux finalités déterminées.

Équité et légitimité
Les organisations humanitaires doivent gérer les données de manière équitable et légitime. La gestion équitable des données permet de mener l'action humanitaire dans une totale neutralité et impartialité. Les motifs légitimes de gestion des données incluent : l'intérêt supérieur et/ou vitaux des communautés et des populations affectées par les crises, conformément au mandat de l'organisation; l'intérêt public dans le cadre du mandat de l'organisation; et tout autre motif légitime spécifiquement identifié par le cadre réglementaire de l'organisation et/ou les lois applicables.

Approche basée sur les droits humains
La gestion des données doit être conçue et mise en œuvre de manière à respecter, protéger et promouvoir les droits humains. Cela comprend les libertés fondamentales et les principes d'égalité et de non-discrimination tels qu'ils sont définis dans les cadres des droits humains, ainsi que les droits spécifiques aux données promulgués dans la législation applicable.

Approche inclusive et axée sur la personne
Les populations affectées doivent avoir la possibilité de participer, d'être incluses, représentées et habilitées à exercer leur pouvoir tout au long de la gestion des données, et ce à chaque fois que le contexte opérationnel le permet. L'autonomie humaine des populations affectées par les crises doit guider la gestion des données humanitaires. Des efforts particuliers doivent être déployés pour soutenir la participation et l'engagement des individus qui ne sont pas bien représentés ou qui peuvent être marginalisés lors des activités de gestion des données (par exemple, en raison de leur âge, de leur sexe et d'autres facteurs de diversité tels que les handicaps, l'appartenance ethnique, la religion ou l'orientation sexuelle), ou qui sont d'une façon ou d'une autre rendues "invisibles", conformément à l'engagement de ne laisser personne de côté. Il s'agit notamment d'encourager la maîtrise des données au sein des communautés.

Protection des données à caractère personnel

Lors de la gestion des données à caractère personnel, les organisations humanitaires sont tenues d'adhérer (i) aux lois nationales et régionales applicables en matière de protection des données, ou (ii) si elles bénéficient de privilèges et d'immunités tels que les lois nationales et régionales ne sont pas applicables, à leurs propres politiques en matière de protection des données.[19] Ces lois et politiques contiennent les principes de protection des données à caractère personnel, tels qu'une liste des bases légitimes valables pour le traitement des données à caractère personnel, dont le consentement.[20] Les organisations humanitaires soumises à une législation nationale ou régionale doivent également tenir compte des lignes directrices et des préavis émis par les autorités compétentes en matière de protection des données au sein de leur juridiction 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 lorsqu'elles élaborent des cadres basés sur des données ouvertes (open data). Conformément à leur engagement en faveur de la redevabilité envers les populations affectées, de l'inclusion et du respect des droits humains, elles doivent défendre le droit des individus concernés à être informés, d'une manière facilement accessible et appropriée, du traitement de leurs données personnelles, à pouvoir demander l'accès, la rectification, la suppression, l'opposition ou des informations sur le traitement de leurs données à caractère personnel, et à ne pas faire l'objet d'une prise de décision automatisée, sauf dans les conditions spécifiques énoncées dans les cadres juridiques applicables à une organisation.

Qualité

La qualité des données doit être maintenue de manière à ce que les propriétaires, les utilisateurs et les autres parties prenantes soient en mesure de se fier aux activités de 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, normalisées, interopérables, bien documentées, actualisées et interprétables, conformément à l'utilisation prévue et en tenant compte du contexte opérationnel donné. Lorsque cela est possible et approprié, et sans compromettre les présents principes, les organisations doivent s'efforcer de collecter et d'analyser les données de manière désagrégée, et ce en fonction de l'âge, du sexe et du handicap, ainsi que par d'autres caractéristiques de la diversité, en fonction des finalités définies d'une activité.

Conservation et destruction

Les organisations doivent établir un calendrier de conservation et de destruction qui indique la durée de conservation des données, le moment où elles doivent être détruites et comment les détruire de manière à rendre leur récupération impossible. 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 stipulée par les lois en vigueur ou les règles d'audit des donateurs. Lorsque les données sensibles sont conservées, les organisations doivent spécifier et garantir un stockage sécurisé et sûr afin d'éviter toute utilisation abusive ou exposition irresponsable. Les données non sensibles peuvent être conservées indéfiniment, conformément aux lois, réglementations et politiques applicables, et à condition que des droits d'accès soient établis et que la sensibilité des données soit réévaluée régulièrement.

19. 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.

20. Les organisations humanitaires peuvent ne pas être en mesure de s'appuyer sur le consentement pour tous les traitements de données à caractère personnel. Pour plus de détails sur les bases juridiques du traitement des données personnelles, voir le **Manuel du CICR sur la protection des données dans l'action humanitaire** (2e édition, 2020). Indépendamment de la base légitime choisie, les droits des personnes concernées garantissent l'agence et l'implication des individus en ce qui concerne la manière dont leurs données personnelles sont traitées.

Transparence
Les organisations doivent gérer les données de manière à offrir une transparence significative aux acteurs humanitaires et aux parties prenantes, en particulier aux populations affectées. Elles doivent notamment fournir des informations pertinentes quant à l'activité de gestion des données, telles que ses objectifs, l'utilisation prévue et les méthodes de partage des données, ainsi que les limites et les risques qui y sont associés.

EXEMPLE D'ÉQUILIBRE DES PRINCIPES EN PRATIQUE

Consulter l'annexe C pour plus d'exemples.

L'exemple ci-dessous illustre la manière dont les Principes interagissent et peuvent être pris en compte conjointement lors de la prise de décisions concernant la gestion des données dans le cadre de l'action humanitaire.

Lors de l'élaboration d'un tableau de bord interactif illustrant les opérations humanitaires dans le cadre d'une intervention, une organisation doit décider si elle autorise l'accès externe, car le tableau de bord présente des données sensibles et non sensibles. D'une part, le principe de confidentialité indique que l'accès doit être restreint. D'autre part, le principe de coordination et de collaboration ainsi que le principe de transparence indiquent que les données non sensibles doivent être mises à disposition.

Pour résoudre cette tension dans l'application des Principes, le développeur ajoute une fonction qui permet de spécifier le contrôle d'accès pour chaque couche de données incluse dans le tableau de bord. Le développeur limite alors l'accès à la couche contenant des données sensibles à certains partenaires humanitaires de confiance qui ont besoin de ces informations pour éclairer leur réponse et à d'autres fins légitimes. La couche contenant les données non sensibles est mise à la disposition du public. Conformément au principe de redevabilité, des procédures opérationnelles (SOPs) sont préparées pour documenter le processus de gestion des données lié à l'élaboration et à la diffusion de ce tableau de bord, avec des rôles, des responsabilités et des autorités clairement définis pour chaque étape et pour les décisions qui ont été prises lors de la conception du tableau de bord, y compris celles concernant les restrictions d'accès.

Grâce à ce processus de décision réfléchi, les Principes sont équilibrés de manière à permettre une approche sécurisée, éthique et efficace de la visualisation des données et de la diffusion des produits de données.

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 de l'ensemble du système (1), au niveau du cluster/secteur (2) et au niveau de l'organisation (3). Par la mise en œuvre de ces actions, les acteurs humanitaires favorisent une gestion sécurisée, éthique et efficace des données.

Les actions s'appliquent à tous les contextes d'intervention humanitaire et à tous les acteurs impliqués dans la gestion opérationnelle des données. Les actions sont destinées à servir de référence commune pour la mise en œuvre de la Responsabilité des données dans un contexte d'intervention humanitaire donné. La mise en œuvre variera selon le contexte d'intervention et nécessitera une adaptation en fonction de la nature d'une crise ou d'une situation particulière. Si certaines de ces actions peuvent être nouvelles au niveau de l'ensemble du système, du cluster/secteur ou de l'organisation dans différents contextes, toutes les actions s'appuient sur les pratiques, processus et outils existants et les complètent. Les acteurs humanitaires et leurs partenaires devront identifier les points d'entrée appropriés pour mettre en œuvre ces actions sur la base de leur évaluation commune de l'état de la Responsabilité des données dans leur contexte.[21]

La mise en œuvre de ces actions à différents niveaux devra être guidée par les Principes présentés dans la section précédente. Les acteurs doivent promouvoir la centralité des populations affectées, leurs droits et leur bien-être lorsqu'ils adaptent les actions aux différents contextes. Pour garantir la mise en œuvre et l'impact durables de ces actions en matière de Responsabilité des données, les acteurs humanitaires devraient identifier les ressources financières, humaines et technologiques nécessaires et prendre des mesures pour les mettre à disposition.

Le tableau ci-dessous présente une description de chaque action et de son objectif par rapport à 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. **L'annexe B** propose des modèles pour soutenir la mise en œuvre des actions. **L'annexe C** présente des exemples de mise en œuvre de ces actions dans différents contextes et domaines programmatiques, tels que la redevabilité aux populations affectées (AAP) et l'assistance sous forme de transferts monétaires.

21. À titre d'exemple, voir le PPI élaboré en 2021 pour l'intervention en Somalie : **https://reliefweb.int/report/somalia/somalia-information-sharing-protocol-september-2021**

Les actions pour la Responsabilité des données dans l'action humanitaire	
Action	**Description et objectif**
Diagnostic de la responsabilité des données [Modèle de diagnostic de la Responsabilité des données]	Un diagnostic de la Responsabilité des données fournit une vue d'ensemble des actions de Responsabilité des données qui ont été mises en œuvre dans le contexte d'intervention. Ce diagnostic permet d'éclairer la hiérarchisation des actions à mettre en œuvre aux trois niveaux.
Registre de gestion des données [Modèle de registre de gestion des données]	Un registre de gestion des données fournit une liste récapitulative des principales activités de gestion des données menées par différents acteurs dans le contexte d'intervention, y compris les données gérées dans le cadre de ces activités. Le registre favorise la complémentarité et la convergence (y compris avec les processus axés sur le développement à plus long terme), facilite la collaboration et permet la priorisation et la prise de décision stratégique concernant la gestion responsable des données. Le registre favorise également une compréhension commune de l'écosystème des données dans le cadre de l'intervention.
Analyse de l'impact des données[22] [Modèle d'analyse de l'impact sur les données]	Une analyse de l'impact des données permet de déterminer les impacts attendus d'une activité de gestion des données et d'identifier des recommandations pour atténuer les impacts négatifs potentiels. Elle doit éclairer la conception et la mise en œuvre d'une activité de gestion des données afin d'en maximiser les avantages et d'en minimiser les risques.
La Responsabilité des données dès la conception [Modèle pour la Responsabilité des données dès la conception] [Modèle d'une POS pour une activité de gestion des données]	La Responsabilité des données dès la conception implique de suivre un ensemble d'étapes et de développer des résultats connexes afin de garantir une gestion sécurisée, éthique et efficace des données dans le cadre d'une activité donnée. L'intégration de considérations relatives à la Responsabilité des données dans la conception, la mise en œuvre, le suivi et l'évaluation des activités de gestion des données permet de maximiser leurs avantages et de minimiser les risques.
Protocole de partage des informations [Modèle de protocole de partage des informations]	Le protocole de partage de l'information (PPI) à l'échelle du système est le principal document de référence régissant le partage des données et des informations dans le cadre de l'intervention. Il doit inclure une classification de la sensibilité des données et des informations spécifiques au contexte[23] soulignant la sensibilité de données et d'informations spécifiques, ainsi qu'une approche recommandée pour le partage de différents types de données dans le cadre de l'intervention. Bien qu'il soit généralement établi à l'échelle du système, les PPI peuvent également être mis en place au niveau du cluster/secteur.
Accord de partage des données [Modèle d'accord de partage de données]	Un accord de partage des données établit les termes et conditions qui régissent le partage de données personnelles et de données non personnelles sensibles entre deux ou plusieurs parties. De nombreux cadres de protection des données exigent un accord de partage des données comme garantie nécessaire pour le partage des données à caractère personnel. Ce type d'accord est essentiel pour le respect des obligations juridiques, politiques et normatives liées au partage des données personnelles et non personnelles sensibles.

22. L'analyse de l'impact des données' est un terme générique qui renvoie à plusieurs types d'évaluations, tels que définis à l'annexe A. Il convient de noter qu'une analyse d'impact sur la protection des données (AIPD) est l'outil et le processus établis dans la législation sur la protection des données qui doivent être utilisés (spécifiquement) pour évaluer les risques liés à la protection des données à caractère personnel et la conformité avec le cadre pertinent de protection des données. Compte tenu du champ d'application des DPIA (limité aux données personnelles), une DIA peut compléter une AIPD en couvrant les avantages, les risques et les inconvénients attendus de la gestion des données non personnelles.

23. La classification de la sensibilité des données et des informations indique le niveau de sensibilité des différents types de données et d'informations dans un contexte donné. Il s'agit d'un élément clé de la ISP, qui doit être élaboré dans le cadre d'un exercice collectif au cours duquel les différentes parties prenantes s'accordent sur ce qui constitue des données sensibles dans leur contexte.

Gestion des incidents liés aux données[24] [Modèle de SOP pour la gestion des incidents liés aux données]	La gestion des incidents liés aux données fait référence aux processus et aux outils permettant d'identifier, de résoudre, de suivre et de communiquer sur les incidents liés aux données. Il s'agit notamment d'une procédure opérationnelle standard pour la gestion des incidents liés données et d'un registre ou d'un journal qui recueille des informations clés sur la nature, la gravité et la résolution de chaque incident. La gestion des incidents liés aux données permet aux acteurs de traiter les incidents. Elle soutient également le développement d'une base de connaissances pour prévenir et mieux traiter les incidents futurs. La communication sur les incidents liés aux données favorise ainsi des approches plus coordonnées de la gestion des incidents au fil du temps et sensibilise l'ensemble du secteur. Lorsque l'incident constitue une violation de données à caractère personnel, les obligations établies dans le cadre de la protection des données et dans les accords de partage de données applicables doivent être respectées.
Coordination et prise de décision sur l'action collective pour la Responsabilité des données	La coordination ainsi que la prise de décision en matière de Responsabilité des données impliquent l'utilisation de différents mécanismes pour encourager l'action collective dans ce domaine. 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 les acteurs impliqués dans une intervention à identifier les possibilités d'améliorer la Responsabilité des données, à suivre les progrès et les difficultés et à s'aligner sur les priorités. Elles favorisent également la responsabilisation et l'investissement commun dans la mise en œuvre des autres actions de ces directives opérationnelles.

24. 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 suivante: https://centre.humdata.org/wp-content/uploads/2019/08/guidanceNote2_dataincidentmanagement.pdf.

Niveau 1: Les actions pour la Responsabilité des données au niveau de l'ensemble du système

Afin de faire progresser la Responsabilité des données au niveau de l'ensemble 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 le HCR[25] , ainsi que d'autres structures de coordination, telles que le ICCG/ISCG et l'IMWG ont des rôles importants à jouer pour soutenir ces actions.

Les organisations humanitaires doivent également travailler avec le ICCG/ISCG et l'IMWG, l'HCT et les officiers de liaison du gouvernement dans le pays pour assurer un engagement significatif avec les organisations et les autorités nationales, en fonction du contexte donné.[26] Un tel engagement va renforcer la capacité de réponse des acteurs nationaux, instaurer la confiance et créer un espace de collaboration productive et de gestion des questions liées aux données.

Étant donné que l'adoption de la Responsabilité des données varie au sein et à travers les contextes de réponse humanitaire, les actions ci-dessous sont destinées à servir de socle commun pour l'adaptation et la mise en œuvre dans un contexte donné. Si certaines actions peuvent être nouvelles à l'échelle du système dans certains contextes, toutes les actions sont conçues pour s'appuyer sur les pratiques, processus et outils existants au sein du système humanitaire et les compléter. Les rôles et responsabilités spécifiques pour la mise en œuvre de chaque action sont présentés dans le tableau ci-dessous.

Actions pour la Responsabilité des données au niveau de l'ensemble du système	
Action	**Approche recommandée**
Mener un diagnostic de la Responsabilité des données au niveau de l'ensemble du système [Modèle de diagnostic de la Responsabilité des données]	Le diagnostic de la Responsabilité des données au niveau de l'ensemble du système présente un aperçu des actions inter-agences/inter-clusters/inter-secteurs pour la Responsabilité des données. Il soutient la prise de décision conjointe sur la manière de cibler et de prioriser l'action collective sur la Responsabilité des données. Ce diagnostic doit être réalisé annuellement par **le(s) mécanisme(s) inter-agence(s) concerné(s)** (y compris le **ICCG/ISCG** et **l'IMWG**) avec le soutien de **OCHA**. Le diagnostic doit être présenté à **l'EHP** et, si possible, partagé avec l'ensemble de la communauté d'intervention par les canaux appropriés, en tant qu'outil de suivi des progrès accomplis sur les questions clés en matière de renforcement de la Responsabilité des données.
Créer et maintenir un registre de gestion des données au niveau de l'ensemble du système [Modèle de registre de gestion des données]	Le registre de gestion des données au niveau de l'ensemble du système fournit un aperçu des activités de gestion des données menées dans le cadre de la réponse humanitaire. Le registre nécessite la contribution des clusters/secteurs et d'autres entités inter-agences. Le registre de gestion des données au niveau de l'ensemble du système doit être mis à jour de manière continue par **le(s) mécanisme(s) interagence(s) concerné(s)** (le **ICCG/ISCG** et le **IMWG**) et présenté à **l'EHP** pour référence. Une version publique du registre de gestion des données devrait être disponible via ReliefWeb.

25. 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 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.

26. 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://reliefweb.int/report/world/operational-guidance-cluster-lead-agencies-working-national-authorities-july-2011, 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.

Développer et maintenir un Protocole de partage des informations au niveau de l'ensemble du système [Modèle de protocole de partage d'informations]	Le protocole de partage des informations (PPI) est le principal document de référence régissant le partage des données et des informations dans le cadre d'une réponse humanitaire. Il doit comprendre une classification de la sensibilité des données et des informations spécifiques au contexte, décrivant la sensibilité de données et d'informations spécifiques ainsi qu'une approche recommandée pour le partage de différents types de données dans le cadre de la réponse. Le PPI doit être élaboré de manière collective et sous la direction **de(s) mécanisme(s) inter-agence(s) concerné(s)** (le **ICCG/ISCG** et le **IMWG**), avec le soutien de **OCHA** et après consultation avec les autorités locales, le cas échéant. Une fois finalisé, le PPI doit être présenté à **HCT** pour approbation. Tous les acteurs impliqués dans la gestion des données dans le cadre de la réponse doivent avoir connaissance du PPI et de leurs rôles et obligations respectifs. Le PPI doit être révisé annuellement, ou plus fréquemment, au besoin. Une version publique du PPI doit être mise à disposition via ReliefWeb, si possible.
Suivre et communiquer au sujet des incidents liés aux données [Modèle SOP pour la gestion des incidents liés aux données]	Au niveau de l'ensemble du système, le suivi des incidents de données doit inclure un registre central qui répertorie les détails clés sur la nature, la gravité ainsi que la résolution des incidents. Le cas échéant, ce registre peut être relié à d'autres processus et outils de suivi des incidents déjà en place au niveau de l'ensemble du système, par exemple les systèmes de surveillance de la sécurité et de l'accès. Des mesures de confidentialité et de protection des données sensibles doivent être prises lors de la création d'un tel registre. Lorsque l'incident constitue une violation de données à caractère personnel, les obligations établies dans le cadre pertinent de protection des données et dans les accords de partage de données applicables doivent être respectées. Le **ICCG/ISCG** et **IMWG** sont chargés d'établir et de maintenir un registre central des incidents de données et de fournir des mises à jour régulières à **HCT**. Ce registre nécessite des contributions des clusters/secteurs et des organisations individuelles.
Soutenir la coordination et la prise de décision sur les actions collectives liées à la Responsabilité des données par le biais des mécanismes interagences existants	Les structures inter-agences et inter-clusters/secteurs doivent fournir un forum ou une plateforme commune pour la coordination et la prise de décision sur la Responsabilité des données au niveau de l'ensemble du système. Ces structures doivent également assurer le suivi des progrès collectifs et/ou des défis et opportunités liés à la Responsabilité des données dans le contexte spécifique. **L'EHP** est responsable du suivi des questions liées à la responsabilité des données. L'**ICCG/ISCG** et **l'IMWG** sont chargés de fournir des rapports réguliers à **l'EHP** sur leurs domaines respectifs en matière de Responsabilité des données.

EXEMPLE D'ACTIONS POUR LA RESPONSABILITÉ DES DONNÉES AU NIVEAU DE L'ENSEMBLE DU SYSTÈME

Des régions d'un pays sont sous le contrôle d'une faction armée depuis cinq ans. La population du nord a besoin d'une aide humanitaire, les besoins les plus importants étant liés à la protection ainsi qu'à la nutrition. La communauté humanitaire a été confrontée à des problèmes d'accès, la faction armée ayant mis en place des restrictions sur le nombre de travailleurs humanitaires dans la région, ainsi que sur le type d'assistance fournis.

Pour faire respecter ces restrictions et recueillir des informations sur la population de la région sous leur contrôle, la faction a contacté l'équipe humanitaire du pays (EHP) pour demander que les listes de bénéficiaires ainsi que les données détaillées sur l'évaluation des besoins au niveau des individus ou des ménages soient partagées mensuellement. L'EHP a également reçu un nombre croissant de rapports de convois arrêtés et retenus aux points de contrôle lorsqu'ils quittent la région du nord. Au cours de ces arrêts, les membres de la faction armée ont exigé que les appareils électroniques stockant des données ainsi que les mots de passe des systèmes de gestion de l'information leur soient remis. L'EHP vise à déterminer s'il existe un moyen de structurer le partage de données et d'informations avec la faction armée afin de prévenir de futurs blocus tout en respectant les principes humanitaires.

Au préalable, les membres de l'IMWG ont assumé leur responsabilité commune de mener une analyse de l'impact sur la protection des données (AIPD), étant donné que les listes de bénéficiaires constituent des données à caractère personnel. Cette analyse a pour but de comprendre l'impact du partage des données sur les personnes concernées et de formuler des recommandations pour l'atténuer. À la suite de cette analyse, les membres de l'IMWG décident de procéder à l'échange de données à caractère personnel afin de garantir un accès continu au territoire à des fins humanitaires et d'éviter de mettre en danger les travailleurs humanitaires. En tant que coresponsables de cette décision, les membres de l'IMWG définissent leurs rôles et responsabilités dans la mise en œuvre des recommandations de l'AIPD, par exemple en veillant à ce que les bénéficiaires, en tant que personnes concernées, soient informés du partage des données, et en mettant en œuvre d'autres garanties opérationnelles, techniques et juridiques afin d'empêcher l'accès non autorisé et l'utilisation abusive des données à caractère personnel par le groupe armé.

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

Faire progresser la Responsabilité des données au niveau des clusters/secteurs nécessite une action collective dans un certain nombre de domaines qui complètent les actions au niveau de l'ensemble du système ainsi qu'au niveau des organisations. Ces actions doivent être mises en œuvre conformément aux directives existantes de l'IASC et des clusters mondiaux. Les homologues des clusters mondiaux doivent être consultés, le cas échéant, lors de la conception et/ou de la mise en œuvre d'actions à ce niveau.

Étant donné que la mise en œuvre de la Responsabilité des données varie au sein et à travers les contextes de réponse humanitaire, les actions ci-dessous pour le niveau des clusters/secteurs sont destinées à servir de socle commun pour l'adaptation et la mise en œuvre dans un contexte donné. Si certaines actions peuvent être nouvelles dans certains contextes, toutes les actions sont conçues pour s'appuyer sur et compléter les pratiques, processus et outils existants au sein du système humanitaire. En fonction du contexte de l'intervention, ces actions peuvent être mises en œuvre par les Leads et Co-Leads des clusters/secteurs et leurs membres respectifs tant au niveau national que local.

Les agences Leads et Co-Leads des clusters/secteurs sont chargées de veiller à la mise en œuvre des actions dans le cadre de la gestion des données opérationnelles d'un cluster/secteur donné. Elles sont également chargées de promouvoir l'adhésion aux lois mondiales et nationales en matière de protection des données (le cas échéant), ainsi que des normes, politiques et standards humanitaires pertinents. Les clusters/secteurs doivent assurer un engagement significatif[27] 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 de collaboration productive et de gestion des questions liées à la gestion des données.

27. 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://reliefweb.int/report/world/operational-guidance-cluster-lead-agencies-working-national-authorities-july-2011, 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.

Les actions pour la Responsabilité des données au niveau des clusters/secteurs	
Action	**Approche recommandée**
Mener un diagnostic de la responsabilité des données au niveau des clusters/secteurs [Modèle de diagnostic de la Responsabilité des données]	Le diagnostic de la Responsabilité des données au niveau des clusters/secteurs présente un aperçu des actions existantes en matière de Responsabilité des données en vigueur au sein des clusters/secteurs. Il permet de hiérarchiser les actions supplémentaires et les activités de soutien fournies par les clusters/secteurs en matière de Responsabilité des données. Il complète et informe le diagnostic au niveau de l'ensemble du système. Les clusters/secteurs doivent également se référer à ce registre avant d'entreprendre toute nouvelle collecte de données afin d'éviter tout doublon, et l'utiliser pour identifier les lacunes dans les données disponibles. Ce diagnostic doit être réalisé puis mis à jour annuellement (ou plus fréquemment si nécessaire) par les **agences Leads et Co-Leads des clusters/secteurs** en collaboration avec leurs **membres**, et mis à disposition sur des plateformes de partage appropriées pour les membres des clusters/secteurs.
Créer et maintenir à jour un registre de gestion des données des clusters/secteurs [Modèle de registre de gestion des données]	Le registre de gestion des données du cluster/secteur doit inclure toutes les activités de gestion des données menées par les clusters/secteurs et celles menées par ses membres. Le registre de gestion des données permet d'éviter la duplication des efforts et de soutenir le partage des données et des informations au sein du cluster/secteur et de manière plus générale pour l'ensemble de la réponse. Il permet également au cluster/secteur de contribuer au registre de gestion des données au niveau de l'ensemble du système. Le registre de gestion des données du cluster/secteur doit être complété puis mis à jour annuellement, ou plus fréquemment si nécessaire, **par les agences Leads et Co-Leads des clusters/secteurs** en collaboration avec leurs **partenaires**.
Développer et maintenir un protocole de partage d'informations au niveau des clusters/secteurs [Modèle de protocole de partage des informations]	Dans les cas où les besoins d'un cluster/secteur en matière de partage de données et d'informations ne sont pas suffisamment pris en compte dans le PPI au niveau de l'ensemble du système, un PPI supplémentaire doit être élaboré et approuvé par tous les membres du cluster/secteur. Le PPI spécifique au cluster/secteur doit être cohérent sur le PPI au niveau de l'ensemble du système[28] et le compléter, ainsi que s'aligner sur les lois, normes, politiques et standards pertinents applicables dans le contexte spécifique. Ce type de PPI doit être développé de manière collective et sous la direction des **agences Leads et Co-Leads des clusters/secteurs** en collaboration avec leurs **partenaires**. Une fois rédigé, le PPI doit être approuvé par tous les partenaires des clusters/secteurs et présenté au(x) mécanisme(s) inter-agences concerné(s) pour référence. Le cas échéant, une version publique du PPI doit être mise à disposition via ReliefWeb. *Remarque : si les membres du cluster/secteur prévoient de partager des données personnelles entre eux, ils doivent établir des accords de partage des données à cette fin (voir Niveau 3 : Actions pour la Responsabilité des données au niveau des organisations).*

28. For an example, see the ISP developed in 2021 for the Somalia response: https://reliefweb.int/report/somalia/somalia-information-sharing-protocol-september-2021

Proposer un appui technique et consultatif aux membres du cluster/secteur en matière de Responsabilité des données	Les ressources humaines, financières et technologiques dédiées à la Responsabilité des données au niveau du cluster/secteur sont essentielles pour renforcer la Responsabilité des données 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 pour le bénéfice de l'ensemble du cluster/secteur. Les contenus relatifs à la Responsabilité des 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 Leads et Co-Leads des clusters/secteurs** ont la responsabilité de promouvoir les ressources nécessaires au sein du cluster/secteur ainsi que de ses partenaires pour être en mesure de gérer les données de manière responsable et de promouvoir les activités de renforcement des capacités pertinentes.
La responsabilité des données dès la conception dans les activités de gestion des données au niveau des clusters/secteurs **[Modèle pour la Responsabilité des données dès la conception]** **[Modèle SOP sur la Responsabilité des données]**	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 entre les membres et avec le gouvernement, le cas échéant. Les **agences Leads et Co-Leads des clusters/secteurs** doivent s'efforcer de concevoir des activités de gestion des données dirigées par les clusters conformément aux présentes directives opérationnelles. Cela pourrait se faire, par exemple, en incluant la Responsabilité des données dans les stratégies des clusters.
Suivre et communiquer au sujet des incidents liés aux données au sein du cluster/secteur **[Modèle SOP pour la gestion des incidents liés aux données]**	Le suivi et la communication des incidents de données au sein du cluster/secteur contribuent à réduire le risque de répétition des incidents. Les activités relatives aux incidents de données comprennent l'établissement d'un registre commun contenant des détails clés sur la nature, la gravité et la résolution des incidents. Un tel registre doit garantir des mesures adéquates de confidentialité et empêcher la divulgation non autorisée de données sensibles. Un mécanisme au niveau des clusters/secteurs pour les incidents de données doit contribuer au suivi des incidents de données au niveau de l'ensemble du système en partageant les informations sur les incidents ainsi que les pratiques exemplaires pour atténuer les risques au sein de la communauté élargie. **Les agences Leads et Co-Leads des clusters/secteurs** ont la responsabilité d'établir et de maintenir un registre des incidents de données qui se 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 de l'ensemble du système.

EXEMPLE D'ACTIONS POUR LA RESPONSABILITÉ DES DONNÉES AU NIVEAU DES CLUSTERS/SECTEURS

Les besoins humanitaires d'un pays ont diminué et la situation sécuritaire s'est stabilisée à telle enseigne que la communauté internationale décide de réduire l'aide humanitaire. Une approche de développement sera mise en place pour remplacer les structures de coordination humanitaire. Cela signifie que le système des clusters sera progressivement éliminé et que les organisations dotées d'un mandat humanitaire réduiront considérablement leur présence. Les organisations à double mandat resteront dans le pays et renforceront leurs activités de développement dans certains cas. L'aide au développement ciblera le risque d'inondations saisonnières, ce qui entraînera des déplacements de population ainsi que la réparation des infrastructures physiques et sociales. Le gouvernement est étroitement impliqué dans la fourniture de l'aide au développement, notamment dans la gestion des données et de l'information.

Les clusters et les partenaires humanitaires déterminent comment gérer de manière responsable les données qu'ils ont collectées au cours de la dizaine d'années depuis le début de la crise humanitaire. Une agence Lead d'un cluster décide de d'élaborer un registre de gestion des données pour son cluster afin d'obtenir un aperçu de ses activités de gestion des données et des données gérées au sein de chaque activité. À l'aide du modèle de registre de gestion des données, le point focal de gestion de l'information du cluster développe le registre. En fonction du registre et du protocole de partage de l'information disponible dans la réponse, le Lead du cluster détermine pour chaque donnée personnelle et non personnelle si elle doit être transmise aux partenaires restés dans le pays, conservée ou détruite.

Chaque organisation sera responsable de la décision de conserver ou de supprimer les données à caractère personnel qu'elle a collectées conformément à son propre calendrier de conservation, et de notifier les personnes concernées.

Le partage des données à caractère personnel avec le gouvernement nécessitera probablement une analyse de l'impact du transfert de données et une notification aux personnes concernées par le transfert de leurs données.

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

Le maintien de la Responsabilité des données au niveau de l'organisation dans un contexte d'intervention donné est essentiel à la mise en œuvre des actions pour la Responsabilité des données à la fois au niveau de l'ensemble du système et au niveau des clusters/secteurs. 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.

Étant donné que les niveaux de prise en compte de la Responsabilité des données varient au sein et à travers les contextes de réponse humanitaire, les actions ci-dessous doivent servir de socle commun pour l'adaptation et la mise en œuvre dans un contexte donné. Si certaines actions peuvent être nouvelles pour une organisation, toutes les actions sont conçues pour s'appuyer sur et compléter les pratiques, processus et outils existants au sein du système 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 de l'organisation. 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. En outre, les organisations doivent se mettre en rapport avec les organes de coordination tels que l'ICCG/ISG et l'IMWG, les partenaires, les bailleurs de fonds et d'autres organisations dans leur contexte d'intervention afin de demander un soutien technique ou consultatif, le cas échéant.

Les actions pour la Responsabilité des données au niveau des organisations	
Action	**Approche recommandée**
Mener un diagnostic de la Responsabilité des données au niveau des organisations **[Modèle de diagnostic 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'une organisation dans un contexte humanitaire donné. Le diagnostic facilite la priorisation de l'action collective en matière de Responsabilité des données et favorise l'identification des opportunités de collaboration et d'action collective en matière de Responsabilité des données au sein du/des clusters/secteurs et d'autres forums inter-agences dont l'organisation est membre. Ce diagnostic doit être réalisé annuellement ou lorsque les circonstances dans un contexte d'intervention ou les politiques ou pratiques de gestion des données d'une organisation changent considérablement.
Créer et maintenir à jour un registre de gestion des données au niveau de l'organisation **[Modèle de registre de gestion des données]**	Les organisations doivent faire le suivi toutes les activités de gestion des données qu'elles dirigent ou auxquelles elles interviennent via un registre de gestion des données. Elles doivent se référer à ce registre lorsqu'elles contribuent aux registres de gestion des données des clusters/secteurs et au niveau de l'ensemble du système. Les organisations doivent également se référer à ce registre avant d'entreprendre toute nouvelle collecte de données afin d'éviter tout doublon, et l'utiliser pour identifier les lacunes dans les données disponibles. 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 **[Modèle d'analyse de l'impact des données]**	Des analyses de l'impact des données (AID) doivent être réalisées pour toutes les activités de gestion des données impliquant des données sensibles. 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 doit être remodelée ou interrompue si les risques et les préjudices prévisibles dépassent les bénéfices escomptés, et ce en dépit des mesures de prévention et d'atténuation. Les résultats des AID doivent être partagés avec les acteurs clé impliqués dans une activité de gestion des données et, le cas échéant, avec les partenaires qui planifient une activité similaire dans le contexte spécifique. Cela favorise la cohérence de l'évaluation, du suivi et de l'atténuation des risques liés aux données au fil du temps. *Note : De nombreuses organisations disposent de politiques, d'exigences et de directives spécifiques sur la manière dont les AID doivent être menées. Pour celles qui n'en ont pas, le modèle présent en **Annexe B** peut servir de référence utile.*
La Responsabilité des données dès la conception dans les activités de gestion des données dirigées par les organisations **[Modèle pour la Responsabilité des données dès la conception]** **[Modèle POS sur la Responsabilité des données]**	Les organisations doivent intégrer la Responsabilité des données dans les activités de gestion des données, et ce dès leur conception dans le cadre de la planification de toute activité de gestion des données. La Responsabilité des données dès la conception comprend, par exemple, les étapes et considérations suivantes : • Résoudre les points identifiés dans l'analyse de l'impact sur les données d'une activité de gestion des données par des mesures de prévention et d'atténuation appropriées, réalisables et solides pour tous les risques majeurs identifiés. • Lors de la sélection des outils de gestion des données, favoriser la complémentarité, l'interopérabilité (le cas échéant, y compris avec les systèmes gouvernementaux et autres systèmes locaux) et l'harmonisation (y compris en ce qui concerne la terminologie, les typologies et la structure des données). • Promouvoir les mesures de gestion sécurisée des données (par exemple, pour l'anonymisation des données,[29] la fourniture de solutions de stockage et de transfert de données sécurisées, etc.) • Adhérer aux directives et protocoles pertinents en matière de Responsabilité des données et aux processus et procédures connexes, y compris les PPI. Il s'agit notamment de veiller à ce que toutes les données qui doivent être partagées à des fins spécifiques soient mises à disposition par des canaux appropriés de manière sécurisée, avec les garanties nécessaires pour les données à caractère personnel et dans le respect des cadres applicables en matière de protection des données. • Établir des procédures opérationnelles normalisées claires et reproductibles et du matériel de formation pour le personnel, ainsi qu'un calendrier pour la formation du nouveau personnel à la Responsabilité des données. • Veiller à ce que les individus puissent demander l'accès, la vérification, la rectification et la suppression de leurs données à caractère personnel.

29. Il peut s'agir d'approches techniques telles que le contrôle de la divulgation statistique, qui est une technique utilisée en statistique pour évaluer et réduire le risque qu'un individu ou une organisation soit réidentifiés à partir des résultats d'une analyse de données d'enquête ou de données administratives, ou lors de la publication de microdonnées. Pour plus d'informations, voir The Centre for Humanitarian Data, Guidance Note : Statistical Disclosure Control (2019), disponible à l'adresse suivante : **https://centre.humdata.org/guidance-note-statistical-disclosure-control/**.

Établir des accords de partage de données afin de réguler le transfert de données à caractère personnel et/ou de données non personnelles sensibles **[Modèle d'accord de partage de données]**	Les organisations doivent conclure des accords de partage de données pour permettre le partage responsable de données à caractère personnel ou de données non personnelles sensibles avec d'autres intervenants, conformément aux exigences institutionnelles, juridiques et réglementaires appropriées; ainsi qu'aux Principes énoncés dans les présentes directives opérationnelles. Les accords de partage des données peuvent être spécifiques à un contexte ou établis à l'échelle mondiale pour régir le partage des données dans de multiples contextes d'intervention. *Note : Bien que les objectifs, les modalités et les circonstances du partage des données diffèrent plus que de raison pour fournir un modèle unique d'accord de partage de données, le modèle figurant à **l'annexe B** offre un ensemble de points à prendre en considération pour élaborer de tels accords, au cas où des modèles n'existeraient pas déjà au sein de l'organisation.*
Établir des procédures opérationnelles standards pour la gestion des incidents liés aux données **[Modèle de POS pour la gestion des incidents liés aux données]**	Les organisations doivent élaborer et mettre en place leurs propres procédures opérationnelles standard (POS) pour gérer les incidents liés aux données. Ces procédures doivent inclure un processus de notification, de classification, de traitement et de clôture de l'incident. Elles doivent également prévoir un moyen d'enregistrer les incidents dans la base de connaissances de l'organisation (par exemple, en utilisant un registre qui répertorie des informations clés sur la nature, la sévérité et la résolution de chaque incident). Ces procédures doivent également prévoir des voies de rectification et de recours appropriées pour les individus touchés par un incident, conformément au cadre applicable en matière de protection des données et de la vie privée. Les organisations doivent partager leur expérience en matière de gestion et d'atténuation des incidents liés aux données avec d'autres acteurs, c'est-à-dire au niveau des clusters/secteurs et du système.

EXEMPLE D'ACTIONS POUR LA RESPONSABILITÉ DES DONNÉES AU NIVEAU DES ORGANISATIONSLEVELLEVEL

Dans un pays qui souffre depuis longtemps de crises prolongées, on s'attend à une recrudescence de la violence à l'occasion des élections controversées qui se tiendront d'ici la fin de l'année. Un groupe particulièrement vulnérable subit des violences depuis des décennies et craint que ces élections n'entraînent une nouvelle détérioration de sa situation. De l'autre côté de la frontière, où ce groupe est moins discriminé, il y a un camp de réfugiés où le groupe X est majoritaire.

Dans le cadre de son plan de contingence, une organisation humanitaire s'attend à un afflux de réfugiés et demande des fonds d'aide d'urgence pour modifier son système d'enregistrement. L'organisation propose d'utiliser les scans d'iris comme système d'enregistrement et de gestion de l'identité. L'identifiant fonctionnel ancré dans un identifiant biométrique sera essentiel pour gérer la livraison d'articles non alimentaires (NFI) dans le camp, en veillant à ce que l'aide NFI ne soit reçue que par des personnes qui sont enregistrés comme bénéficiaires officiels au nom de leur ménage et dans les quantités auxquelles le ménage a droit.

Pour évaluer les risques et les préjudices prévisibles associés à la collecte proposée de données biométriques, l'organisation réalise une analyse d'impact sur la protection des données, dirigée par son responsable de la protection des données. La boîte à outils de protection des données de l'organisation contient un modèle d'analyse d'impact sur la protection des données (AIPD) à utiliser pour les données à caractère personnel. L'AIPD commence par évaluer les finalités définies et la proportionnalité de la collecte de données biométriques, et examine si les mêmes finalités pourraient être atteintes par des moyens moins intrusifs pour la vie privée que la biométrie. Elle examine ensuite le fondement légitime de l'utilisation des scanners de l'iris et détermine si l'organisation est en mesure de proposer d'autres modalités de vérification de l'identité et de donner aux bénéficiaires le libre choix quant à la manière de s'authentifier pour recevoir de l'aide. L'analyse contextuelle montre que l'utilisation des données biométriques est proportionnée aux finalités déclarées et qu'aucune autre modalité d'authentification disponible n'offre le même niveau d'assurance que les données biométriques. Étant donné que l'organisation ne peut pas fonder le traitement des données biométriques sur le consentement, elle doit établir des procédures pour traiter les objections des personnes concernées à l'enregistrement biométrique. L'organisation doit également prendre en considération les implications à long terme de la collecte de données biométriques, telles que, par exemple, les pressions prévisibles exercées par les autorités nationales pour qu'elles transmettent les données biométriques de l'ensemble de la population du camp.

SUIVI, ÉVALUATION ET APPRENTISSAGE

Compte tenu de l'évolution rapide de l'écosystème des données humanitaires et de l'importance croissante de la gestion des données dans tous les domaines de l'action humanitaire, le suivi, l'évaluation et l'apprentissage (MEL) sont essentiels à une pratique efficace de la Responsabilité des données.

Le diagnostic de la Responsabilité des données (outil inclus dans **l'annexe B**) doit constituer la base du MEL pour la Responsabilité des données. Un tel diagnostic fournit un aperçu des mesures prises quant à la Responsabilité des données au niveau de l'ensemble du système, des clusters/secteurs ou de l'organisation dans un contexte d'intervention. En plus d'aider à identifier les opportunités ainsi que les défis liés à la gestion des données et d'éclairer la priorisation d'actions supplémentaires pour la Responsabilité des données dans le contexte, un diagnostic peut également servir de base de référence pour le suivi du statut d'adoption et de la maturité des différentes actions pour la Responsabilité des données par rapport auxquelles les organisations, les clusters/secteurs et les entités au niveau de l'ensemble du système peuvent suivre et évaluer leurs progrès au fil du temps.

Dans le cadre d'une réponse humanitaire :

- Un diagnostic au **niveau de l'ensemble du système** doit être réalisé conjointement par **ICCG/ISCG** et **l'IMWG** avec le soutien de **OCHA**, et présenté à l'**EHP** pour référence.

- Un diagnostic **au niveau du cluster/secteur** doit être réalisé par les **agences Leads et Co-Leads des clusters/secteurs** en collaboration avec leurs membres et partagé avec les entités concernées à l'échelle du système afin de favoriser l'apprentissage entre pairs.

- Un diagnostic au **niveau de l'organisation** doit être réalisé par un groupe interfonctionnel de personnel impliqué dans la gestion des données et présenté à la direction pour examen.

À chaque niveau, le diagnostic doit être réalisé et mis à jour annuellement ou plus fréquemment, au besoin (en cas de changements importants dans le contexte opérationnel ou la réponse humanitaire par exemple).

En plus de vérifier quand et comment différentes mesures ont été prises en matière de Responsabilité des données, les acteurs aux différents niveaux de l'intervention humanitaire doivent également évaluer l'impact de ces mesures au fil du temps. Les entités, les clusters/secteurs ainsi que les organisations au niveau de l'ensemble du système doivent définir des indicateurs d'évaluation de l'impact adaptés au contexte et susceptibles d'être suivis et vérifiés systématiquement dans le cadre des activités globales de gestion des programmes et des résultats.

ANNEXE A: TERMES ET DÉFINITIONS

Accord de partage de données : Accord qui établit les modalités régissant le partage de données personnelles et de données sensibles non personnelles. Il est principalement utilisé pour le partage de données entre deux ou plusieurs parties. Conformément aux cadres de protection des données, la signature d'un accord de partage des données peut être requise pour le partage de données à caractère personnel.

Activité de gestion des données : Toute activité distincte impliquant la gestion de données et d'informations dans le cadre de la réponse humanitaire. Cela comprend la conception de l'activité, ainsi que la collecte, la réception, le stockage, l'assurance qualité, l'analyse, le partage, l'utilisation, la conservation et la destruction des données et des informations par les acteurs humanitaires.

Analyse de l'impact des données : L'analyse de l'impact des données est un terme générique qui fait référence à une variété d'outils utilisés pour déterminer les impacts positifs et négatifs potentiels d'une activité de gestion des données. Il s'agit notamment d'outils couramment utilisés et parfois exigés par la loi tels que les évaluations de l'impact sur la protection des données et les évaluations de l'impact sur la vie privée.

Analyse d'impact relative à la protection des données : Un outil et un processus permettant d'évaluer les impacts sur la protection des personnes concernées lors du traitement de leurs données personnelles et d'identifier les mesures correctives nécessaires afin d'éviter ou de minimiser ces impacts.[30]

Analyse d'impact sur la vie privée : Un processus qui aide les organisations à identifier et à minimiser les risques pour la vie privée des nouveaux projets ou des nouvelles politiques.[31]

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.[32]

Consentement : Toute indication librement donnée, spécifique, informée et claire de l'accord de l'individu concerné pour le traitement de ses données à caractère personnel.[33] [34]

Données : Représentation ré-interprétable de l'information, de manière formalisée qui convient à la communication, l'interprétation ou le traitement.[35]

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

31. United Kingdom, Information Commissioner's Office (ICO), *Conducting Privacy Impact Assessments Code of Practice*, undated, https://ico.org.uk/media/about-the-ico/consultations/2052/draft-conducting-privacy-impact-assessments-code-of-practice.pdf.

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

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

34. Les enfants dépendent souvent du consentement d'autres personnes pour leur participation à des programmes et services susceptibles de générer et d'enregistrer des données à caractère personnel. Même lorsque les enfants ont le choix d'accepter ou de refuser un service, il peut leur être difficile, en fonction de leur stade de développement, d'évaluer les risques et les avantages qui y sont associés. C'est pourquoi les enfants doivent faire l'objet d'une attention particulière quant à la manière dont ils sont informés de leurs droits en tant que personnes concernées. Ces **modèles de l'UNICEF** peuvent contribuer à garantir que les informations relatives au consentement/à l'ascension sont fournies de manière appropriée et intelligible.

35. 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.

Données à caractère personnel : Toute information se rapportant à une personne physique identifiée ou identifiable (“personne concernée”).[36]

Données à caractère non personnel : Toute information qui ne se rapporte pas à une personne concernée.[37]

Données anonymes : Données qui ont fait l’objet d’un processus technique de suppression ou de modification de tous les identifiants et codes personnels de telle sorte que les individus concernés ne puissent être identifiées par aucun moyen raisonnablement susceptible d’être utilisé à partir des données seules ou en combinaison avec d’autres données. Cela résulte d’un processus spécifique au contexte dans lequel ce processus technique est complété, le cas échéant, par d’autres mesures techniques, organisationnelles ou juridiques ou par d’autres engagements contraignants visant à réduire les risques de réidentification des individus concernés.[38]

Données biométriques : Données utilisées pour la reconnaissance automatisée des individus sur la base de leurs caractéristiques biologiques et comportementales.[39]

Données sensibles : Données qui, si elles sont divulguées ou consultées sans autorisation appropriée, sont susceptibles de causer :

- un préjudice (tel que des sanctions, une discrimination) à tout individu, y compris la source des informations ou d’autres individus ou groupes identifiables.
- un impact négatif sur la capacité d’une organisation à mener à bien ses activités ou sur la perception du public à l’égard de cette organisation.[40]

Les données personnelles et non personnelles peuvent être sensibles. La sensibilité des données est définie en fonction du contexte de l’intervention. Les mêmes types de données peuvent présenter des niveaux de sensibilité différents selon le contexte, et la sensibilité peut évoluer au fil du temps. De nombreuses organisations disposent de systèmes de classification et d’outils spécifiques pour évaluer ce qui constitue des données sensibles, et ce afin de faciliter les pratiques de gestion responsable des données.[41]

Éthique des données : L’éthique des données est la branche de l’éthique qui étudie et évalue les problèmes moraux liés aux données (y compris la génération, l’enregistrement, la conservation, le traitement, la diffusion, le partage et l’utilisation), aux algorithmes (y compris l’intelligence artificielle, les agents artificiels, l’apprentissage automatique et les robots) et aux pratiques correspondantes (y compris l’innovation responsable, la programmation, le piratage et les codes professionnels).[42]

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

37. En se basant sur la définition de ‘personal data’ in ICRC, *Handbook on Data Protection in Humanitarian Action* (2020), https://www.icrc.org/en/data-protection-humanitarian-action-handbook.

38. UNHCR, *General Policy on Personal Data Protection and Privacy* (2022), https://www.refworld.org/docid/63d3bdf94.html.

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

40. Basé sur la définition du Groupe consultatif sur les “Normes professionnelles” dirigé par le CICR, 2018, 3e édition. Normes professionnelles pour le travail de protection ; Chapitre 6 : Gestion des données et des informations aux fins de la protection https://www.icrc.org/en/publication/0999-professional-standards-protection-work-carried-out-humanitarian-and-human-rights.

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

42. Floridi L., Taddeo M. *What is data Ethics?* (2016) Phil. Trans. R. Soc. A 374: 20160360. http://dx.doi.org/10.1098/rsta.2016.0360.

Gestion opérationnelle des données : La collecte ou la réception, le stockage, l'assurance qualité, l'analyse, le partage, l'utilisation, la conservation et la destruction de données et d'informations par les acteurs humanitaires en vue d'une réponse opérationnelle. La gestion des données opérationnelles s'inscrit dans le cadre de l'action humanitaire tout au long du cycle de planification et d'intervention et comprend des activités telles que l'analyse de la situation, l'évaluation des besoins, la gestion des données sur la population, l'enregistrement et le recensement, la gestion des cas, la communication avec les populations touchées, le suivi de la protection, ainsi que le suivi et l'évaluation de l'intervention.

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, provoqués de façon accidentelle ou intentionnelle, avec des objectifs illégaux ou autrement non autorisés, causant des dommages ou ayant le potentiel.[43]

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.[44]

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.[45]

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 dont bénéficie cette personne physique en ce qui concerne ses données à caractère personnel, même lorsque ces données sont recueillies, collectées ou traitées d'une autre manière par d'autres personnes.[46]

Préjudice : Les implications négatives d'une initiative de traitement des données sur les droits d'une personne concernée ou d'un groupe de personnes concernées, ou d'autres personnes, y compris, mais sans s'y limiter, les préjudices physiques et psychologiques, la discrimination et le refus d'accès à des services.[47]

Prise de décision automatisée : Processus de prise de décision par le traitement de données à caractère personnel par des moyens automatisés et sans examen ni intervention de la part d'un individu.[48]

Protection des données : L'application systématique d'un ensemble de garanties institutionnelles, techniques et physiques qui préservent le droit à la vie privée en ce qui concerne le traitement des données à caractère personnel.[49]

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

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

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

46. UN OCHA, *OCHA Data Responsibility Guidelines* (2021), https://centre.humdata.org/the-ocha-data-responsibility-guidelines/.

47. UN OCHA, *OCHA Data Responsibility Guidelines* (2021), https://centre.humdata.org/the-ocha-data-responsibility-guidelines/.

48. UNHCR, *General Policy on Personal Data Protection and Privacy* (2022), https://www.refworld.org/docid/63d3bdf94.html.

49. Définition élaborée par le UN Privacy Policy Group (2017).

Protocole de partage de l'information : Le principal document de référence régissant le partage des données et des informations dans le cadre d'une intervention, y compris une classification de la sensibilité des données et des informations et les modalités de partage.

Redevabilité envers les populations affectées : L'AAP est un engagement des humanitaires à utiliser le pouvoir de manière responsable : prendre en compte, rendre compte et être tenu pour responsable par les personnes que nous cherchons à aider.[50]

Registre de gestion des données : Un registre de gestion des données fournit un résumé des principales activités de gestion des données menées par différents acteurs dans le contexte de la réponse humanitaire, y compris les données gérées dans le cadre de ces activités.[51]

Ré-identification : Processus par lequel des données dépersonnalisées, pseudonymes ou anonymes peuvent être retracées ou reliées à une ou plusieurs personnes ou à un ou plusieurs groupes de personnes par des moyens raisonnablement disponibles au moment de la réidentification des données.[52]

Responsabilité des données : La gestion sécurisée, éthique et efficace des données personnelles et non personnelles en vue d'une réponse opérationnelle.

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 accidentelles ou intentionnelles, illégales ou non autorisées.[53]

Vie privée : Le concept selon lequel 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.[54]

50. IASC, *Strengthening Accountability to Affected People (n.d.)*: https://interagencystandingcommittee.org/strengthening-accountability-affected-people.

51. En se basant sur la définition du Centre for Humanitarian Data, *Tip Sheet on Understanding Data Ecosystems* (2022), https://data.humdata.org/dataset/2048a947-5714-4220-905b-e662cbcd14c8/resource/3281e066-2643-46f0-aecf-43ee7374a453/download/tip-sheet-understanding-data-ecosystems.pdf?_gl=1*cgh816*_ga*MTE2OTY5MjM0My4xNjcyNzU2NDcz*_ga_E60ZNX2F68*MTY3MzYxODU0MS4xMy4xLjE2NzM2MTk0OTUuNjAuMC4w.

52. With minor edits, based on UN OCHA, *OCHA Data Responsibility Guidelines* (2021), https://centre.humdata.org/the-ocha-dataresponsibility-guidelines/.

53. The Centre for Humanitarian Data. *Glossary*: https://centre.humdata.org/glossary/.

54. UN General Assembly, International Covenant on Civil and Political Rights (1976), https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx.

ANNEXE B: MODÈLES POUR LA RESPONSABILITÉ DES DONNÉES

Les modèles suivants sont conçus pour soutenir la mise en œuvre des actions recommandées pour la Responsabilité des données présentées dans ces directives opérationnelles.

Ces modèles sont fournis à titre d'exemple pour aider les entités au niveau de l'ensemble du système, les clusters/secteurs et les organisations à mettre en pratique les actions présentées dans ces directives opérationnelles. Ils ne remplacent pas les modèles existants lorsque ceux-ci existent déjà dans une organisation, que ce soit par la pratique ou par la politique.

Ces modèles continueront d'être mis à jour en fonction des commentaires reçus et des enseignements tirés de leur utilisation au fil du temps. Chaque modèle comprend une section d'introduction décrivant son objectif, sa (ses) source(s) ainsi que des instructions pour son adaptation et son utilisation.

- **Modèle de diagnostic de la Responsabilité des données**
- **Registre de gestion des données**
- **Modèle d'analyse de l'impact des données**
- **La Responsabilité des données dès la conception**
- **Procédure opérationnelle standard pour une activité de gestion des données**
- **Modèle de protocole de partage d'informations (y compris une classification de la sensibilité des données)**
- **Modèle d'accord de partage de données**
- **Procédure opérationnelle standard pour la gestion des incidents liés aux données**

ANNEXE C: EXEMPLES DE RESPONSABILITÉ DES DONNÉES DANS LA PRATIQUE

Le groupe de travail sur la Responsabilité des données (DRWG) continuera à suivre la mise en œuvre de la Responsabilité des données dans la pratique dans différents contextes d'intervention et à mettre à jour **cette liste d'exemples (en anglais)**. Les exemples illustrent le caractère pratique des Principes en montrant comment ils peuvent éclairer et influer sur la gestion des données opérationnelles.

Les acteurs humanitaires désireux de partager leurs expériences en matière de Responsabilité des données peuvent soumettre leurs exemples au moyen de **ce formulaire**.

ANNEXE D: RESSOURCES ET RÉFÉRENCES

Les documents suivants ont été inclus dans l'analyse documentaire qui a alimenté la rédaction des présentes directives opérationnelles[55] en 2020 et sa révision ultérieure en 2022.[56]

Abraham, Schneider, Vom Brocke, 2019. Data Governance, A Conceptual Framework, Structured Review and Research Agenda, **https://doi.org/10.1016/j.ijinfomgt.2019.07.008**

Ada Lovelace Institute, 2021. Participatory Data Stewardship: **https://www.adalovelaceinstitute.org/report/participatory-data-stewardship/**

African Union (AU-ISC), 2018. AU Data Policy Framework: **https://au.int/sites/default/files/documents/42078-doc-AU-DATA-POLICY-FRAMEWORK-ENG1.pdf**

ASEAN TELMIN (AEC), 2016. ASEAN Framework on Personal Data Protection: **https://www.dataguidance.com/legal-research/asean-framework-personal-data-protection**

Baker, E. and Nia, G. (Atlantic Council), 2022. Attacks on Hospitals from Syria to Ukraine: **https://www.atlanticcouncil.org/wp-content/uploads/2022/06/Attacks-on-Hospitals-from-Syria-to-Ukraine-Improving-Prevention-and-Accountability-Mechanisms.pdf**

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 Raftree, L., 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**

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

Core Humanitarian Standard 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**

Council of Europe, 1981. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS 108) and Protocols, Strasbourg: **https://www.coe.int/en/web/data-protection/convention108-and-protocol**

55. Consulter l'analyse documentaire réalisée par le sous-groupe de l'IASC sur la responsabilité en matière de données en collaboration avec l'Université de Delft à l'adresse suivante : **https://centre.humdata.org/survey-results-on-priorities-for-data-responsibility-in-humanitarian-action/**

56. Les résultats de l'analyse documentaire menée par le groupe de travail sur la Responsabilité des données en collaboration avec l'université de Yale sont disponibles sur demande auprès du DRWG.

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://www.calpnetwork.org/wp-content/uploads/2020/06/DataStarterKitforFieldStaffELAN.pdf

European Centre for Development Policy Management (ECDPM), 2022. Digitalisation in humanitarian aid: opportunities and challenges in forgotten crises: https://ecdpm.org/wp-content/uploads/Digitalisation-humanitarian-aid-ECDPM-Briefing-note-143-2022.pdf

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

Fast, L., 2022. Data Sharing between humanitarian organizations and donors: https://www.humanitarianstudies.no/resource/data-sharing-between-humanitarian-organisations-and-donors/

Floridi L., Taddeo M. 2016. What is data Ethics? Philosophical Transactions of the Royal Society A: 20160360: http://dx.doi.org/10.1098/rsta.2016.0360

Gazi, T., 2022. Data To The Rescue: How Humanitarian Organizations Should Collect Information Based on the GDPR: https://jhumanitarianaction.springeropen.com/articles/10.1186/s41018-020-00078-0

Geiß, R. and Lahmann, H., 2021. Protection of Data in Armed Conflict: https://digital-commons.usnwc. edu/cgi/viewcontent.cgi?article=2964&context=ils

Global Public Policy Institute (GPPI), 2021. Risks associated with humanitarian data sharing with donors: https://gppi.net/2021/09/06/data-sharing-with-humanitarian-donors

Global Migration Group (GMG) & OHCHR, 2018. Principles and Guidelines, Supported by Practical Guidance, on the Human Rights Protection of Migrants in Vulnerable Situations: https://www.ohchr.org/en/migration/migrants-vulnerable-situations

Global Partnership for Sustainable Development Data (Data4SDGs), 2022. The Data Values Project White Paper Reimagining Data and Power: A roadmap for putting values at the heart of data: https://www.data4sdgs.org/reimagining-data-and-power-roadmap-putting-values-heart-data

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.pdf

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

Human Rights Watch, 2014. Data privacy policies and procedures for handling data: https://www.hrw.org/privacy-policy-0

International Committee of the Red Cross (ICRC)-led Advisory Group on Professional Standards, 2018, 3rd edition. 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

International Committee of the Red Cross (ICRC), 2015. Data Protection Framework: https://www.icrc.org/en/document/icrc-data-protection-framework

International Federation of Red Cross and Red Crescent Societies (IFRC), 2021. Code of Conduct for the International Red Cross and Red Crescent Movement and NGOs in Disaster Relief: https://www.ifrc.org/code-conduct-international-red-cross-and-red-crescent-movement-and-ngos-disaster-relief

Institute of Development Studies (by Iffat Idris), 2021. Documentation of survivors of gender-based violence (GBV):
https://reliefweb.int/report/world/documentation-survivors-gender-based-violence-gbv

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

Inter-Agency Standing Committee (IASC), 2017. Commitments on Accountability to Affected People and Protection from Sexual Exploitation and Abuse, available at:
https://interagencystandingcommittee.org/accountability-affected-populations-including-protection-sexual-exploitation-and-abuse/documents-56

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 Medical Corps, 2022. Privacy Policy:
https://internationalmedicalcorps.org/privacy-policy/

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

Krishnan, A, 2022. Humanitarian Digital Ethics: A Foresight and Decolonial Governance Approach: https://carrcenter.hks.harvard.edu/publications/humanitarian-digital-ethics

Médecins Sans Frontières, 2013. Data Sharing Policy: https://www.msf.org/sites/default/files/msf_data_sharing_policy_final_061213.pdf

Médecin Sans Frontières (MSF), 2021. Information on how DWB handles data collection and management of personal information: https://www.doctorswithoutborders.ca/privacy-notice#:~:text=We%20collect%20personal%20information%20in,for%20which%20it%20was%20collected

Mercy Corps, 2022. Data Protection and Privacy Guides. https://github.com/mercycorps/DPP-guides Alternate format: https://www.mercycorps.org/research-resources/data-protection-privacy-guides

Mercy Corps, 2020. Responsible Data Toolkit: https://www.mercycorps.org/research-resources/responsible-data-toolkit

MERL Tech, 2022. Responsible Data Governance for M&E in Africa: https://merltech.org/new-guides-responsible-data-governance-for-me-in-africa/

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

Organization for Economic Cooperation and Development (OECD), 2013. Data Protection Principles for the 21st century: https://www.repository.law.indiana.edu/facbooks/23/

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 Cluster (Ukraine), 2022. Protecting and Prioritising People with Specific Needs in the Ukrainian Humanitarian Response: https://reliefweb.int/report/ukraine/protecting-prioritising-people-specific-needs-ukrainian-humanitarian-response-may-2022-enuk

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.im-portal.org/sites/alnap-dev.mrmdev.co.uk/files/content/attachments/2021-05-25/1.01%20Introduction%20to%20Tdh%20Data%20Protection%20Starter%20Guide.pdf

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

United Kingdom, Information Commissioner's Office (ICO), undated. Conducting Privacy Impact Assessments Code of Practice: https://ico.org.uk/media/about-the-ico/consultations/2052/draft-conducting-privacy-impact-assessments-code-of-practice.pdf

Adapted from United Kingdom National Archives, 2017. Information Asset Fact Sheet: https://www.nationalarchives.gov.uk/documents/information-management/information-assets-factsheet.pdf

United Nations, 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

United Nations Department of Management, Archives and Records Management Section, 2012. User Guide to Retention Schedule Implementation: https://archives.un.org/sites/archives.un.org/files/general/documents/guideline_retention_schedule_implementation.pdf

United Nations Department of Management, Archives and Records Management Section. Examples of Retention Schedules: https://archives.un.org/content/retention-schedules

UN General Assembly, 1976. International Covenant on Civil and Political Rights: https://www.ohchr. org/en/professionalinterest/pages/ccpr.aspx

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

United Nations Office for the Coordination of Humanitarian Affairs (UN OCHA), 2021. OCHA Data Responsibility Guidelines: https://centre.humdata.org/the-ocha-data-responsibility-guidelines/

United Nations Office for the Coordination of Humanitarian Affairs (UN OCHA), Centre for Humanitarian Data, 2019. Guidance Note: Data Incident Management: https://centre.humdata.org/wp-content/uploads/2019/08/guidanceNote2_dataincidentmanagement.pdf

United Nations Office for the Coordination of Humanitarian Affairs (UN OCHA), Centre for Humanitarian Data, 2020. Guidance Note: Humanitarian Data Ethics: https://centre.humdata.org/guidance-note-humanitarian-data-ethics/

United Nations Office for the Coordination of Humanitarian Affairs (UN OCHA), Centre for Humanitarian Data, 2019. Guidance Note on Statistical Disclosure Control:
https://centre.humdata.org/guidance-note-statistical-disclosure-control/

United Nations Office for the Coordination of Humanitarian Affairs (UN OCHA), Centre for Humanitarian Data, 2020. Guidance Note on Data Responsibility in Public-Private Partnerships:
https://centre.humdata.org/guidance-note-data-responsibility-in-public-private-partnerships/

United Nations Office for the Coordination of Humanitarian Affairs (UN OCHA), Centre for Humanitarian Data, 2020. Guidance Note on Data Impact Assessments:
https://centre.humdata.org/guidance-note-data-impact-assessments/

United Nations Office for the Coordination of Humanitarian Affairs (UN OCHA), Centre for Humanitarian Data, 2020. Guidance Note on Data Responsibility in Cash and Voucher Assistance:
https://centre.humdata.org/guidance-note-data-responsibility-in-cash-and-voucher-assistance/

United Nations Office for the Coordination of Humanitarian Affairs (UN OCHA), Centre for Humanitarian Data, 2020. Guidance Note on Responsible Data Sharing with Donors:
https://centre.humdata.org/guidance-note-responsible-data-sharing-with-donors/

United Nations Office for the Coordination of Humanitarian Affairs (UN OCHA), Centre for Humanitarian Data, 2020. Guidance Note on Responsible Approaches to Data Sharing:
https://centre.humdata.org/guidance-note-responsible-approaches-to-data-sharing/

United Nations Office for the Coordination of Humanitarian Affairs (UN OCHA), Centre for Humanitarian Data, 2022. Tip Sheet on Understanding Data Ecosystems:
https://centre.humdata.org/tip-sheet-understanding-data-ecosystems/

United Nations Office for the Coordination of Humanitarian Affairs (UN OCHA), 2022. OCHA on Message: Humanitarian Principles:
https://www.unocha.org/sites/unocha/files/OOM_Humanitarian%20Principles_Eng.pdf

United Nations Office for the Coordination of Humanitarian Affairs (UN OCHA) / World Economic Forum (WEF), prepared for IASC, 2007. Guiding Principles for Public-Private Collaboration for Humanitarian Action: https://digitallibrary.un.org/record/613220?ln=en

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

United Nations 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

United Nations Secretariat, 2022. Data strategy of the Secretary-General for action by everyone, everywhere with insight, impact and integrity, 2020-22:
https://digitallibrary.un.org/record/3872047?ln=en

United Nations Children's Fund (UNICEF), 2021. Procedures for Ethical Standards in Research, Evaluation, Data Collection and Analysis: UNICEF Ethics in EEG (unicef-irc.org)

United Nations Children's Fund (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

United Nations Children's Fund (UNICEF), 2020. UNICEF Policy on Personal Data Protection: https://www.unicef.org/supply/media/5356/file/Policy-on-personal-data-protection-July2020.pdf.pdf

United Nations Children's Fund (UNICEF), 2020. Do-It-Yourself Toolkit: https://data.unicef.org/wp-content/uploads/2020/12/Data-for-Children-Do-It-Yourself-Toolkit.pdf

United Nations Children's Fund (UNICEF)/NYU Governance Laboratory (GovLab), 2019. Responsible Data for Children Synthesis report: https://rd4c.org/files/rd4c-report-final.pdf

United Nations Children's Fund (UNICEF)/NYU Governance Laboratory (GovLab), 2022. RD4C Toolkit: https://rd4c.org/tools/

United Nations Children's Fund (UNICEF)/NYU Governance Laboratory (GovLab)/United Nations Office for the Coordination of Humanitarian Affairs (OCHA), 2021. Comparative Assessment of the IASC and RD4C Principles: https://rd4c.org/articles/rd4c-brief-data-responsibility-in-humanitarian-action-to-improve-childrens-lives/index.html

United Nations High Commissioner for Refugees (UNHCR), 2022. General Policy on Personal Data Protection and Privacy: https://www.refworld.org/docid/63d3bdf94.html

United Nations High Commissioner for Refugees (UNHCR), 2015. Policy on the Protection of Personal Data of Persons of Concern to UNHCR: https://www.refworld.org/pdfid/55643c1d4.pdf

United Nations High Commissioner for Refugees (UNHCR), 2018. Guidance on the Protection of Personal Data of Persons of Concern to UNHCR: https://www.refworld.org/docid/5b360f4d4.html

United Nations High Commissioner for Refugees (UNHCR), 2019. Data Transformation Strategy 2020-2025: Supporting protection and solutions: https://www.unhcr.org/5dc2e4734.pdf

United Nations 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

United Nations 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

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

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

United Nations 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

United Nations 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

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

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

United Nations 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

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

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

United Nations 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

United States Agency for International Development (USAID), 2019. Considerations for Using Data Responsibly at USAID: https://www.usaid.gov/responsibledata

World Food Programme (WFP), 2016. WFP Guide to Personal Data Protection and Privacy: https://docs.wfp.org/api/documents/e8d24e70cc11448383495caca154cb97/download/

World Food Programme (WFP), 2022. Strategic Evaluation of WFP's use of technology in constrained environments: https://www.wfp.org/publications/strategic-evaluation-wfps-use-technology-constrained-environments

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

World Health Organization (WHO) (European Region), 2020. Collection and Integration of Data on Refugee and Migrant Health in the WHO European Region: https://apps.who.int/iris/bitstream/handle/10665/337694/9789289055369-eng.pdf

World Bank Group, 2018. Personal Data Privacy Policy: http://documents.worldbank.org/curated/en/466121527794054484/pdf/Privacy-Board-Paper-050318-vF-05042018.pdf

World Refugee Council and Centre for International Governance (Dragana Kaurin), 2019. Data Protection and Digital Agency for Refugees: https://www.cigionline.org/static/documents/documents/WRC%20Research%20Paper%20no.12.pdf

World Vision International, 2017. Data Protection, Privacy, and Security for Humanitarian and Development Programs: https://www.wvi.org/health/publication/data-protection-privacy-and-security-humanitarian-development-programs

ANNEXE E: CONTEXTE DE L'ÉLABORATION ET DE LA RÉVISION DES PRÉSENTES DIRECTIVES OPÉRATIONNELLES

Contexte de la première édition (approuvée en février 2021)
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[57] qui représentent les différentes parties prenantes du système humanitaire.

Le sous-groupe a élaboré les présentes directives opérationnelles dans le cadre d'un processus de collaboration et de consultation avec les membres du IASC et la communauté humanitaire au sens large, les ONG, les organismes des Nations unies, d'autres organisations internationales et les donateurs aux niveaux mondial, régional et national. L'élaboration des directives opérationnelles s'est appuyée sur une analyse documentaire,[58] une consultation publique,[59] une période de retour d'information ouverte et trois phases d'examen structuré et organisationnel du projet de directives opérationnelles à différents stades de développement.

Les directives opérationnelles ont été approuvées par le IASC en février 2021. La première édition peut être consultée **sur cette page**.

Contexte de la deuxième édition (révisée en 2022 et approuvée en mars 2023)
Compte tenu de la nature dynamique et évolutive des défis et des opportunités en matière de la Responsabilité des données dans l'action humanitaire, le IASC a convenu de réviser et d'actualiser les présentes directives opérationnelles[60] de manière collaborative et consultative tous les deux ans. En juin 2022, l'OPAG d'IASC a officiellement délégué la responsabilité de diriger ce processus de révision au groupe de travail mondial sur la Responsabilité des données (DRWG).[61]

Le DRWG a achevé le processus de révision entre juin 2022 et février 2023. La révision s'est appuyée sur les actions suivantes :

- Une analyse documentaire.
- Une consultation publique auprès des acteurs humanitaires de plus de 50 pays.
- 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.

57. 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.

58. Le sous-groupe a procédé à l'analyse documentaire des orientations existantes sur la responsabilité des données avec le soutien de l'Université technique de Delft.

59. La consultation publique a été réalisée en ligne du 27 février au 18 mars 2020. Les résultats sont disponibles ici : **https://centre.humdata.org/survey-results-on-priorities-for-data-responsibility-in-humanitarian-action/**.

60. OCHA sera chargé de lancer le processus de révision et de mise à jour de ces directives opérationnelles.

61. Le DRWG est un organe de coordination mondial qui s'efforce de faire progresser la Responsabilité des données dans l'ensemble du système humanitaire. Il rassemble un groupe diversifié de parties prenantes, dont des entités des Nations unies, d'autres organisations internationales, des organisations non gouvernementales et d'autres acteurs engagés dans la coordination et la mise en œuvre de l'action humanitaire. Le DRWG est coprésidé par le Conseil danois pour les réfugiés (DRC), l'OIM, l'OCHA et le HCR. Plus d'informations sur le DRWG sont disponibles **ici**.

- Une période de rétroaction ouverte au cours de laquelle 100 collègues de 25 organisations différentes ont apporté des contributions et des commentaires sur le projet de directives opérationnelles.
- Trois phases d'examen structuré et organisationnel du projet de directives opérationnelles à différents stades de sa révision.