OCHA CONSIGNES SUR LA RESPONSABILITÉ DES DONNÉES

TRADUCTION FRANÇAISE

OCTOBRE 2021

OCHA CENTRE FOR
HUMANITARIAN DATA

OCHA

centre for humdata

TABLE DES MATIERES

AVANT-PROPOS

La Responsabilité des données dans l'action humanitaire désigne la gestion sécurisée, éthique et efficace des données à caractère personnel et non personnel (ci-après 'les données personnelles et non personnelles') dans la réponse opérationnelle. La Responsabilité des données est une question cruciale à aborder, et les enjeux sont importants.

Les Consignes d'OCHA sur la Responsabilité des données ('les 'Consignes') offrent un ensemble de principes, procédures et outils qui favorisent la Responsabilité des données dans le travail d'OCHA.[1]

Le principal utilisateur visé par les Consignes est le personnel d'OCHA qui gère les données dans le cadre des fonctions essentielles d'OCHA telles que la coordination, le plaidoyer, la politique, le financement humanitaire et la gestion de l'information, avec un accent particulier sur le travail sur le terrain.

Les Consignes s'appliquent sur une série d'analyses concernant les lacunes existantes ainsi que des études et les apprentissages sur le terrain menées par OCHA au cours des dernières années.[2] Cela inclut un pilotage intensif d'une version préliminaire des consignes par les bureaux d'OCHA dans dix contextes de réponse en 2019 et 2020, avec le soutien du Centre for Humanitarian Data d'OCHA (" le Centre "). Ces pilotes ont alimenté la révision des consignes en vue de leur finalisation et de leur approbation en 2021.

Les Directives reflètent les dernières orientations et les instructions politiques globales au sein du Secrétariat des Nations Unies (ONU) et du système humanitaire au sens large, notamment :

- Plan d'action de coopération numérique du Secrétaire général[3]
- The Secretary-General's Data Strategy[4]
- Les Directives opérationnelles de l'IASC sur la Responsabilité des données dans l'action humanitaire[6]

Les Consignes reflètent également les publications administratives à venir en matière de protection des données et de la vie privée pour l'organisation. Consultez l'annexe E pour une liste des références qui ont servi à l'élaboration des Consignes et l'annexe F pour une sélection de ressources supplémentaires relatives à la responsabilité en matière de données dans l'action humanitaire.

Les Consignes seront revisitées tous les deux ans.

[1] En tant que bureau du Secrétariat des Nations Unies, OCHA est soumis aux politiques et directives applicables du Secrétariat. Aux fins des Consignes sur la Responsabilité des données d'OCHA, le terme Bureau est utilisé pour désigner OCHA. Toutefois, les références aux principes et aux actions en matière de responsabilité des données au sein des et entre les 'organisations humanitaires' s'appliquent à OCHA en tant que bureau du Secrétariat des Nations Unies.

[2] Cela comprend : (a) des recherches menées en 2016 avec le NYU Governance Lab (GovLab) et l'Université de Leiden pour mieux comprendre le contexte des politiques et de la protection de la vie privée, et pour comprendre les meilleures pratiques connexes des organisations partenaires ; (b) une enquête menée par le Centre for Humanitarian Data en mars 2018 auprès du personnel d'OCHA travaillant avec des informations et/ou des données ; et (c) des études de terrain menées en 2018 avec le Centre et les bureaux d'OCHA pour mieux comprendre comment les données sensibles sont partagées et utilisées par le personnel d'OCHA et les partenaires humanitaires dans les environnements de conflit.

[3] Nations Unies, Assemblée Générale (2020), Rapport du Secrétaire général: **Plan d'action de coopération numérique : application des recommandations du Groupe de haut niveau sur la coopération numérique**.

[4] United Nations, **Data Strategy of the Secretary-General, 2020-2022**.

[5] Inter-Agency Standing Committee (2021), **Directives opérationnelles sur la Responsabilité des données dans l'action humanitaire**.

STRUCTURE DES CONSIGNES

Les Consignes comprennent cinq sections et des annexes connexes.

Section 1: Introduction offre une vue d'ensemble des notions clés en matière de la Responsabilité des données dans l'action humanitaire, explique le rôle d'OCHA dans la gestion des données humanitaires et clarifie le champ d'application des Consignes.

Section 2: Principes pour la Responsabilité des données introduit les principes au niveau du système visant à guider la mise en œuvre des Consignes.

Section 3: La Responsabilité des données en pratique fournit des conseils pratiques sur la manière dont OCHA devrait soutenir les actions en faveur de la Responsabilité des données au niveau du système, des clusters/secteurs et des organisations (c.-à-d. dans les bureaux d'OCHA et dans les activités de gestion des données d'OCHA).

Section 4: Redevabilité décrit les principaux rôles et responsabilités pour assurer l'adoption des Consignes et explique leur lien avec les fonctions de gouvernance et de contrôle établies par les futurs textes administratifs du Secrétariat des Nations Unies en matière de protection des données et de la vie privée.

Section 5: Services d'appui à l'adoption des Consignes offre un aperçu des services disponibles au personnel d'OCHA pour mettre en œuvre les Consignes. Ces services sont proposés par le Centre for Humanitarian Data d'OCHA et sont disponibles sur demande.

Annexe A - Définitions présente les définitions principales utilisées dans les Consignes.

Annexe B - Principes pour la Responsabilité des données présente une description détaillée des Principes.

Annexe C - La Responsabilité des données dans la gestion des données d'OCHA présente une série d'étapes que le personnel d'OCHA doivent suivre pour maintenir la Responsabilité des données dans une activité de gestion des données spécifique.

Annexe D - Modèles pour la Responsabilité des données présente tous les différents modèles qui ont été référencés dans les Consignes. Des versions modifiables de chaque modèle sont disponibles via les liens inclus dans l'annexe.

Annexe E - Bases fondatrices pour la Responsabilité des données au sein d'OCHA présente une vue d'ensemble des instruments existants qui guident directement ou indirectement la gestion des données d'OCHA.

Annexe F - Ressources additionnelles présente une série de références relatives à la Responsabilité des données dans le secteur.

COMMENT UTILISER LES CONSIGNES

Les Consignes présentent une approche globale et constituent les normes minimales pour la Responsabilité des données à travers OCHA. Étant donné que la Responsabilité des données varie en fonction des fonctions et des réponses opérationnelles, la manière dont ces Consignes seront utilisées prendra plusieurs formes. Le tableau ci-dessous présente quelques recommandations pour une utilisation efficace des Consignes dans différents scénarios dans lesquels le personnel d'OCHA gère des données.

Scénario	Comment utiliser les Consigne
Préparation aux situations d'urgence[6]	Le personnel impliqué dans les préparations aux situations d'urgence doit considérer les actions dans les sections 3.1 et 3.3 des Consignes. • Concernant le profilage et monitoring des risques (Risk Profiling and Monitoring), réaliser un diagnostic de la Responsabilité des données au niveau du système. • Concernant les Mesures minimales de Préparation (Minimum Preparedness Actions en anglais), élaborer un protocole de partage des informations au niveau du système et des procédures opérationnelles pour toute activité de gestion des données dirigée par OCHA. • Concernant les Mesures de préparation avancées (Advanced Preparedness Actions) et le Plan de contingence (Contingency Planning), élaborer une procédure opérationnelle standard pour la gestion des incidents liés aux données. Les modèles d'OCHA dans l'annexe D incluent des instructions pour la préparation aux situations d'urgence.
Nouveau contexte de réponse	Dans un nouveau contexte de réponse, le personnel devrait se focaliser sur les différentes actions au niveau du système humanitaire, telles que précisées dans la section 3.1 des Consignes. En soutenant ces actions dès le début de la réponse, un standard élevé sera instauré pour la gestion des données ce qui permettra aussi à OCHA de se positionner comme facilitateur en matière de la Responsabilité des données.
Contexte de réponse déjà existant sans actions établies pour la Responsabilité des données	Dans un contexte de réponse 'en cours' mais sans actions établies en matière de la Responsabilité des données, le personnel a deux possibilités pour commencer à utiliser les Consignes: • En commençant avec les actions au niveau du système, telles que la mise en place d'un protocole de partage des informations, suivis par les actions pour la Responsabilité des données au sein des différentes activités de gestion des données dirigées ou coordonnées par l'OCHA. • En introduisant d'abord les actions pour la Responsabilité des données au sein d'une activité de gestion des données spécifique (telle qu'une évaluation des besoins) pour démontrer l'importance du travail en matière de responsabilité des données, avant d'initier des actions au niveau du système.

[6] Ces instructions sont en ligne avec les **IASC Guidelines on Emergency Response Preparedness (draft for field testing)**, Juillet 2015.

Contexte de réponse déjà existant avec quelques actions établies pour la Responsabilité des données	La majorité des contextes de crise prolongée dans lesquels OCHA est présent auront mis en place au moins quelques actions pour la Responsabilité des données. Dans de tels contextes, le personnel devrait réaliser un diagnostic de la Responsabilité des données au niveau du système (voir section 3.1) afin de déterminer quelles actions sont prioritaires.
Équipes globales ou régionales qui dirigent ou soutiennent des activités de gestion des données	Le personnel au siège et dans les bureaux régionaux chargé de la gestion des données doit se concentrer sur les conseils et les résultats dans l'annexe C.

De nombreux services de soutien sont à la disposition du personnel qui utilise les Consignes dans ces scénarios et dans d'autres situations. Pour plus d'informations, consultez la **section 5: Services d'appui à l'adoption des Consignes**.

ACRONYMES

3W	Who is doing What, Where?
4W	Who is doing What, Where, When?
AID	Analyse de l'impact des données
APD	Accord de partage des données
AAWG	Groupe de travail sur l'évaluation et l'analyse
EHP	Equipe humanitaire du pays
HAO	Chargé des affaires humanitaires
HoO	Chef de bureau
IASC	Inter-Agency Standing Committee (Comité permanent interorganisations)
ICCG	Groupe de coordination inter-cluster (Inter-Cluster Coordination Group)
IM	Gestion de l'information (Information Management)
IMB	Direction de la gestion de l'information (Information Management Branch)
IMO	Responsable de la gestion de l'information (Information Management Officer)
IMWG	Groupe de travail de la gestion de l'information (Information Management Working Group)
ISCG	Groupe de coordination inter-secteur (Inter-Sector Coordination Group)
OCHA	IBureau de la coordination des affaires humanitaires des Nations Unies
ONG	Organisations nongouvernementales
ONU	Organisation des Nations unies
POS	Procédure opérationnelle standard
PPI	Protocole de partage des informations

1. INTRODUCTION

1.1 LA RESPONSABILITÉ DES DONNÉES

Les données se trouvent au centre des réponses humanitaires. La gestion des données relatives aux contextes de crises, des personnes affectées et des actions humanitaires permet à la communauté humanitaire de répondre plus efficacement. Cependant, comme les organisations gèrent des volumes de données de plus en plus importants, elles sont également confrontées à des défis et à des risques plus complexes.

La gestion irresponsable des données dans le cadre d'une réponse humanitaire peut exposer les personnes et les communautés déjà vulnérables à des risques accrus, par exemple en exposant leur localisation ou en identifiant une vulnérabilité particulière. Cette situation est particulièrement préoccupante lorsque les acteurs humanitaires traitent des données sensibles, c'est-à-dire des données susceptibles d'exposer les personnes concernées à des risques élevés en cas d'exposition.

Les données personnelles et non personnelles peuvent être sensibles dans l'action humanitaire. S'il existe une compréhension commune de la sensibilité des données personnelles dans le secteur, la détermination de la sensibilité des données non personnelles se révèle plus complexe. La localisation des centres médicaux, par exemple, peut être sensible dans des contextes de conflit en mettant les patients et le personnel en danger, tandis que cette information est typiquement moins sensible dans des contextes de réponse aux catastrophes naturelles. Les Consignes aident le personnel d'OCHA à déterminer la sensibilité des données et à prendre des actions pour assurer une gestion responsable des données.

Ces dernières années, nous avons assisté au développement de principes, de politiques et de stratégies pour la Responsabilité des données dans l'action humanitaire. Il s'agit notamment des documents d'orientations à l'échelle du système, tel que les Directives opérationnelles du Comité permanent interorganisations (CPIO ou IASC en anglais) sur la Responsabilité des données dans l'action humanitaire, ainsi que de stratégies et de politiques globales visant à encadrer la gestion des données au sein du système des Nations Unies, tel que la 'Roadmap for Digital Cooperation' du Secrétaire général et les publications administratives à venir pour l'organisation concernant la protection des données et la vie privée. Malgré des progrès considérables, des lacunes subsistent entre les cadres globaux et leur application pratique dans les opérations sur le terrain.

Les Consignes sur la Responsabilité des données d'OCHA ('les Consignes') sont conçues pour combler ces lacunes en appuyant le personnel d'OCHA à intégrer les cadres globaux sur la responsabilité des données dans leur travail quotidien.

DÉFINITIONS

La **Responsabilité des données** est la gestion sécurisée, éthique et efficace des données personnelles et non personnelles pour la réponse opérationnelle, conformément aux cadres réglementaires en vigueur sur la protection des données à caractère personnel.

- **Sécurisée** | Les activités de gestion des données garantissent la sécurité des données à tout moment, respectent les droits humains et autres obligations légales, et sont mises en œuvre de façon à ne pas nuire (principe du 'Do No Harm').
- **Éthique** | Les activités de gestion des données sont conformes aux cadres et aux standards en vigueur concernant l'éthique humanitaire[7] et la gestion éthique des données.
- **Efficace** | Les activités de gestion des données atteignent les objectifs qui ont motivé leur mise en place.

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

La Responsabilité des données exige la mise en œuvre d'actions fondées sur des principes à tous les niveaux de la réponse humanitaire. Ceci inclut par exemple des actions pour garantir la protection des données et la sécurité des données, ainsi que des stratégies pour atténuer les risques tout en maximisant les bénéfices de la gestion des données opérationnelles. Bien que la Responsabilité des données soit liée à la protection des données et à la sécurité des données, il s'agit de termes différents.

La protection des données fait référence à l'application systématique d'un ensemble de garanties institutionnelles, techniques et physiques qui préservent le droit à la vie privée dans le respect du traitement des données personnelles.

La sécurité des données, applicable à la fois aux données à caractère personnel et non personnel, fait référence aux mesures techniques et organisationnelles visant à préserver la confidentialité, la disponibilité et l'intégrité des données.

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

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

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

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

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

1.2 LE RÔLE D'OCHA DANS LA GESTION DES DONNÉES HUMANITAIRES

OCHA joue un rôle important et unique dans la gestion des données humanitaires à travers ses fonctions principales de plaidoyer, de coordination, de financement, de gestion de l'information, et de stratégie. Alors que d'autres organisations humanitaires traitent les données principalement pour leur propre usage, la gestion des données d'OCHA est principalement axée sur l'agrégation et l'analyse pour la communauté humanitaire au sens large.

Dans la majorité des réponses, les agences, fonds et programmes des Nations Unies et les organisations non-gouvernementales (ONG) partenaires collectent des données spécifiques au secteurs ou au clusters, telles que des données sur les besoins en abri ou sur la consommation alimentaire, pour guider leurs propres activités de réponse. OCHA rassemble les données de ces différents partenaires pour créer une vue globale de la situation humanitaire. Ceci aide à éviter la duplication, et favorise la prise de décisions par les responsables des opérations et des politiques sur le terrain et aux sièges.

OCHA a également un rôle essentiel dans la coordination des activités de gestion des données impliquant un groupe diversifié d'acteurs.

Le nombre d'acteurs engagés dans la réponse aux crises ayant augmenté, le modèle traditionnel de coordination centralisée ("hub and spoke model" en anglais) s'est transformé en un modèle de réseau. Dans ce modèle, l'OCHA continue d'agréger les données pour l'analyse de la situation mais assume également le rôle additionnel en tant que 'facilitateur de réseau'. Le rôle d'OCHA en matière de données dans un réseau est de connecter les partenaires les uns aux autres, en fournissant des services tels que des normes communes et une infrastructure basée sur le cloud pour le stockage et le transfert responsable des données. En cette époque de données numériques, le rôle d'OCHA en tant que 'facilitateur de réseau' doit prendre en compte le risque d'héberger ou de servir de relais pour les données sensibles des partenaires humanitaires et des tiers. Les Consignes sont conçues pour soutenir ce rôle.

1.3 CHAMP D'APPLICATION DES CONSIGNES

Les Consignes s'appliquent à toutes les données opérationnelles gérées directement par OCHA, les données gérées au nom d'OCHA, ou les données gérées par des acteurs humanitaires dans le cadre d'activités coordonnées par OCHA dans différents contextes de réponse. Cela inclut les types de données suivants :

- **Les données sur le contexte** dans lequel se déroule une réponse (par exemple les cadres juridiques, les conditions politiques, sociales et économiques, l'infrastructure, etc.) et les éléments de contexte spécifiques à la situation humanitaire (par exemple les incidents de sécurité, les risques de protection, les facteurs et les causes sous-jacentes de la crise).

- **Les données sur les populations affectées par la situation humanitaire**, leurs besoins, les menaces et les vulnérabilités auxquelles elles sont confrontées, ainsi que leurs capacités (par exemple les données des évaluations des besoins, les données démographiques, les données sur la mobilité).

- **Les données sur les acteurs de la réponse humanitaire et leurs activités** (par exemple les données sur les 3W, les données sur l'accès, les données sur la perception des communautés, et les données sur le financement humanitaire).

Des activités de gestion des données opérationnelles courantes pour OCHA incluent les analyses situationnelles, les évaluations des besoins, les 3W/4W, la communication avec les populations affectées, le suivi de l'accès, et le suivi et l'évaluation de la réponse. La gestion des données liées au fonctionnement interne d'OCHA, telles que les données liées aux ressources humaines et au financement, est réglée par des règlements en vigueur au sein du Secrétariat de l'ONU et ne relèvent pas du champ d'application des Consignes.

Les Consignes abordent également la manière dont OCHA doit soutenir la mise en œuvre des Directives opérationnelles de l'IASC sur la Responsabilité des données au niveau du système, des clusters/secteurs et des bureaux (organisations) d'OCHA.

Les Consignes s'adressent principalement au personnel d'OCHA impliqué dans la gestion des données à travers les fonctions principales d'OCHA, avec un accent particulier sur le terrain.

2. PRINCIPES POUR LA RESPONSABILITÉ DES DONNÉES DANS L'ACTION HUMANITAIRE

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

Les Principes suivants pour la Responsabilité des données dans l'action humanitaire (ci-après définis comme les "Principes") sont conçus pour permettre la gestion sécurisée, éthique et efficace des données dans l'action humanitaire. Ils ont été développés et approuvés dans le cadre des Directives opérationnelles de l'IASC sur la Responsabilité des données. Les Principes doivent guider le personnel d'OCHA et ses partenaires dans leur mise en application des actions recommandées en matière de Responsabilité des données issues de ces Consignes. Les Principes ci-dessous sont présentés par ordre alphabétique (dans leur ordre original en anglais) sans hiérarchie particulière.

Les Principes pour la Responsabilité des données dans l'action humanitaire	
Redevabilité	Confidentialité
Coordination et Collaboration	Sécurité des données
Finalité, nécessité et proportionnalité	Equité et légitimit
Approche basée sur les droits humains	Approche inclusive et axée sur la personne
Protection des données à caractère personnel	Qualité
Conservation et destruction	Transparence

Consultez l'annexe B pour une description détaillée des Principes.

Ces Principes reposent sur une analyse de principes existants relatifs à la gestion des données à travers le secteur humanitaire et le secteur du développement.[8] Ces Principes aident à renforcer l'engagement primordial des humanitaires envers le principe humanitaire cardinal de "**Ne pas nuire**" (Do No Harm), tout en **maximisant les avantages** que les données apportent à l'action humanitaire.[9] Les Principes réaffirment également que les populations affectées, leurs droits et leur bien-être sont au cœur de l'action humanitaire.

La gestion de **données personnelles** doit être guidée par le *Principe sur la protection des données personnelles*[10] alors que la gestion des **données non personnelles** doit être guidée par les autres Principes. Les Principes ci-dessous sont présentés par ordre alphabétique sans hiérarchie particulière.

Lorsque ces principes sont en conflit les uns avec les autres dans leur interprétation ou leur application, les acteurs humanitaires doivent évaluer soigneusement la manière de procéder en fonction de la dynamique particulière de la réponse. En cas de conflit entre ces Principes et les politiques internes ou les obligations légales applicables, ces dernières prévalent.

[8] Une liste complète des documents analysés par le Sous-groupe sur la responsabilité des données est disponible dans les Directives opérationnelles sur la Responsabilité des données dans l'action humanitaire.

[9] Voir: Mary B. Anderson, *Do No Harm: How Aid Can Support Peace - Or War*, (1999).

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

3. LES ACTIONS RECOMMANDÉES PAR L'IASC POUR LA RESPONSABILITÉ DES DONNÉES DANS LE CONTEXTE DE LA RÉPONSE HUMANITAIRE

3 LES ACTIONS RECOMMANDÉES PAR L'IASC POUR LA RESPONSABILITÉ DES DONNÉES DANS LE CONTEXTE DE LA RÉPONSE HUMANITAIRE

Les Directives opérationnelles de l'IASC sur la Responsabilité des données dans l'action humanitaire recommande **huit actions** pour la Responsabilité des données. Ces actions sont résumées dans le tableau ci-dessous. Les actions sont conçues pour être réalisées à trois niveaux dans une réponse donnée: au niveau du système (par exemple au niveau de l'Équipe humanitaire du pays, ou des groupes de coordination inter-secteur/inter-cluster), au niveau des clusters/secteurs, et au niveau des organisations. Cette section des Consignes présente des orientations additionnelles pour le personnel d'OCHA pour faciliter ou mettre en œuvre les actions pour la Responsabilité des données à ces différents niveaux. Dans ces Consignes, le 'niveau des organisations' s'applique aux bureaux d'OCHA.

Diagnostic de la Responsabilité des données

Un diagnostic de la Responsabilité des données implique l'identification et l'examen des lois, normes, politiques et standards existants dans le contexte spécifique de la réponse, ainsi que des processus et procédures et des outils techniques pour la gestion des données.

Cartographie de l'écosystème des données et registre des ressources de données

La cartographie de l'écosystème des données présente un résumé des activités de gestion des données, y compris l'échelle, la portée, et les types de données qui sont traitées, les parties prenantes, les flux de données entre les différents acteurs, ainsi que les procœssus et plateformes utilisés.

Un registre de ressources de données présente le résumé des jeux de données clés qui sont générés et gérés par différents acteurs dans un contexte donné.

Analyse de l'impact des données[11]

L'analyse de l'impact des données (AID) permet de déterminer les risques et les bénéfices envisagés, ainsi que les impacts d'une activité de gestion des données sur la vie privée, la protection des données, et/ou sur les droits humains.

La Responsabilité des données à la conception

La Responsabilité des données dès la conception implique que les Principes pour la Responsabilité des données dans l'action humanitaire sont pris en compte dès le début d'une activité de gestion des données (y compris les phases de conception et de planification) et que l'adhésion à ces Principes peut être vérifiée tout au long du processus.

Protocole de partage des informations & Classification de la sensibilité des données et informations

Un Protocole de partage des informations (PPI) doit inclure une classification de la sensibilité des données et informations pour le contexte spécifique,[12] les actions communes en vue de promouvoir la Responsabilité des données, des clauses quant au respect de la protection des données personnelles au besoin, et aussi inclure des instructions quant au traitement des incidents.

Accord de partage des données

Un accord de partage des données (APD) établit les modalités qui régissent le partage des données personnelles ou des données sensibles non personnelles. Il est utilisé surtout pour le partage de données bilatéral et est typiquement établi au niveau national. Conformément aux cadres de la protection des données, la signature d'un APD est obligatoire pour le partage de données personnelles.

Gestion des incidents liés aux données[13]

Afin de gérer, répertorier et communiquer sur les incidents liés aux données, il faut établir une procédure opérationnelle standard pour la gestion des incidents et un registre central qui reflète les détails clés concernant la nature, la sévérité et la résolution de chaque incident.

Coordination et prise de décisions sur l'action collective pour la Responsabilité des données

Des mécanismes existants peuvent être employés pour coordonner et prendre des décisions sur l'action collective pour la Responsabilité des données aux différents niveaux d'une réponse humanitaire. Ceci inclut, entre autres, l'Équipe humanitaire du pays (EHP, ou HCT en anglais), le mécanisme de coordination inter-clusters, et les clusters/secteurs.

[11] 'Analyse de l'impact des données' (AID) est un terme générique qui fait référence à de multiples types d'évaluations, telles que définies dans l'annexe A.

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

[13] Pour plus d'informations sur la gestion des incidents liés aux données, veuillez consulter : OCHA Centre for Humanitarian Data, *Note d'orientation: La gestion des incidents liés aux données* (2019), disponible à l'adresse : **https://data.humdata.org/dataset/2048a947-5714-4220-905b-e662cbcd14c8/resource/f9fd4b55-d7c7-4f93-9345-b6365098e15d/download/guidance-note-2-french-updated.pdf**.

3.1 LE RÔLE D'OCHA DANS LES ACTIONS POUR LA RESPONSABILITÉ DES DONNÉES AU NIVEAU DU SYSTÈME

Le niveau du système désigne les structures de coordination majeures dans une réponse donnée, par exemple l'équipe humanitaire de pays (EHP ou HCT en anglais) et le groupe de coordination inter-clusters/inter-secteurs (ICCG/ISCG). En tant que convocateur de l'ICCG/ISCG et de divers groupes de travail techniques (par exemple, le groupe de travail sur la gestion de l'information [IMWG], le groupe de travail sur l'accès [AWG], le groupe de travail sur l'évaluation et l'analyse [AAWG], etc.), OCHA a un rôle important à jouer en soutenant les actions pour la Responsabilité des données au niveau du système. Il y a cinq actions que le personnel d'OCHA doit prioriser au niveau du système.

01

Mener un diagnostic de la Responsabilité des données au niveau du système

Objectif:

Un diagnostic de la Responsabilité des données au niveau du système aide à identifier des opportunités et défis communs pour la gestion responsable des données, informe la priorisation des actions pour la Responsabilité des données à différents niveaux d'une réponse, et permet de présenter à l'EHP une compréhension globale de la Responsabilité des données dans la réponse.

Rôle d'OCHA:

OCHA est responsable d'initier et de faciliter le diagnostic de la Responsabilité des données au niveau du système, et de présenter le diagnostic finalisé à l'EHP pour commentaires.

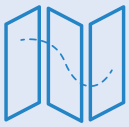
Approche recommandée:

- ☐ Préparez un projet de diagnostic à l'aide du **modèle pour Diagnostic de la Responsabilité des données** de l'IASC. Un tel exercice nécessitera probablement des contributions des équipes de coordination et de gestion de l'information (IM) du bureau.
- ☐ Faites circuler le projet de diagnostic parmi les membres de l'ICCG/ISCG et de l'IMWG pour commentaires.
- ☐ Consolidez les commentaires et finaliser le projet de diagnostic afin qu'il soit examiné et validé collectivement lors d'une réunion conjointe de l'ICCG/ISCG, de l'IMWG ou tout autre groupe de travail technique au besoin, tels que l'AWG ou l'AAWG.
- ☐ Partagez la version finale avec l'EHP et offrez de faire une présentation des principaux résultats et des recommandations connexes pour la responsabilité des données dans la réponse.
- ☐ Idéalement, partagez le diagnostic avec la cartographie de l'écosystème des données (voir ci-dessous).

Outil ou modèle à consulter:

Modèle pour Diagnostic de la Responsabilité des données de l'IASC

02



Créer et maintenir à jour une cartographie de l'écosystème de données au niveau du système

Objectif:

La cartographie de l'écosystème des données, au niveau du système, présente un résumé des activités de gestion des données dans le cadre d'une réponse humanitaire. Elle aide à identifier les lacunes et les duplications potentielles des données, facilite la collaboration et permet la priorisation et la prise de décision stratégique en matière de gestion responsable de données.

Rôle d'OCHA:

OCHA est responsable de soutenir le(s) mécanisme(s) de coordination pertinent(s) pour créer une cartographie de l'écosystème des données. Une fois finalisée, OCHA doit présenter la cartographie de l'écosystème des données à l'EHP pour référence. OCHA doit aussi soutenir les mises à jour/révisions de la cartographie de l'écosystème au fur et à mesure de l'évolution de la réponse.

Approche recommandée:

☐ Préparez un projet de cartographie de l'écosystème des données en utilisant le **modèle de la cartographie de l'écosystème des données**. Il est recommandé que l'équipe IM dirige cet exercice, tandis que l'équipe de Coordination fournira des contributions et commentaires au besoin.

☐ Faites circuler le projet de diagnostic parmi les membres de l'IMWG pour tout commentaire.

☐ Consolidez les commentaires et finaliser le projet de la cartographie de l'écosystème des données afin qu'il soit examiné et validé collectivement lors d'une réunion conjointe de l'ICCG/ISCG, de l'IMWG ou tout autre groupe de travail technique au besoin, tels que l'AWG ou l'AAWG.

☐ Partagez la cartographie de l'écosystème validée avec l'EHP pour référence. Facilitez les mises à jour périodiques de la cartographie de l'écosystème en fonction de l'évolution de la réponse.

Outil ou modèle à consulter

Modèle de la Cartographie de l'écosystème des données

03

Développer et maintenir un Protocole de partage des informations au niveau du système

Objectif:

Un Protocole de partage des informations (PPI) est le document principal qui détermine l'échange des données et informations dans le cadre d'une réponse humanitaire. Un PPI inclut une classification de la sensibilité des données et informations indiquant le degré de sensibilité et le protocole de divulgation relatifs aux principaux types de données.

Rôle d'OCHA:

OCHA est responsable de soutenir l'ICCG/ISCG dans la rédaction conjointe d'un PPI pour la réponse.

Approche recommandée:

☐ Présentez la possibilité d'élaborer un PPI au niveau du système dans le(s) forum(s) de coordination compétent(s) et décidez d'une approche et d'un calendrier pour cette tâche avec les membres.

☐ Développez un projet de protocole en utilisant le **Modèle d'un Protocole de partage des informations** de l'IASC et faites-le circuler parmi l'ICCG/ISCG, l'IMWG et d'autres groupes de travail thématiques ou techniques au besoin, par exemple l'AWG et l'AAWG.

☐ Présentez le PPI à l'EHP pour révision et approbation dès qu'il a été révisé par l'ICCG/ISCG.

☐ Tous les acteurs impliqués dans la gestion des données doivent être informés du PPI et de leurs obligations respectives. En fonction de la réponse, OCHA doit publier le PPI approuvée (par exemple sur ReliefWeb, HRInfo ou un autre site spécifique à la réponse).

Outil ou modèle à consulter:

Modèle de l'IASC de Protocole de partage des informations

04

Répertoriez les incidents liés aux données

Objectif:

Le suivi des incidents liés aux données et la communication à leur sujet favorisent l'apprentissage, soutiennent des approches coordonnées de la gestion des incidents liés aux données et contribuent à réduire le risque que des incidents se produisent.

Rôle d'OCHA:

OCHA est responsable d'établir et de maintenir un registre central d'incidents et de fournir des rapports périodiques à l'EHP.

Approche recommandée:

☐ Mettez en place un registre central qui répertorie les détails clés concernant la nature, la sévérité et les modalités de résolution de chaque incident. Le cas échéant, ce registre peut être combiné à d'autres processus et outils de suivi des incidents au niveau du système, par exemple les systèmes de suivi sur la sécurité et l'accès. Limitez l'accès au registre pour éviter toute divulgation inutile sur les incidents.

☐ Présentez le registre à l'ICCG/ISCG et à l'IMWG et assurez-vous que tous les acteurs concernés sont au courant du processus pour contribuer, y compris les groupes de travail thématiques ou techniques, le cas échéant, par exemple l'AWG et l'AAWG.

☐ Encouragez les contributions des clusters/secteurs au nom de leurs membres. Les organisations individuelles peuvent également fournir des contributions basées sur leur propre suivi de la gestion des incidents si ces contributions ne sont pas déjà couvertes par les contributions du groupe/secteur concerné.

☐ Préparez des rapports périodiques qui résument la nature, la gravité et les tactiques de résolution utilisées par les acteurs. Dans ces rapports, respectez la confidentialité et ne partagez pas les données sensibles.

Outil ou modèle à consulter:

Modèle de l'IASC de POS pour la gestion des incidents liés aux données

Modèle d'OCHA de POS pour la gestion des incidents liés aux données

05

Soutenir la coordination et la prise de décision quant aux actions collectives

Objectif:

La coordination et les actions collectives permettent à la communauté humanitaire de faire le suivi du progrès, et d'identifier les défis et opportunités pour améliorer la Responsabilité des données. Cette approche permet également de favoriser la redevabilité et l'investissement conjoint dans la mise en œuvre des actions recommandées pour la Responsabilité des données.

Rôle d'OCHA:

OCHA est responsable de fournir des mises à jour régulières à l'EHP. OCHA doit également encourager l'alignement entre les clusters/secteurs et entre les actions au niveau du système et des clusters/secteurs.

Approche recommandée:

☐ Informez régulièrement l'EHP des avancées en matière de la Responsabilité des données, en couvrant le progrès collectif, ainsi que les défis et opportunités quant à la Responsabilité des données dans un contexte donné.

☐ Assurez une approche commune en conseillant l'ICCG/ISCG, l'IMWG et d'autres groupes techniques de travail en amont des réunions de l'EHP, et selon les besoins, en coordonnant des actions de suivi.

☐ Intégrez la Responsabilité des données comme un sujet prioritaire dans les briefings de sécurité et autres présentations pertinentes dans la réponse.

Outil ou modèle à consulter:

Briefing Pack on Data Responsibility, OCHA's role and the IASC Operational Guidance

2-page high-level summary of the Guidelines for OCHA management

2-page high-level summary of the Guidelines for external use

3.2 LE RÔLE D'OCHA DANS LES ACTIONS POUR LA RESPONSABILITÉ DES DONNÉES AU NIVEAU DES CLUSTERS/SECTEURS

Faire progresser la Responsabilité des données au niveau des clusters/secteurs complétera les actions menées au niveau du système et au niveau des organisations. Les agences Lead et Co-Lead des clusters/secteurs sont responsables de s'assurer que les actions entreprises s'intègrent bien dans le cadre d'une réponse particulière, conformément aux Directives opérationnelles sur la Responsabilité des données dans l'action humanitaire. Les actions à ce niveau sont principalement conçues pour les clusters/secteurs au niveau national, mais les clusters régionaux (couvrant plusieurs pays) et les clusters sous-nationaux peuvent également mettre en œuvre ces actions dans certaines réponses et contextes.

OCHA n'a pas de rôle direct dans la réalisation des actions à ce niveau, mais doit sensibiliser aux actions pour la Responsabilité des données recommandées par l'IASC au niveau des clusters/secteurs. OCHA peut apporter son soutien aux agences Lead et Co-Lead des clusters/secteurs en consultant sur des questions techniques et en assurant la liaison avec les structures de coordination compétentes lorsque nécessaire. Cela comprend la prise en compte des actions au niveau du cluster/secteur pour la responsabilité des données dans le cadre du soutien à la gestion de l'information pour les clusters/secteurs.

OCHA peut également donner des conseils sur le développement de PPI spécifiques aux clusters/secteurs et d'autres actions à ce niveau. OCHA devrait faire le suivi de l'adoption et de la mise en œuvre des actions pour la Responsabilité des données à ce niveau et encourager l'alignement avec les actions au niveau du système dans la mesure du possible.

3.3 LA RESPONSABILITÉ DES DONNÉES DANS LES BUREAUX D'OCHA

Le respect de la Responsabilité des données au niveau de l'organisation dans un contexte d'intervention donné est essentiel pour assurer le succès des actions de Responsabilité des données au niveau du système et des clusters/secteurs. En raison de la portée de ce niveau dans les Directives opérationnelles de l'IASC sur la responsabilité des données dans l'action humanitaire, les actions recommandées pour la responsabilité des données se rapportent aux bureaux d'OCHA.[14] Certaines actions à ce niveau, telles que le développement d'une procédure opérationnelle standard pour la gestion des incidents liés aux données, seront également applicables aux divisions du siège d'OCHA dans leur gestion opérationnelle des données.

Il existe **sept actions** en particulier qui devraient être priorisées par le personnel d'OCHA à ce niveau.

01

Mener un diagnostic de la Responsabilité des données au niveau du bureau

Objectif:

Le diagnostic de la Responsabilité des données présente un aperçu des mesures en matière de Responsabilité des données en vigueur au sein d'un bureau d'OCHA et facilite la priorisation d'actions supplémentaires en matière de Responsabilité des données dans la réponse. Le diagnostic permet à OCHA de mieux comprendre la politique et la gouvernance, les outils et l'infrastructure, ainsi que les compétences et les capacités liées à la gestion des données dans une réponse. À son tour, cette compréhension facilite la priorisation des actions ultérieures en matière de responsabilité des données.

Approche recommandée:

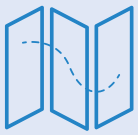
- ☐ Le diagnostic de la Responsabilité des données doit être mené conjointement par un staff Chargé des affaires humanitaires (HAO) et un staff Responsable de la gestion de l'information (IMO).
- ☐ Le modèle de diagnostic de la responsabilité des données d'OCHA permet de réaliser un diagnostic à ce niveau.
- ☐ Le diagnostic doit être mis à jour annuellement ou lorsque les circonstances et/ou les politiques et pratiques de gestion des données de l'OCHA changent.

Outil ou modèle à consulter:

OCHA Data Responsibility Diagnostic Template

[14] Data sharing between OCHA offices and/or with headquarters sections should be informed by the Guidelines and also follow the forthcoming administrative issuances on data protection and privacy for the UN Secretariat.

02



Créer un registre de ressources de données pour le bureau

Objectif:

Un registre de ressources de données présente une vue d'ensemble des données opérationnelles gérées par un bureau d'OCHA, favorise la gestion responsable des données au sein du bureau et alimente les cartographies au niveau des clusters/secteurs et du système.

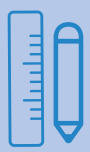
Approche recommandée:

- ☐ Le registre des ressources de données doit être créé et mis à jour par un Responsable de la gestion de l'information. Tout le personnel impliqué dans la gestion des données doit être au courant du registre et savoir comment le mettre à jour.
- ☐ Le registre doit au minimum inclure les noms de chaque jeu de données géré par le bureau, l'origine des données, une brève description, la méthode de collecte ou de réception, le lieu de stockage, l'accessibilité du jeu de données, la classification de la sensibilité, et le délai pour conservation et destruction.
- ☐ Le partage des données doit également être enregistré, soit dans le registre, soit dans un document distinct sur le partage des données. Les informations sur le partage des données doivent inclure, au minimum, le destinataire, la méthode de partage et la date du partage.
- ☐ Notez que les données peu ou pas sensibles doivent être conservées et rester accessibles au public par défaut.

Outil ou modèle à consulter:

OCHA Data Asset Registry Template

03



Définir les activités de gestion des données au sein du bureau pour mettre en oeuvre la Responsabilité des données

Objectif:

L'inclusion 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 minimiser les risques et de maximiser les avantages. Pour OCHA, les activités opérationnelles courantes de gestion des données comprennent, entre autres, les analyses de situation, les évaluations des besoins coordonnées, 3W/4W, la communication avec les populations affectées, le suivi de la situation de l'accès, et le suivi et l'évaluation de la réponse (y compris s'ils sont exécutés par des tiers). Ces activités comportent généralement les huit étapes suivantes : Planification, collecte, réception et stockage, assurance de la qualité, partage, analyse, présentation, conservation et destruction, et évaluation.

Approche recommandée:

- ☐ Lors de la conception d'une activité de gestion des données, le personnel responsable doit suivre les conseils relatifs aux huit étapes présentées dans le cycle figurant à la page 26 et reprises dans l'annexe C.
- ☐ Ces conseils et les résultats correspondants permettent au personnel d'identifier et d'atténuer les risques, de sélectionner les outils techniques appropriés, d'utiliser et de partager les données de manière sécurisée, éthique et efficace, et de respecter les directives et protocoles applicables au cours d'une activité de gestion des données.
- ☐ Contactez le Centre pour savoir comment adapter ces conseils à votre environnement de réponse et à une certaine activité de gestion des données.

[15] Cette action 'Assurer la disponibilité d'outils appropriés pour la gestion des données au sein du bureau' est incluse ici comme un complément aux actions pour la Responsabilité des données au niveau des organisations incluses dans les Directives opérationnelles de l'IASC sur la Responsabilité des données dans l'action humanitaire.

04

Etablir des accords de partage des données

Objectif:

Les accords de partage des données sont essentiels pour le respect des obligations juridiques, politiques, et normatives dans le cadre de la gestion des données opérationnelles. Ces obligations portent généralement sur le partage de données personnelles et, dans certains cas, de données sensibles non personnelles. Pour un bureau d'OCHA, ces données sont entre autres les résultats non traités des enquêtes, les listes de bénéficiaires ou les données détaillées sur les restrictions d'accès.

Approche recommandée:

- ☐ Établissez des accords de partage des données quand vous partagez des données personnelles ou des données sensibles non personnelles avec d'autres organisations.
- ☐ Les accords de partage de données doivent être élaborés conjointement par un staff Chargé des affaires humanitaires (HAO) et un staff Responsable de la gestion de l'information (IMO), et négociés avec le partenaire avec lequel les données sont partagées.
- ☐ Demandez toujours au Bureau exécutif (EO) d'OCHA d'examiner les accords de partage de données avant de les signer.

Outil ou modèle à consulter:

OCHA Data Sharing Agreement Template

05

Établir une procédure opérationnelle standard pour traiter les incidents liés aux données

Objectif:

Une procédure opérationnelle standard (POS) pour la gestion des incidents liés aux données permet de réduire le risque qu'un incident se reproduise et de soutenir le développement d'une base communes de connaissances.

Approche recommandée:

- ☐ La POS doit être établie conjointement par un HAO et un IMO et doit être validée par le chef du bureau (HoO).
- ☐ La POS doit inclure une procédure pour notifier, classifier, traiter et clôturer un incident. Elle doit aussi spécifier les moyens appropriés pour la correction et la réparation vis-à-vis des individus qui sont touchés par l'incident liés aux données, tels que déterminés par les publications administratives du Secrétariat de l'ONU à venir en matière de protection des données et de vie privée.
- ☐ Mettez en place un registre qui reflète les détails clés concernant la nature, la sévérité et la résolution de chaque incident.
- ☐ Les bureaux d'OCHA doivent partager leur expérience en matière de gestion et d'atténuation des incidents liés aux données avec d'autres acteurs, c.-à-d. au niveau des clusters/ secteurs et au niveau du système pour favoriser des approches plus coordonnées pour la gestion des incidents liés aux données.

Outil ou modèle à consulter:

IASC SOP for Data Incident Management Template

OCHA Data Incident Registry Template

06

Assurer la disponibilité d'outils appropriés pour la gestion des données au sein du bureau[15]

Objectif:

OCHA utilise un nombre d'outils et directives pour soutenir la gestion efficace des données (p.ex **IM Toolbox**). L'utilisation de l'outil approprié favorise la gestion sécurisée, éthique et efficace des données, et assure l'alignement sur les normes internes, y compris les **Policy Instruction on Technology Standards**.

Approche recommandée:

- ☐ Le personnel impliqué dans la gestion des données doit indiquer les outils dont ils ont besoin Le chef de l'IMB surveillera la mise en œuvre de la 'Policy Instruction on Technology Standards' et déléguera la gestion des normes spécifiques d'OCHA aux membres appropriés de l'IMB.
- ☐ Utilisez les outils approuvés par UN Office of Information and Communications Technology (OICT), et figurant des normes actuelles en matière de logiciels et de matériel informatique approuvés qui est tenue à jour ici: **OCHA IMB SharePoint page on Technology Standards**.
- ☐ Si un outil n'est pas approuvé et absolument nécessaire pour une activité de gestion des données donnée, suivez le processus décrit sur la page SharePoint de l'OCHA IMB sur les normes technologiques pour demander l'examen et l'approbation de l'outil.
- ☐ Confirmez l'utilisation d'outils spécifiques avec Digital Services Section de l'IMB si nécessaire.

Outil ou modèle à consulter:

OCHA IMB SharePoint page on Technology Standards

07

Soutenir la gestion des connaissances en matière de Responsabilité des données au sein du bureau[16]

Objectif:

Les documents générés dans le cadre des actions et des processus liés à la responsabilité des données doivent être conservés dans un répertoire central au sein du bureau. Cela comprend, entre autres, le diagnostic de responsabilité des données, les accords de partage des données, les procédures opérationnelles standard et les analyses de l'impact des données pour les différentes activités de gestion des données, ainsi que le registre des sources de données.

Approche recommandée:

- ☐ Tous les collègues impliqués dans la gestion des données doivent contribuer au répertoire central.
- ☐ Les procédures d'accueil du nouveau personnel dans le cadre de la réponse devraient inclure une référence aux documents du répertoire ainsi qu'un briefing sur la Responsabilité des données.
- ☐ Les bureaux sont également encouragés à partager ces documents avec le Centre afin de promouvoir l'apprentissage et la cohérence des pratiques au sein d'OCHA.

[15] Cette action 'Assurer la disponibilité d'outils appropriés pour la gestion des données au sein du bureau' est incluse ici comme un complément aux actions pour la Responsabilité des données au niveau des organisations incluses dans les Directives opérationnelles de l'IASC sur la Responsabilité des données dans l'action humanitaire.

[16] Cette action 'Soutenir la gestion des connaissances en matière de Responsabilité des données au sein du bureau' est incluse ici comme un complément aux actions pour la Responsabilité des données au niveau des organisations incluses dans les Directives opérationnelles de l'IASC sur la Responsabilité des données dans l'action humanitaire.

LA RESPONSABILITÉ DES DONNÉES DANS LE CYCLE DE GESTION DES DONNÉES D'OCHA

Planification

L'identification et la documentation des différents éléments (par exemple, les sources et les flux de données, les outils et les capacités, etc.) qui constituent l'activité de gestion des données, ainsi que l'évaluation de l'impact et la prise de mesures d'atténuation des risques.

Conseils

- Réalisez une analyse de l'impact des données (AID) pour l'activitéthe.
- Assurez la disponibilité de l'infrastructure appropriée.
- Mettez en place des procédures opérationnelles standard (POS).
- Prenez des précautions additionnelles pour des activités de gestion de données qui impliquent la gestion de données sensibles.

Résultats

- L'analyse de l'impact des données est réalisée.
- Un accord de partage des données, procédure opérationnelle standard et/ou termes de référence, qui inclut les délais de conservation et de destruction des données, est mis en place.

Collecte, Réception, et Stockage

La collecte, la réception et le stockage de données.

Conseils

- Confirmez le niveau de sensibilité des données en amont de leur collecte ou réception.
- Utilisez des outils et canaux sécurisés.
- Stockez les données de manière responsable.
- Prenez des précautions additionnelles pour des activités de gestion de données qui impliquent la gestion de données sensibles.

Résultats

- Les données requises pour l'activité de gestion des données sont disponibles.

Assurance qualité

Le nettoyage des données, et la documentation des limites et restrictions conformément aux POS et normes pertinentes.

Conseils

- Nettoyez les données à l'aide de méthodes et outils appropriés pour l'activité en question et conformément aux critères applicables.
- Documentez toutes les limites et restrictions.

Résultats

- Les jeux de données, y compris les métadonnées, sont prêts pour le partage et/ou l'analyse.

Partage

Le partage de données en privé avec des partenaires ou leur mise à disposition publique en accès libre.

Conseils

- Choisissez l'approche responsable pour le partage conformément au Protocole de partage ou toute autre orientation applicable.
- Mettez en place des accords de partage des données et des licences.
- Fournissez les métadonnées.
- Prenez des précautions additionnelles lors du partage de données sensibles.
- Enregistrez le partage des données dans le registre des ressources de données.

Résultats

- Les données sont partagées de manière responsable.
- Le partage de données est enregistré dans le registre des ressources de donnée.

Analyse

L'extraction d'informations nécessaires au développement de produits d'informations.

Conseils

- Assurer une documentation claire des méthodes utilisées.
- Empêchez l'exposition de données sensibles pendant l'analyse ou la visualisation.
- Prenez des précautions additionnelles si vous utilisez des méthodes d'analyse avancées.

Résultats

- Tableaux, graphiques ou cartes présentant des informations, accompagnés d'une documentation appropriée.

Présentation

L'intégration d'informations tirées des données dans des produits d'information et des sites web internes ou publics.

Conseils

- Incluez le contexte et les sources de données dans les produits publiés.
- Obtenez l'approbation appropriée avant la diffusion et choisissez une licence adéquate.

Résultats

- Des produits d'information publiés de manière responsable.

Conservation et destruction

Le maintien des données disponibles pour une utilisation future ou la suppression des données d'une manière qui rend leur récupération impossible.

Conseils

- Évaluez la valeur future potentielle des données.
- Balancez le risque et l'utilité des données.
- Choisissez le moyen approprié pour le stockage à long terme.
- Réévaluez régulièrement le niveau de sensibilité des données conservées.
- Assurez la destruction efficace des données.

Résultats

- Les jeux de données sont conservés de manière sécurisée.
- Les jeux de données sont effectivement détruits, et une documentation claire de cette étape et les jeux de données a été rédigée.

Évaluation des données

L'examen interne de l'activité de gestion des données ou un examen conjoint avec les partenaires, au besoin.

Conseils

- Incluez la Responsabilité des données dans les exercices d'évaluation de l'activité.
- Communiquez l'utilisation des données avec les acteurs concernés.
- Enregistrez tout incident lié aux données qui s'est produit tout au long de l'activité.

Résultats

- L'activité de gestion des données est finalisée, y compris la documentation connexe sur les incidents liés aux données.

4. REDEVABILITÉ

4 REDEVABILITÉ

Tout le personnel d'OCHA et le personnel auxiliaire (par exemple, les contractants, les partenaires de réserve et les détachés) qui sont autorisés à gérer les données et les ressources connexes à travers OCHA doivent suivre les Consignes. Bien qu'une adoption véritable des Consignes nécessite la participation de tout le personnel d'OCHA, la redevabilité concernant le respect des Consignes incombe aux cadres supérieurs au niveau du siège et des bureaux.

Le **chef de la Direction de la gestion de l'information (IMB) et le Lead de la fonction de gestion de l'information sont responsables de l'adoption des Consignes au sein d'OCHA**. Chaque année, **le chef de la Direction de la gestion de l'information (IMB) soumettra un rapport au Data Steward d'OCHA**[17] sur les progrès réalisés quant à l'adoption des Consignes, ainsi que sur les incidents liés aux données qui ont été signalés.

Le **Centre for Humanitarian Data d'OCHA** suivra et soutiendra l'adoption des Consignes, et apportera son soutien au chef de la Direction de la gestion de l'information (IMB) pour faire le point sur le progrès comme indiqué ci-dessus. Le Centre assurera la liaison avec **le(s) point(s) focal(aux) chargé(s) de la protection des données**, si nécessaire, pour mener à bien ces tâches. Le Centre fournira également des mises à jour régulières au **Data Responsibility Working Group**[18] concernant les progrès et les leçons apprises par OCHA dans la mise en œuvre des Consignes.

Au niveau global, tous les **Functional Leads, et les chefs des Directions ou Section** dont les équipes gèrent les données sont responsables de l'adoption des Consignes.

Au niveau du terrain, les, **Chefs de Bureau** sont responsables d'assurer le respect des Consignes au sein de leur bureau.

Les Chefs des Unités sont responsables de l'application appropriée des Consignes dans le travail de gestion des données quotidien d'OCHA.

Les Chargés des affaires humanitaires et **les Responsables de la gestion de l'information** sont responsables pour soutenir l'application des Consignes dans leur domaine respectif.

Le tableau ci-dessous résume les principales responsabilités des différents groupes/unités dans le soutien à l'adoption des Consignes.

[17] Les publications administratives à venir pour l'organisation en matière de protection des données et de vie privée énoncent un ensemble de *'Fonctions de protection des données'* dans les différentes entités onusiennes. Cela inclut un *Data Steward' (typiquement le chef de l'entité) et des Points focaux pour la Protection des données.*

[18] Le Data Responsibility Working Group (DRWG) est un groupe de coordination global qui a pour objectif de faire progresser la responsabilité des données dans le secteur humanitaire. Il rassemble une diversité de parties prenantes, notamment des entités des Nations unies (ONU), d'autres organisations internationales (OI), des organisations non gouvernementales (ONG) et autres acteurs engagés dans la coordination et la mise en œuvre de l'action humanitaire. Le DRWG a débuté en tant que sous-groupe du Comité permanent interorganisations (IASC) en 2020 et s'est transformé en groupe de travail au niveau du système au début de 2021. L'objectif principal du DRWG est de coordonner, soutenir et surveiller l'action collective sur la responsabilité des données, principalement par le biais des Directives opérationnelles de l'IASC sur la responsabilité des données dans l'action humanitaire. Pour en savoir plus sur le DRWG, cliquez ici : **https://reliefweb.int/topics/data-responsibility-working-group-drwg**.

RESPONSABILITÉS LIÉES À L'ADOPTION DES CONSIGNES D'OCHA SUR LA RESPONSABILITÉ DES DONNÉES

Groupe / Unité	Responsabilités
Chef de l'IMB and chef de la Fonction Gestion des Informations [Chief of IMB and head of IM Function]	• Fournissent un rapport annuel sur l'adoption des Consignes sur la responsabilité des données au Data Steward d'OCHA. • Évaluent l'efficacité de l'adoption des Consignes tous les deux ans.
Functional Leads, Directeurs and Chefs de Directions [Functional Leads, Directors and Branch Chiefs]	• Sensibilisent et familiarisent le personnel avec les Consignes. • Prennent des mesures correctives et mettent à disposition les ressources nécessaires à la gestion des incidents liés aux données.
Chefs de bureau et Chefs des Sections [Heads of Office and Section Chiefs]	• Encouragent la sensibilisation et la consultation des Consignes dans la gestion quotidienne des données. • Assurent la disponibilité des compétences et des ressources nécessaires à la Responsabilité des données. • Favorisent la Responsabilité des données au-delà d'OCHA dans leurs relations avec les partenaires.
Chefs des Unités [Unit Heads]	• Veillent à l'application appropriée des Consignes dans la gestion des données au quotidien. • Appuient la Responsabilité des données au-delà d'OCHA dans les relations avec les partenaires impliqués dans l'écosystème des données. • Soutiennent le chef de bureau ou le chef de section dans le rapportage systématique de tout incident lié aux données. • Signalent systématiquement tout incident lié aux données via le moyen approprié pour le suivi et le soutien.
Chargés des affaires humanitaires et Responsables de la gestion de l'information [Humanitarian Affairs Officers and Information Management Officers]	• Mettent en œuvre les actions pour la responsabilité des données au(x) niveau(x) pertinent(s) et dans le contexte de leurs domaines respectifs d'intervention (par exemple, l'accès, la coordination, la gestion de l'information, etc. • Appliquent l'action 'Définir les activités de gestion des données au sein du bureau de façon à mettre en œuvre la Responsabilité des données' dans la conception et la mise en œuvre des activités de gestion des données. • Signalent tout incident lié aux données conformément à la procédure appropriée.

OCHA Centre for Humanitarian Data	• Contribue et réagit au rapport annuel du 'Data Steward' qui est envoyé par le chef du IMB. • Conseille sur les meilleures approches pour mettre en œuvre les Consignes au sein d'OCHA. • Préconise l'utilisation des Consignes. • Conseille sur la gestion des incidents liés aux données. • Conseille sur les priorités en matière de formation et de développement des capacités liées à la responsabilité des données.

Consultez la section 5 pour plus d'informations sur les services proposés par le Centre pour soutenir l'adoption des Consignes.

5. SERVICES D'APPUI À L'ADOPTION DES CONSIGNES

5 SERVICES D'APPUI À L'ADOPTION DES CONSIGNES

Le Centre s'engage à apporter son soutien aux bureaux et sections d'OCHA pour l'adoption des Consignes. Le Centre peut fournir les services suivants sur demande.

- **Présentation d'introduction**
  Le Centre offre des webinaires d'introduction aux bureaux ou sections qui le souhaitent. Ce service vise à promouvoir une compréhension générale des Consignes et à répondre aux questions sur la manière dont le personnel peut entamer leur mise en œuvre dans leur contexte.

- **Diagnostic et exercice d'évaluation**
  La plupart des bureaux d'OCHA ont déjà mis en place un certain nombre d'actions et de résultats clés pour la responsabilité en matière de données (voir la section 3 des Lignes directrices). Un diagnostic et une évaluation du niveau de responsabilité des données dans un bureau donné aideront les collègues à déterminer les actions à privilégier dans leurs efforts pour adopter et faire respecter les Consignes. Le Centre est disponible pour mener cet exercice ou pour accompagner les équipes d'OCHA dans sa réalisation.

- **Services de conseil ad hoc**
  Les bureaux ou les sections peuvent contacter le Centre avec des questions spécifiques sur l'interprétation ou l'application des Consignes. Le Centre prendra note de ces questions et les conseils respectifs pour aussi encourager l'apprentissage entre différents bureaux.

- **Missions de soutien**
  Pour les contextes où un soutien plus approfondi est nécessaire, le Centre propose des missions de soutien. Ces missions visent à adapter et à adopter les Consignes, et à faciliter les discussions et des ateliers avec le personnel et les partenaires d'OCHA sur les questions liées à la responsabilité des données. Les missions permettent aussi de développer des protocoles spécifiques au contexte pour une gestion responsable des données.

- **Outils et modèles**
  Les Centre développe en continu des outils et modèles pour faciliter l'application des Consignes à des activités spécifiques.

- **Formations**
  Le Centre dispose d'une gamme de matériel de formation sur les compétences en matière de Responsabilité des données pour le personnel et les partenaires d'OCHA. Il offre également un soutien ciblé à la formation sur demande.

- **Publications sur des thématiques spécifiques liées à la Responsabilité des données**
  Le Centre collabore avec différentes équipes au sein d'OCHA pour rédiger des orientations plus spécifiques sur l'adoption de la Responsabilité des données dans différents domaines thématiques.

ANNEXE

ANNEXE A DÉFINITIONS

Accord de partage des données : Accord qui établit les modalités régissant le partage des données personnelles ou des données sensibles non personnelles. Il est utilisé surtout pour le partage de données entre deux parties et est typiquement établi au niveau national.[19]

Analyse de l'impact des données : Une analyse de l'impact des données (AID) est un terme générique pour une variété d'outils qui sont utilisés pour déterminer les conséquences positives et négatives d'une activité de gestion des données. Il s'agit notamment d'outils couramment utilisés - et parfois légalement requis - tels que les analyses de l'impact sur la protection des données et les analyses de l'impact sur la vie privée.[20]

Atténuation des risques : Application de mesures spécifiques visant à prévenir et/ou à minimiser la probabilité de risques potentiels liés au traitement des données et à empêcher les risques ou à en minimiser l'ampleur et la gravité.

Cartographie de l'écosystème de données : Sont considérés comme des sources de données l'ensemble de données ou d'informations, défini et géré en tant qu'une entité unique afin que cet ensemble puisse être compris, partagé, protégé et exploité efficacement.[22]

Registre des ressources de données : Une cartographie de l'écosystème des données fournit un résumé des principales activités de gestion des données, y compris l'échelle, la portée et les types de données traitées, les parties prenantes impliquées, les flux de données entre les différents acteurs, ainsi que les processus et les plateformes utilisés.[23]

Consentement : Le consentement est toute indication librement donnée, spécifique et informée d'un accord par la personne concernée pour le traitement de ses données personnelles.[22]

Contrôle de la divulgation statistique : Technique utilisée en statistique pour évaluer et réduire le risque qu'une personne ou une organisation soit ré-identifiée à partir des résultats d'une analyse de données d'enquête ou administratives, ou lors de la diffusion de microdonnées.[23]

Données : Représentation ré-interprétable de l'information, de manière formalisée qui convient à la communication, l'interprétation ou le traitement.[24]

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

[19] IASC, ***Directives opérationnelles sur la Responsabilité des données dans l'action humanitaire*** (2021).

[20] IASC, ***Directives opérationnelles sur la Responsabilité des données dans l'action humanitaire*** (2021).

[21] IASC, ***Directives opérationnelles sur la Responsabilité des données dans l'action humanitaire*** (2021).

[22] Publications administratives à venir pour l'organisation en matière de protection des données et de vie privée.

[23] The Centre for Humanitarian Data, **Guidance Note on Statistical Disclosure Control** (2019).

[24] UN, **Data Strategy of the Secretary-General for Action by Everyone, Everywhere with Insight, Impact and Integrity, 2020-22** (2020).

Données à caractère non personnel : Toute information ne se rapportant pas à une personne concernée. Les données non personnelles peuvent être classées en fonction de leur origine, à savoir : les données qui ne se rapportent jamais à une personne concernée, telles que les données sur le contexte dans lequel une réponse humanitaire est en cours, ainsi que les données sur les acteurs humanitaires et leurs activités ; ou les données qui étaient, à la base, des données à caractère personnel, mais qui ont été rendues anonymes ultérieurement, telles que les données sur les populations affectées par la situation humanitaire et leurs besoins, les risques et vulnérabilités auxquels elles sont exposées, et leurs capacités. Les données à caractère non personnel incluent les informations démographiquement identifiables (Demographically Identifiable Information, ou DII en anglais), à savoir les données qui permettent l'identification d'un groupe d'individus par des facteurs géographiques définis, tels que l'ethnicité, le sexe, l'âge, l'occupation, la religion ou la localisation.[25]

Données agrégées : Données accumulées obtenues en combinant des données au niveau individuel. Il s'agit de données qui sont (1) collectées à partir de plusieurs sources et/ou plusieurs mesures, variables ou individus et (2) compilées dans des résumés de données ou des rapports de synthèse, généralement à des fins de rapport public ou d'analyse statistique.[26]

Données primaires : Données qui ont été générées par le chercheur lui-même, à travers des enquêtes, entretiens, expériences, spécialement conçus pour comprendre et résoudre le problème de recherche en question.[27]

Données secondaires : Données recueillies à l'origine dans un but de recherche spécifique ou non (par exemple, un recensement national), et qui sont maintenant utilisées par d'autres chercheurs pour un objectif différent.[28]

Données sensibles : Les données classées comme sensibles en fonction de la probabilité et de la sévérité des risques qui sont susceptibles de résulter de leur divulgation dans un contexte particulier. Les données, qu'elles soient personnelles ou non, peuvent, toutes deux, être sensibles. Beaucoup d'organisations disposent de systèmes de classifications spécifiques quant à ce qui constitue des données sensibles, afin de faciliter les pratiques de gestion des données.[29] Pour le Secrétariat de l'ONU, le système de classification est défini dans ST/SGB/2007/6 sur la sécurité, la classification et la gestion de l'information,[30] et les publications administratives à venir pour l'organisation en matière de protection des données et de vie privée.

Gestion des données : Le cycle de gestion des données comprend les étapes suivantes: planification, collecte et réception, stockage, nettoyage, transfert, alayse, communication et diffusion, feedback et évaluation, et conservation et destruction.

Gestion de l'information : La collecte, le partage et l'utilisation des données et des informations, qui sont le fondement de la coordination, de la prise de décision et du plaidoyer.

[25] IASC, ***Directives opérationnelles sur la Responsabilité des données dans l'action humanitaire*** (2021).

[26] IASC, ***Directives opérationnelles sur la Responsabilité des données dans l'aaction humanitaire*** (2021).

[27] **Public Health Research Guide, Primary & Secondary Data Definitions**.

[28] IASC, ***Directives opérationnelles sur la Responsabilité des données dans l'action humanitaire*** (2021).

[29] The Centre for Humanitarian Data, **Glossary**.

[30] **UN ST/SGB/2007/6**.

Gestion opérationnelle des données : La conception des activités de gestion des données, incluant la collecte ou la réception de données, le stockage, le traitement, l'analyse, le partage, l'utilisation, la conservation et la destruction des données et des informations par des acteurs humanitaires. Ces activités font (pleinement) partie de l'action humanitaire, tout au long du cycle de planification et de réponse des clusters/secteurs et incluant de façon non exhaustive, les analyses de situation, les évaluations des besoins, la gestion des données démographiques, l'enregistrement et l'inscription des bénéficiaires aux programmes d'aide, la gestion des cas, la communication avec les populations affectées, suivi des activités de protection, et le suivi et l'évaluation des réponses.[31]

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 au contraire intentionnelle, avec des objectifs, illégaux ou autrement non autorisés, causant des dommages ou en ayant le potentiel.[32]

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.[33]

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.[34]

Nettoyage des données : Le processus de détection et de correction (ou de suppression) des données corrompues ou inexactes dans un jeu de données, un tableau ou une base de données. Il consiste à identifier les parties incomplètes, incorrectes, inexactes ou non pertinentes des données, puis à remplacer, modifier ou supprimer les données corrompues ou inutilisables.

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

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

Protection des données : L'application systématique d'un ensemble de mesures institutionnelles, techniques et physiques qui préservent le droit à la vie privée dans le cadre du traitement des données personnelles.[35]

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

[31] IASC, ***Directives opérationnelles sur la Responsabilité des données dans l'action humanitaire*** (2021).

[32] The Centre for Humanitarian Data, ***Note d'orientation: Contrôle de la divulgation des données statistiques*** (2019).

[33] The Centre for Humanitarian Data, ***Note d'orientation: Contrôle de la divulgation des données statistiques*** (2019).

[34] CICR, Manuel sur la protection des données dans l'action humanitaire (2020).

[35] Définition établie par UN Privacy Policy Group (2017).

Registre des ressources de données : Un registre des ressources de données fournit un résumé des principaux jeux de données générés et gérés par différents acteurs dans un contexte donné.[36]

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

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

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

Sécurité des données : Un ensemble de mesures physiques, technologiques et procédurales qui préservent la confidentialité, l'intégrité et la disponibilité des données et empêchent leur perte, destruction, altération, acquisition ou divulgation, accidentelle ou intentionnelle, illégale ou non autorisée.[37]

Sensibilité des données : Classification des données en fonction de la probabilité et de la sévérité des dommages potentiels qui peuvent se matérialiser du fait de leur exposition dans un contexte particulier.[38]

Sources de données : Sont considérés comme des sources de données l'ensemble de données ou d'informations, défini et géré en tant qu'une entité unique afin que cet ensemble puisse être compris, partagé, protégé et exploité efficacement.[39]

Traitement des données : Toute opération ou ensemble d'opérations effectuées sur des données ou des ensembles de données, par des moyens automatisés ou non, telles que la collecte, l'enregistrement, le stockage, l'adaptation ou la modification, le nettoyage, le classement, la récupération, l'utilisation, la diffusion, le transfert et la conservation ou la destruction.

Transfert de données : Le processus qui consiste à transférer des données ou à les rendre accessibles à un partenaire par n'importe quel moyen, tel que la copie papier, les moyens électroniques ou l'internet.

Vie privée : Nul ne sera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes illégales à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes.[40]

Violation des données : La perte, la destruction, l'altération, l'acquisition ou la divulgation d'informations à des fins accidentelles ou intentionnelles, illégales ou autrement non autorisées, qui compromettent la confidentialité, l'intégrité et/ou la disponibilité des informations.

[36] IASC, ***Directives opérationnelles sur la Responsabilité des données dans l'action humanitaire*** (2021).

[37] The Centre for Humanitarian Data, **Glossary**.

[38] The Centre for Humanitarian Data, **Glossary**.

[39] Adaptée de: **Information Asset Fact Sheet** (2017).

[40] UN General Assembly, **International Covenant on Civil and Political Rights** (1976).

ANNEXE B

PRINCIPES POUR LA RESPONSABILITÉ DES DONNÉES DANS L'ACTION HUMANITAIRE[41]

Redevabilité
Conformément aux règles pertinentes applicables, les organisations humanitaires ont une obligation de justifier et d'assumer la pleine responsabilité quant à leurs activités de gestion de données. Les organisations humanitaires sont redevables vis-à-vis des populations affectées par les crises, des structures de gouvernance internes, des partenaires humanitaires nationaux et internationaux, et, le cas échéant, vis-à-vis des gouvernements nationaux et des organismes de réglementation. Pour atteindre leurs engagements en matière de redevabilité, les organisations humanitaires doivent mettre en place toutes les mesures nécessaires pour respecter et suivre la bonne adhésion à ces Principes. Ceci inclut la mise en place de politiques et mécanismes appropriés, et la responsabilité d'assurer la disponibilité de compétences, ressources, et capacités adéquates, en termes de personnel, ressources et infrastructure.[42]

Confidentialité
Les organisations humanitaires doivent mettre en œuvre des garanties et des procédures organisationnelles appropriées pour préserver la confidentialité des données sensibles à tout moment. Les mesures doivent être conformes aux normes générales de confidentialité ainsi qu'aux normes spécifiques du secteur humanitaire[43] ou les présents Principes. La coordination et la collaboration doivent également viser à garantir la création de passerelles et liens adéquats entre les activités de gestion des données opérationnelles humanitaires et les processus et investissements en matière de données qui soutiennent le développement. La capacité locale et nationale doit être renforcée dans la mesure du possible, et ne doit, en aucun cas, être affaiblie.

Coordination et Collaboration
La gestion coordonnée et collaborative des données implique une inclusion véritable des partenaires humanitaires, des autorités nationales et locales, des populations affectées par les crises, et les autres parties prenantes dans les activités de gestion des données, le cas échéant et sans compromettre les principes humanitaires[44] or these Principles. Coordination and collaboration should also aim to ensure that appropriate connections are established between humanitarian operational data management activities and longer-term development-oriented data processes and data investments. Local and national capacity should be strengthened wherever possible, and not be undermined.

Sécurité des données
Les organisations humanitaires doivent mettre en place des mesures de protection, procédures et systèmes appropriés, tant au niveau organisationnel que technique, afin de prévenir, atténuer, signaler et répondre aux incidents de sécurité. Ces mesures doivent être suffisantes pour assurer la protection contre les attaques externes, ainsi que se prémunir, en interne, contre l'accès ou la manipulation non autorisés ou inappropriés; et contre la divulgation accidentelle, les dommages, les altérations, les pertes et les autres risques liés à la gestion des données.[45] Ces mesures doivent être ajustées en fonction de la sensibilité des données gérées, et mises à jour en fonction de l'évolution des meilleures pratiques en matière de sécurité des données, tant pour les données numériques que pour les données analogiques.

[41] These Principles were developed and endorsed as part of the IASC Operational Guidance on Data Responsibility. The text of the Principles is reproduced as endorsed, with minor additions in the form of references to OCHA-specific policies and guidance where relevant. These Principles should be interpreted in-line with forthcoming administrative issuances for the organization related to data protection and privacy.

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

[43] Le Manuel sur la protection des données dans l'action humanitaire du CICR (2020) et la politique de l'IASC sur la Protection dans l'action humanitaire (2016) donnent des conseils sur la confidentialité. Ces normes doivent être interprétées conformément aux politiques organisationnelles et orientations pertinentes, y compris les publications administratives à venir pour l'organisation en matière de protection des données et de vie privée.

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

[45] La sécurité des données est particulièrement importante lors du transfert et du partage des données.

Finalité, nécessité et proportionnalité
La gestion des données humanitaires et les activités associées doivent se définir sur la base d'une finalité précise. La conception des processus et des systèmes de gestion des données doit contribuer à améliorer les résultats des actions humanitaires, être cohérente avec les mandats associés et cohérente avec les droits et libertés concernés, en les considérant en balance avec soin quand cela s'avère nécessaire.[46] Conformément au concept de la minimisation des données, la gestion des données dans le cadre de l'action humanitaire doit être pertinente, limitée et proportionnée - en termes d'investissement requis ainsi qu'en termes de risque identifié - aux finalités déterminées.

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

Approche basée sur les droits humains
La gestion des données doit être conçue et mise en œuvre de façon à respecter, protéger et promouvoir les droits humains. Cela comprend les libertés fondamentales et les principes d'égalité et de non-discrimination tels que définis dans les cadres traitant des droits humains, et plus particulièrement le droit à la vie privée et d'autres droits liés aux données. Et aussi, les droits spécifiques en matière de protection des données promulgués dans la législation et dans d'autres règlements applicablesn.[47]

Approche inclusive et axée sur la personne
Les populations affectées doivent avoir la possibilité d'être incluses, représentées et légitimées dans l'exercice de leur autorité tout au long de la gestion des données, lorsque le contexte opérationnel le permet. Conformément aux engagements de ne laisser personne pour compte ('Leave No One Behind' en anglais), des efforts concrets doivent être entrepris pour encourager la participation et l'engagement des personnes qui ne sont pas bien représentées et qui peuvent être marginalisées lors des activités de gestion des données (en raison de l'âge, du sexe et d'autres facteurs de diversité tels que le handicap, l'origine ethnique, la religion, l'orientation sexuelle ou d'autres caractéristiques), ou qui sont d'une façon ou d'une autre rendues 'invisibles'. En matière de gestion des données, une approche inclusive et axée sur les personnes est particulièrement importante dans le développement de normes et de standards spécifiques au contexte.

Protection des données à caractère personnel
Les organisations humanitaires ont une obligation d'adhérer (i) aux lois nationales et régionales applicables en matière de protection des données,[48] ou (ii), à leurs propres politiques en matière de protection des données, si elles bénéficient de privilèges et d'immunités tels que les lois nationales et régionales ne sont pas applicables.[49] Ces lois et politiques contiennent la liste des bases légitimes pour le traitement des données personnelles, dont le consentement.[50]

[46] Cela signifie notamment que la gestion des données doit être pertinente, limitée et adéquate par rapport à la finalité de la gestion des données, ce qui, pour les données non personnelles dans un contexte sensible, doit être conforme aux publications administratives à venir pour l'organisation en matière de protection des données et de vie privée.

[47] En tant que membre du Secrétariat des Nations Unies, l'OCHA bénéficie de privilèges et d'immunités qui entraînent l'inapplication des législations nationales et régionales relatives au traitement des données.

[48] En tant que membre du Secrétariat des Nations Unies, l'OCHA bénéficie de privilèges et d'immunités qui entraînent l'inapplication des législations nationales et régionales relatives au traitement des données.

[49] OCHA doit toujours gérer les données personnelles conformément aux directives applicables, y compris les publications administratives à venir pour l'organisation en matière de protection des données et de vie privée et 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.

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

Lors de la conception des systèmes de gestion des données, les organisations humanitaires doivent respecter les normes de confidentialité et de protection des données dès la conception et par défaut. Les organisations humanitaires doivent également tenir compte de la protection des données personnelles quand elles développent des cadres basés sur des données ouvertes (‘open data’). Conformément à leur engagement en faveur de l'inclusion et du respect des droits humains, elles doivent garantir les droits des personnes concernées à être informées du traitement de leurs données personnelles, et à pouvoir accéder, corriger, supprimer ou s'opposer au traitement de leurs données personnelles.

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

Conservation et destruction
La conservation des données sensibles doit être limitée au temps nécessaire pour atteindre les finalités pour lesquelles elles sont gérées, ou bien, à défaut, limitée à la durée de conservation qui est stipulée par la loi applicable ou les règles d'audit des donateurs. Lorsque leur conservation est nécessaire, un stockage sécurisé et sûr doit être garanti pour éviter que les données sensibles ne soient mal utilisées ou exposées de manière irresponsable. Toutes les autres données peuvent être conservées indéfiniment, à condition que leur niveau de sensibilité soit réévalué à des moments appropriés, que des droits d'accès puissent être définis et mis en oeuvre et - pour les données anonymisées ou agrégées - qu'une évaluation de réidentification soit effectuée. Quel que soit le niveau de sensibilité, un calendrier de conservation doit indiquer quand les données doivent être détruites et comment les détruire de manière à rendre leur récupération impossible. Des durées spécifiques de conservation doivent être définies dans la mesure du possible et, lorsque ce n'est pas le cas, l’examen quant à la nécessité de conserver les données d’une période spécifique doit être déterminé.

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

ANNEXE C

LA RESPONSABILITÉ DES DONNÉES DANS LE CYCLE DE GESTION DES DONNÉES D'OCHA

Le tableau ci-dessous résume les conseils et résultats en matière de Responsabilité des données pour les étapes du cycle de gestion des données qui figure sur la page 26. Des outils pour favoriser la gestion responsable des données lors des différentes étapes du cycle figurent dans la page SharePoint d'OCHA IMB des 'Technology Standards'.

CONSEILS POUR METTRE EN OEUVRE LA RESPONSABILITÉ DES DONNÉES LORS DU CYCLE DE GESTION DES DONNÉES ET RÉSULTATS

Étapes du cycle de gestion des données	Conseils et résultats pour la Responsabilité des données
1. Planification L'identification et la documentation des différents éléments (par exemple, les sources et les flux de données, les outils et les capacités, etc.) qui constituent l'activité de gestion des données, ainsi que l'évaluation de l'impact et la prise de mesures d'atténuation des risques.	**Conseils** ☐ Réalisez une analyse de l'impact des données (AID) pour l'activité. ☐ Assurez la disponibilité de l'infrastructure appropriée. ☐ Mettez en place des procédures opérationnelles standard (POS). ☐ Prenez des précautions additionnelles pour des activités de gestion de données qui impliquent la gestion de données sensibles. **Résultats** ☐ L'analyse de l'impact des données est réalisée. ☐ Un accord de partage des données, procédure opérationnelle standard et/ou termes de référence, qui inclut les délais de conservation et de destruction des données, est mis en place.
2. Collecte, Réception, et Stockage La collecte, la réception et le stockage de données.	**Conseils** ☐ Confirmez le niveau de sensibilité des données en amont de leur collecte ou réception. ☐ Utilisez des outils et canaux sécurisés. ☐ Stockez les données de manière responsable. ☐ Prenez des précautions additionnelles pour des activités de gestion de données qui impliquent la gestion de données sensibles. **Résultats** ☐ Les données requises pour l'activité de gestion des données sont disponibles.
3. Assurance qualité Le nettoyage des données, et la documentation des limites et restrictions conformément aux POS et normes pertinentes.	**Conseils** ☐ Nettoyez les données à l'aide de méthodes et outils appropriés pour l'activité en question et conformément aux critères applicables. ☐ Documentez toutes les limites et restrictions. **Résultats** ☐ Les jeux de données, y compris les métadonnées, sont prêts pour le partage et/ou l'analyse.
4. Partage Le partage de données en privé avec des partenaires ou leur mise à disposition publique en accès libre.	**Conseils** ☐ Choisissez l'approche responsable pour le partage conformément au Protocole de partage ou toute autre orientation applicable. ☐ Mettez en place des accords de partage des données et des licences. ☐ Fournissez les métadonnées. ☐ Prenez des précautions additionnelles lors du partage de données sensibles. ☐ Enregistrez le partage des données dans le registre des ressources de données. **Résultats** ☐ Les données sont partagées de manière responsable.

5. Analyse

L'extraction d'informations nécessaires au développement de produits d'information.

Conseils

- ☐ Assurer une documentation claire des méthodes utilisées.
- ☐ Empêchez l'exposition de données sensibles pendant l'analyse ou la visualisation.
- ☐ Prenez des précautions additionnelles si vous utilisez des méthodes d'analyse avancées.

Résultats

- ☐ Tableaux, graphiques ou cartes présentant des informations, accompagnés d'une documentation appropriée.

6. Présentatio

L'intégration d'informations tirées des données dans des produits d'information et des sites web internes ou publics.

Conseils

- ☐ Incluez le contexte et les sources de données dans les produits publiés.
- ☐ Obtenez l'approbation appropriée avant la diffusion et choisissez une licence adéquate.

Résultats

- ☐ Des produits d'information publiés de manière responsable.

7. RETAINING AND DESTROYING

Le maintien des données disponibles pour une utilisation future ou la suppression des données d'une manière qui rend leur récupération impossible.

Conseils

- ☐ Évaluez la valeur future potentielle des données.
- ☐ Balancez le risque et l'utilité des données.
- ☐ Choisissez le moyen approprié pour le stockage à long terme.
- ☐ Réévaluez régulièrement le niveau de sensibilité des données conservées.
- ☐ Assurez la destruction efficace des données.

Résultats

- ☐ Les jeux de données sont conservés de manière sécurisée.
- ☐ Les jeux de données sont effectivement détruits, et une documentation claire de cette étape et les jeux de données a été rédigée.

8. Évaluation des données

L'examen interne de l'activité de gestion des données ou un examen conjoint avec les partenaires, au besoin.

Conseils

- ☐ Incluez la Responsabilité des données dans les exercices d'évaluation de l'activité.
- ☐ Communiquez l'utilisation des données avec les acteurs concernés.
- ☐ Enregistrez tout incident lié aux données qui s'est produit tout au long de l'activité.

Résultats

- ☐ L'activité de gestion des données est finalisée, y compris la documentation connexe sur les incidents liés aux données.

ANNEXE D

MODÈLES POUR LA RESPONSABILITÉ DES DONNÉES

Les modèles suivants ont été conçus pour soutenir l'adoption des Consignes d'OCHA sur la Responsabilité des données. Certains modèles sont spécifiques à OCHA, d'autres sont tirés des Directives opérationnelles de l'IASC sur la Responsabilité des données dans l'action humanitaire.

Modèles des Directives opérationnelles de l'IASC

- Diagnostic de la Responsabilité des données (au niveau du système)
- Cartographie de l'écosystème des données et Registre des ressources des données
- Protocole de partage des données (including Information and Data Sensitivity Classification)
- Procédure opérationnelle standard pour la gestion des incidents liés aux données

Modèles spécifiques à OCHA (en anglais)

- Data Responsibility Diagnostic (Office Level)
- Data Impact Assessment
- Data Asset Registry
- Data Sharing Agreement
- Data Incident Registry

ANNEXE E

FONDEMENT DE LA RESPONSABILITÉ DES DONNÉES AU SEIN D'OCHA

La gestion des données au sein d'OCHA est encadrée directement et indirectement par une variété d'instruments. Les Consignes complètent et s'inspirent des documents existants énumérés ici.

[NB: Ces ressources sont issues de la version anglaise]

Cadre juridique

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

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

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

Directives existantes du Secrétariat de l'ONU

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

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

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

UN Office of Information Communication Technology (OICT). Technical Guidance on Information Security: https://iseek-external.un.org/department/policies.

UN Office for the Coordination of Humanitarian Affairs (OCHA), Policy Instruction on Technology Standards, https://unitednations.sharepoint.com/sites/OCHAHub/IMB%20Resources/Forms/AllItems.aspx?id=%2Fsites%2FOCHAHub%2FIMB%20Resources%2FShared%20Documents%2FOCHA%20Policy%20Instruction%20on%20Technology%20Standards%20%2D%20September%2-02021%2Epdf&parent=%2Fsites%2FOCHAHub%2FIMB%20Resources%2FShared%20Documents.

UN Secretariat, 2004. Secretary-General's Bulletin on the Use of Information and Communications Technology Resources and Data, ST/SGB/2004/15: https://undocs.org/pdf?symbol=en/st/sgb/2004/15.

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

UN Secretariat, 2010. UN Information Sensitivity Toolkit: http://dag.un.org/handle/11176/387401.

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

Directives du Inter-Agency Standing Committee (IASC)

Inter-Agency Standing Committee (IASC), 2021. Operational Guidance on Data Responsibility in Humanitarian Action: https://interagencystandingcommittee.org/system/files/2021-02/IASC%20Operational%20Guidance%20on%20Data%20Responsibility%20in%20Humanitarian%20Action-%20February%202021.pdf.

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

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.

ANNEXE F RESSOURCES ADDITIONNELLES

[NB: Ces ressources sont issues de la version anglaise]

Orientations spécifiques au secteur humanitaire

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

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

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

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

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

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

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

European Union, 2018. General Data Protection Regulation (GDPR): https://eur-lex.europa.eu/eli/reg/2016/679/oj.

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

Grand Bargain Working Group on Workstream 5, co-convened by ECHO and OCHA, 2019: https://interagencystandingcommittee.org/grand-bargain-official-website/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.

ICRC-led Advisory Group incl. DRC on "Professional Standards", 2018. Professional Standards for Protection Work; Chapter 6: Managing Data and Information for Protection Outcomes: https://reliefweb.int/sites/reliefweb.int/files/resources/0999_002_Protection_web.pdf.

International Conference on Data Protection and Privacy Commissioners, 2009. Madrid Resolution: International Standards on the Protection of Personal Data and Privacy: https://edps.europa.eu/sites/edp/files/publication/09-11-05_madrid_int_standards_en.pdf.

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

International Organization for Migration (IOM), 2018. DTM & Partners Toolkit: Do No Harm Checklist and Guiding Questions for DTM and Partners: Do_No_Harm_ChecklistandGuidingQuestionsforDTMandPartners.docx.

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.alnap.org/help-library/irc-research-toolkit-obtaining-meaningful-informed-consent.

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

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

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

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

Oxfam, 2017. Responsible Data Management Training Pack: https://policy-practice.oxfam.org/resources/responsible-data-management-training-pack-620235/.

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

Protection Information Management (PIM) Initiative, 2015. PIM Principles: http://pim.guide/guidance-andproducts/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/blogs/data-protection-starter-kit-introduction-pack.

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.

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

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

Orientations additionnelles de l'ONU

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

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

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

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

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

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

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

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

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

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

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

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