Cluster Protection
Burkina Faso

PROTOCOLE DE PARTAGE DES INFORMATIONS SUR LA PROTECTION ENTRE LES ORGANISMES CHARGÉS DE LA COLLECTE ET GESTION DES DONNÉES DE PROTECTION AU BURKINA FASO

MOTIVATION

Dans le cadre de la manipulation des données et informations, il s'avère important d'assurer la confidentialité dont le Cluster protection s'attèle à accompagner. La forme des données et informations est variable ; alors elles peuvent être quantitatives ou qualitatives puis désagrégées ou anonymes (codées). D'où leur manipulation s'avère délicate et sensible en protection mais pas toutes. Pour ce faire, les clusters, en général, et le Cluster protection, en particulier, ont une responsabilité concernant le partage efficace de données.[1] Ainsi donc dans le respect des principes humanitaires et de gestion de cas. La raison d'être de cette responsabilité est éviter d'exposer les populations affectées à d'avantage de préjudices, pouvant découler de nos activités.[2]

L'obtention et le partage des données relatives aux risques de protection contre les personnes affectées par le déplacement forcé sont importants pour assurer la bonne gestion des cas de protection. Cela facilitera la coordination, la synergie d'actions humanitaires et la réduction des couts de prise en charge à travers le partage et l'utilisation des données émanant des acteurs humanitaires, des autorités et des directions de l'action humanitaire.

OBJET

Ce protocole de diffusion des informations et des données a pour but d'établir les principes directeurs et de présenter les procédures à suivre pour transmettre des données anonymes consolidées, données statistiques, les matrices et les analyses sur les cas déclarés liés aux incidents de protection et vulnérabilités entre le Conseil National de Secours d'Urgence et de Réhabilitation (CONASUR), les Directions Régionales de la Femme, de la Solidarité Nationale, de la Famille et de l'Action Humanitaire (DRFSNFAH), des structures sanitaires des zones affectées, les acteurs humanitaires, les clusters, groupes de travail et autres partenaires dans le cadre des efforts de prévention et d'intervention face aux incidents de protection au Burkina Faso. L'information est capitale à la réponse humanitaire mais ne doit constituée une source de nuisance aux bénéficiaires, aux structures ni à l'Etat. Il n'est

[1] Voir IASC guidance on information management.
[2] Voir Politique du Comité permanent inter institutions sur la protection dans le cadre de l'action humanitaire, para. 3.1.

pas nécessaire de rechercher la primeur ni la paternité ou le monopole des données au risque de refus de collaboration et de partage.

Les organismes qui recueillent des données reconnaissent que la diffusion et la réception des informations et des données consolidées sur les incidents de protection contribuent à :

- Remplissage des matrices ou autres tableaux ;
- Organiser des conférences ou études de cas ;
- Assister les bénéficiaires avec l'appui de la structure gestionnaire du cas ;
- Faciliter l'analyse des besoins ;
- Identifier les besoins prioritaires et non couverts ;
- Analyser les tendances ;
- Améliorer la coordination inter-organismes ;
- Détecter les failles ou problèmes non résolus ;
- Contribuer à la mobilisation des ressources ;
- Programmer des efforts de réponses aux problèmes de protection ;
- Informer l'opinion et les acteurs humanitaires ;
- Soutenir les efforts de prévention et de réponse, de plaidoyer ;
- Renforcer le suivi et la redevabilité ;
- Évaluer les services fournis ;
- Combler les lacunes et formuler des réajustements ;
- Harmoniser les approches (e.g. outils et procédés).

Au regard du réel besoin d'avoir des données et d'informations sur les personnes en détresse, toutes les structures et entités doivent bien les exploiter à travers un engagement qui garantisse leur confidentialité. Elles doivent s'assurer que les efforts de diffusion des informations ne causent aucun tort aux bénéficiaires, aux survivants, à leurs familles, ni à leur communauté (base du principe du Ne Pas Nuire).

Il faut noter que les informations collectées selon les objectifs et les modalités définies par le présent protocole ne remplacent pas d'autres systèmes de documentation des cas de protection utilisés par les acteurs de protection engagés dans la réponse aux cas de protection (tel que le GBVIMS[3] pour les cas de VBG, la documentation des ENA/ES et d'autres enfants à risque selon les modalités établies, le CP IMS relatif à la Protection de l'enfance, le Monitoring de protection, Mécanisme de Réponse Rapide/RRM &c). C'est un outil qui renforce l'existant et oriente aussi le partage d'informations avec/issues d'autres secteurs humanitaires du terrain et niveau national.

PRINCIPES DU PARTAGE

Principes de base

Le partage d'informations personnelles ne peut avoir lieu qu'avec le consentement éclairé de la personne concernée. Cependant les informations et données dites générales sont validées et autorisées par les structures les ayant générées. Toutefois le caractère commun demeure la confidentialité, la bonne utilisation et la conservation sécurisée (archivage). De plus les structures peuvent s'accorder du type, format et modalité de diffusion qui sont tributaires de la nature des données et informations disponibles ou souhaitées.

[3] GBVIMS : Gender Based Violence – Information Management System / Système de Gestion des Informations sur la Violence Basée sur le Genre.

Les informations partagées avec les acteurs humanitaires seront utilisées pour la mise en œuvre des activités de prise en charge et d'assistance. Elles doivent bien manipulées, gardées et exploitées par les demandeurs. Le respect des règles de partage déterminera la suite de la collaboration dans le partage.

Les informations partagées avec les clusters seront utilisées pour renseigner les outils de la coordination (Dashboard, 5W, Bimensuels, Bulletins, cartes, etc.) et consolidées en vue d'instruire la réponse et mener des plaidoyers.

Principes fondamentaux de partage d'informations

a) S'assurer que les données ne sont partagées et communiquées qu'aux membres du Cluster protection conformément à la conduite de leurs fonctions officielles sur la base du besoin de savoir.
b) S'assurer que les données partagées sont aussi précises que possible (chiffrées, désagrégées, comparaison, analyse, …) et, le cas échéant, les mettre à jour pour s'assurer qu'elles remplissent le(s) but(s) pour lequel elles sont traitées et partagées.
c) Prendre l'information ou la donnée à la bonne source (réduction de risque de déformation/distorsion).
d) S'assurer de la sécurité ou la protection des données sensibles et personnelles par les staffs et les structures.

Principes d'adhésion et de participation

a) Les participants du Cluster protection doivent s'efforcer de ne rapporter que des incidents confirmés qui ont des conséquences sur la protection, ou préciser que les informations partagées ne sont pas encore vérifiées.
b) La source d'information des questions de protection doit rester confidentielle, sauf indication contraire par la source.
c) Les principes énoncés ci-dessus sont obligatoires pour toutes les organisations du Cluster protection ainsi que pour les services étatiques et le Cluster protection peut réviser l'adhésion d'une organisation/agence au protocole si les principes qui sont énoncés ne sont pas respectés.

SECURITE ET PROTECTION DES DONNEES PARTAGEES

Pour assurer la confidentialité et l'intégrité des données, cet article décrit diverses mesures de sécurité des données techniques, managériales et organisationnelles qui doivent être mises en place par les différents acteurs concernés. Ces mesures aident à prévenir la perte, la mauvaise utilisation ou la modification des données reçues et la mauvaise destruction (copies dures). Pour ce faire, il est primordial de :

a) S'assurer que les données sont protégées en tout temps et gardées en sécurité. Cela peut être assuré en installant un logiciel anti-virus à jour pour éviter la corruption et la perte d'informations. Les sauvegardes de la ou des bases de données pertinentes et des informations importantes devraient être effectuées sur une base régulière sans échec et une copie de sauvegarde doit être stockée à distance. En plus, les données doivent toujours être transférées uniquement par l'utilisation de moyens de communication protégés et surs (avec un mot de passe, après un scanning anti-virus, etc.).

b) S'assurer que le(s) membres du Cluster protection n'enregistrent pas les données sur les ordinateurs personnels et que les données ne peuvent être partagées que par courrier électronique officiel.
c) S'assurer que le(s) membres du Cluster Protection désigné(s) est formé(s) sur le contenu de ce Protocole et d'autres documents pertinents de gestion et de partage de données, y compris sur la façon de gérer les informations confidentielles et sur les conséquences de la violation du Protocole ainsi que sur les principes de base de la protection des données personnelles et sensibles. Les agences sont tenues de mener des cours de recyclage trimestriels pour les membres du Cluster protection et de donner des orientations à tous les nouveaux membres afin de s'assurer qu'ils pratiquent les normes convenues.
d) Ne pas partager les informations sensibles concernant les survivant(es) et pouvant permettre de les identifier (e.g. nom, initiales, sous-comité, date de naissance, localité, etc.)
e) Les cas partagés par fiches physiques doivent être gardés dans un endroit sûr et sécurisé, en les classant selon les numéros de cas et en limitant leur accès et exploitation.

LIMITE TEMPORELLE ET GEOGRAPHIQUE

Une fois convenu et signé par un minimum de cinq (05) organisations/agences, ce protocole de partage de données et d'informations entrera en vigueur et sera à l'essai jusqu'au 31 décembre 2021, date à laquelle les organismes chargés de la collecte des données évalueront l'efficacité et l'utilisation du protocole, et leur adhésion à ce dernier.

Le présent protocole de partage d'informations et des données est valable pour tous les acteurs signataires intervenants dans toutes les régions affectées par la crise de déplacement forcé au Burkina Faso.

Le présent protocole bénéficie d'une tacite reconduction tant qu'il y aura des besoins humanitaires dans le pays et pourra être révisé à temps voulu.

L'adhésion à ce circuit conventionnel de réception et diffusion des données est libre et volontaire.

VIOLATIONS DES TERMES DU PROTOCOLE

En cas de violation, par toute partie, de toute disposition du présent protocole de diffusion des données et des informations, la diffusion des informations cessera jusqu'à la résolution du problème, les parties responsables devront rendre compte de leurs actes et le protocole de diffusion des informations sera révisé.

Le Cluster protection peut réviser l'adhésion d'une organisation/agence au protocole si les principes qui sont énoncés sont violés.

Le Cluster protection, le CONASUR/Directions AH et les autres acteurs peuvent également décider de ne plus partager d'informations avec l'organisation qui violerait la disposition convenue. Par conséquent, les organisations au niveau central (capitale) seront informées de l'existence dudit protocole. Toute chose qui sera relayée au niveau terrain et faciliter son application.

ANNEX 1: TYPOLOGIE DES INCIDENTS

Quel type d'incident s'est-il produit ?

1. Violation du droit à la vie et à l'intégrité physique
2. Violences sexuelles
3. Violation du droit à la liberté
4. Violation du droit à la justice
5. Violation du droit à la propriété
6. Violation des droits civiques ou politiques
7. Atteinte au droit à l'unité familiale
8. Atteinte au droit aux services publics et à l'assistance
9. Violation du droit à l'asile
10. Violations de la résolution 1612
11. Mouvements de population
12. Conflit inter communautaire

Quel incident s'est-il produit ?

Type 1

- Meurtre (sans préméditation)
- Assassinat (avec préméditation)
- Coups et blessures/agressions physique
- Torture et traitements inhumains
- Menaces
- Attaque par les hommes armés
- Blessures ou morts dû aux mines

Type 2

- Viol
- Agression sexuelle
- Exploitation sexuelle
- Esclavage sexuel
- Mariage forcé
- Mariage précoce
- Mutilation sexuelle
- Prostitution des enfants
- Prostitution forcée
- Attentat à la pudeur
- Stérilisation forcée

Type 3

- Enlèvement ou disparition forcé
- Recrutement forcé
- Travaux forcés
- Arrestation arbitraire
- Détention illégale (détenu hors du délai exigé par la loi)
- Détention dans des conditions inhumaines
- Déplacement forcé
- Retour forcé

- Relocalisation ou réinstallation forcée
- Limitations ou restrictions sur mouvement
- Refus du droit au retour
- Expulsions forcées

Type 4

- Entrave au droit à un jugement ou une réparation effective
- Perception illégale des frais de justice
- La corruption

Type 5

- Déguerpissement forcé
- Occupation illégale/spoliation des terres
- Destruction de propriété (y inclus incendie)
- Vol ou pillage
- Extorsion (y inclus prélèvement des biens) ou taxes illégales

Type 6

- Refus du droit à la liberté d'expression, de conscience ou de religion
- Refus du droit à la liberté d'association et de regroupement paisible
- Refus du droit de voter
- Refus de délivrance d'un acte de naissance
- Refus de délivrance de documents d'identité (carte d'identité, passeport)
- Refus arbitraire du droit à la nationalité

Type 7

- Séparation familiale

Type 8

- Entrave à l'accès humanitaire
- Entrave au droit à l'assistance humanitaire
- Entrave à l'accès aux services de la santé
- Entrave à l'accès à l'eau et l'assainissement
- Entrave à l'accès à l'éducation

Type 9

- Refus d'accès aux procédures d'asile
- Refoulement
- Fermeture de la frontière

Type 10

- Massacre ou mutilation d'enfants
- Recrutement ou utilisation d'enfants soldats
- Attaques dirigées contre des écoles ou des hôpitaux
- Viol d'enfants et autres actes graves de violence sexuelle à leur égard
- Enlèvement d'enfants
- Refus d'autoriser l'accès des organismes humanitaires aux enfants

ANNEXE 2: SIGNATURE DES ORSGANISATIONS ADHERANTES

Organisation :
Nom et Prénom du Représentant de l'agence / organisation :
Date et signature :

Organisation :
Nom et Prénom du Représentant de l'agence / organisation :
Date et signature :

Organisation :
Nom et Prénom du Représentant de l'agence / organisation :
Date et signature :

Organisation :
Nom et Prénom du Représentant de l'agence / organisation :
Date et signature :

Organisation :
Nom et Prénom du Représentant de l'agence / organisation :
Date et signature :

Organisation :
Nom et prénom du Représentant de l'agence / organisation :
Date et signature :

Organisation :
Nom et prénom du Représentant de l'agence / organisation :
Date et signature :

Organisation :
Nom et prénom du Représentant de l'agence / organisation
Date et signature

Organisation :
Nom et prénom du Représentant de l'agence / organisation
Date et signature :

Organisation :
Nom et prénom du Représentant de l'agence / organisation :
Date et signature :