Politique de Protection des données et de Gestion des Actifs Informatiques

SOMMAIRE

INTERSOS – Organisation Humanitaire Onlus
Via Aniene 26/a – 00198 Rome (RM)
P.IVA 12731101007 – C.F. 97091470589
Tel: +39 06 853 7431 – Fax: +39 06 853 74364
intersos.org – intersos@intersos.org

1. Politique de Protection des Données IT

La Politique de Protection des Données fait partie des politiques relatives aux données des bénéficiaires. Cette politique doit être associée aux politiques suivantes, déjà actives dans INTERSOS :

- Politique de Protection de l'Enfance (PE)
- Politique de Protection contre l'Exploitation et les Abus Sexuels (PEAS)
- Protocole de Protection des Données
- Autres politiques de Protection des Données adoptées au Siège et sur le terrain.

Les mêmes politiques sont à appliquer lorsque les données sont sur support rigide (document papier).

1.1 A quoi sert la protection des données

Les informations recueillies auprès des bénéficiaires étant sensibles, INTERSOS a développé cette politique afin de :

- Garantir une gestion cohérente, l'intégrité et la protection des données sensibles des bénéficiaires ;
- Respecter la vie privée et la confidentialité des bénéficiaires ;
- Élaborer et mettre en œuvre un protocole de sécurité et de mesures d'atténuation des risques liés au respect de la vie privée. Ce protocole concerne la collecte et le traitement des données personnelles des bénéficiaires ;
- Fournir des conseils pratiques pour le traitement, la sauvegarde et le transfert des données personnelles ainsi que pour le partage des données.

Lors de la collecte et du traitement des données de familles et de personnes vulnérables, des risques peuvent survenir tels que la perte, l'interception, le vol, la diffusion accidentelle ou malveillante ou la divulgation non autorisée, pouvant entraîner de graves préjudices pour les personnes concernées ainsi que pour INTERSOS et son personnel. Cette politique relève donc d'une importance capitale pour INTERSOS puisque sa fonction est de promouvoir le respect des principes de protection des données, conformément aux standards et lignes directrices globales. **Cette politique s'applique à toutes les données personnelles que détient INTERSOS, pour n'importe quel projet en cours. Le respect de cette politique est obligatoire pour l'ensemble du personnel d'INTERSOS.**

1.2 Définition des données personnelles

Toute information personnelle obtenue au cours des évaluations de programme de proximité ou de porte-à-porte, provenant de sources externes et/ou internes ou par tout autre moyen, est par définition classée comme étant confidentielle et sensible. Les données personnelles comprennent :

- les données biographiques, telles que la date de naissance, l'état civil, l'adresse, l'origine raciale ou ethnique etc ;

- les données biométriques, telles que la reconnaissance par l'iris, les empreintes digitales etc ;
- les circonstances matérielles, telles que l'opinion politique ou religieuse ou d'autres croyances, la sexualité de violation des droits de l'homme, l'expérience professionnelle etc ;
- archives d'images ;
- rapports externes, tels que des certificats médicaux, rapports de police, procédures pénales ou condamnations etc. ;
- documents personnels, tels que des dossiers de santé, des coordonnées bancaires etc ;
- documents de vérification, tels que des copies de passeports, des certificats du UNHCR etc ;
- toute autre information personnelle de quelque nature que ce soit.

Toutes ces informations doivent être traitées dans des conditions très strictes, comme spécifié dans les paragraphes suivants.

1.3 Lignes directrices pour la gestion des données personnelles

La confidentialité des données personnelles doit être respectée par l'ensemble du personnel d'INTERSOS. Seules les personnes autorisées à traiter les données peuvent y accéder. Les données personnelles doivent toujours être manipulées et traitées correctement, quelle que soit l'approche abordée, c'est-à-dire au cours de l'enregistrement ou la conservation des données ou lors de toute opération sur les données : organisation, adaptation, modification, publication par transmission, diffusion et synchronisation, regroupement, interdiction, effacement ou destruction.

Afin de garantir le respect de la confidentialité des données des bénéficiaires, toute information recueillie – formulaires d'évaluation, formulaires d'orientation, dossiers individuels, certificats externes etc. - doit être classée et conservée de manière à ce qu'elle ne soit accessible uniquement au personnel autorisé et transférée uniquement par des moyens de communication protégés conformément à la présente politique.

Tous les dossiers individuels, qu'ils bénéficient d'une assistance ou non, sont considérés comme des archives permanentes. Ils relèvent de la responsabilité d'INTERSOS et de ses missions, pour une durée définie par la mission, conformément aux règles d'INTERSOS et aux exigences des Donateurs en matière de Tenue des Dossiers concernant la Documentation Officielle des Projets (habituellement cinq (5) ans au moins à compter de la réalisation d'une action spécifique) selon le principe de GDPR (conservation des données personnelles), spécifiant que " les données sensibles et confidentielles ne doivent pas être conservées plus longtemps que nécessaire".

Enfin, toutes les dispositions des Donateurs, si elles sont plus strictes que celles d'INTERSOS, doivent être respectées.

1.4 Gestion des Informations sur la Protection (PIM)

PIM est un processus dirigé, systématisé et collaboratif utilisé pour collecter, traiter, analyser, conserver, partager et utiliser les données et les informations. Il permet d'entreprendre des démarches, fondées sur les preuves, en vue d'obtenir des résultats de qualité en matière de protection.

L'objectif de PIM est de fournir des données et des informations sûres et fiables sur les personnes déplacées. PIM favorise une utilisation efficace et ciblée des ressources et permet la coordination, la conception et la distribution de réponses en matière de protection.
Les principes PIM sous-tendent et caractérisent tous les systèmes PIM, quels que soient leurs objectifs, méthodes ou produits. Ci-dessous l'intégralité des informations sur PIM (voir également http://pim.guide/) :

- Axé sur l'humain et inclusif. Les activités liées aux données et aux informations doivent être guidées par les intérêts, le bien-être et les droits des populations affectées et des communautés d'accueil, qui doivent participer lors de toutes les phases importantes.
- Ne pas nuire. Les activités liées aux données et aux informations doivent comprendre une analyse du risque. Si nécessaire, des mesures doivent être prises afin d'atténuer les risques identifiés. L'analyse du risque doit examiner les conséquences négatives pouvant résulter de la collecte des données et des démarches ultérieures ou de la prestation de services.
- Objectif défini. Compte tenu du caractère sensible et souvent personnel des informations liées à la protection, les activités relatives aux données et aux informations doivent répondre à des besoins et des objectifs spécifiques. L'objectif doit : être clairement défini et communiqué ; être proportionnel aux risques et aux coûts identifiés par rapport à la réponse attendue ; viser des mesures en faveur de la protection telles que le partage et la coordination des données et des informations sur la protection.
- Consentement éclairé et confidentialité. Les informations personnelles doivent être recueillies après avoir obtenu le consentement éclairé de la (des) personne(s) en question, qui doit connaître le but de la collecte. Par ailleurs, la confidentialité doit être clairement expliquée à la personne avant de recueillir les informations.
- Responsabilité, protection et sécurité des données, La responsabilité des données va au-delà de l'aspect privé et de la protection des données. Il s'agit d'un ensemble de principes, d'objectifs et de processus visant à guider le travail humanitaire et à exploiter les données afin d'améliorer les conditions de vie des populations affectées et de leurs communautés d'accueil de manière responsable, tout en respectant les standards internationaux en matière de protection et de sécurité des données. Les activités liées aux données et aux informations doivent respecter les lois et les standards internationaux en matière de protection et de sécurité des données. Les personnes concernées ont le droit de voir leurs données protégées conformément aux standards internationaux relatifs à la protection des données.
- Compétences et capacités. Les personnes participant aux activités liées aux données et aux informations sont chargées de s'assurer que ces activités sont réalisées par les membres du personnel de gestion et de protection des informations, possédant les compétences essentielles en la matière et ayant été formés correctement.
- Impartialité. Toutes les étapes du cycle concernant les données et les informations doivent être entreprises de manière objective, impartiale et transparente, tout en identifiant et en minimisant les distorsions.
- Coordination et collaboration. Toutes les personnes qui mettent en œuvre les activités liées aux données et aux informations doivent respecter les principes mentionnés ci-dessus et promouvoir au maximum la collaboration et la coordination des données et des informations en interne, au sein des travailleurs humanitaires, et en externe, avec et parmi les autres intervenants. Dans la mesure du possible, les activités

liées aux données et aux informations doivent éviter de reproduire d'autres activités de données et d'informations et devraient au contraire s'appuyer sur les efforts et les mécanismes existants.

1.5 Objectif général des Outils IT pour la gestion des données personnelles

1.5.1 Collecte des données

Il existe principalement 3 outils pour la collecte des données :

- Formulaires Web (en ligne)
- Applis Mobile (hors ligne)
- tableur/traitement de texte Word (hors ligne)

Les formulaires web en ligne tels que Google Form sont utilisés pour la collecte d'informations à la fois avec un ordinateur portable et un mobile. Les données étant automatiquement enregistrées dans la base de données après soumission, il n'y a aucun risque de violation de la protection des données (aucune donnée n'est pas enregistrée directement dans l'appareil).

En revanche, les Applis Mobiles telles que Kobotoolbox, ODK Appli ou Fulcrum sauvegardent les données directement sur l'appareil car elles doivent fonctionner hors ligne. Dans ce cas, les règles suivantes doivent être respectées :

- Chaque dispositif utilisé pour la collecte des données doit être communiqué au siège afin d'appliquer la politique de sécurité (PIN/mot de passe) en connectant le dispositif au système MDM d'INTERSOS ;
- Chaque dispositif (Tablette ou smartphone) utilisé pour la collecte des données doit être protégé par un PIN ou un mot de passe ;
- Chaque application installée de collecte des données doit être configurée de manière à supprimer automatiquement les données après leur synchronisation avec la base de données principale. Si cela n'est pas possible (par exemple Fulcrum ne possède pas ce paramètre) les données recueillies doivent être supprimées manuellement ;
- Chaque dispositif doit être constamment mis à jour avec la version la plus récente.

Lorsque la collecte des données est effectuée à l'aide d'outils de bureau classiques tels que Spreadsheet (ex : MS Excel), word processor (ex : MS Word), bases de données locales (ex : MS Access), les fichiers doivent être protégés par un mot de passe. Lorsque le fichier est transféré par e-mail, le mot de passe doit être envoyé dans un second e-mail (séparé) ou via un autre moyen (ex : Skype).

1.5.2 Accès aux données et archives

On appelle "need-to-know" le principe majeur à appliquer lors de l'accès aux données archivées. Ce principe stipule que les données ne doivent pas être accessibles aux personnes qui n'en ont pas le besoin. Si les

données sont recueillies via des documents papiers, elles doivent être conservées dans un coffre-fort/caisson de rangement et ne doivent être accessibles qu'aux personnes qui en ont besoin (need-to-know).

Il existe 3 méthodes pour stocker les données et pour y accéder:

- Une base de données Cloud directement connectée aux formulaires Web (en ligne) ou aux Applis Mobiles
- Un espace de documents Cloud
- Un ordinateur portable personnel ou un serveur de stockage en réseau (Network Area Storage, NAS)

Les bases de données cloud (telles que Kobotoolbox, Fulcrum) sont des sites internet où l'on peut sauvegarder des données collectées par le biais d'applications mobiles. Elles n'ont généralement qu'un accès, celui de l'Administrateur. Le compte de l'administrateur doit être géré par la personne M&E (ou une fonction équivalente) et ne doit pas être partagé au sein du personnel opérationnel.
Remarque: Google form enregistre les données dans Google Drive (voir le paragraphe suivant)

Les **espaces de documents Cloud** (ex : Google Drive, Dropbox) sont des sites internet qui permettent de stocker les données dans des Dossiers/Fichiers (ex : MS Excel, Word, pdf etc). Une des caractéristiques principales est la possibilité de partager les données avec d'autres utilisateurs. Ainsi, les données ne doivent en aucun cas être partagées avec les personnes qui ne sont pas autorisées à y accéder. La personne M&E doit régulièrement vérifier le partage de statuts. Enfin, la personne M&E doit configurer le partage de permission enfin que le personnel opérationnel puisse partager les données avec quelqu'un d'autre.

Il est possible que les données soient conservées dans un **ordinateur portable ou un NAS**: cette méthode doit être évitée dans le mesure du possible. Il existe deux risques majeurs : la perte des données (par exemple, lorsque l'ordinateur portable est formaté en vue de l'utilisation d'une nouvelle personne) et un accès non-autorisé (en règle générale, les NAS ne sont pas protégés par un mot de passe). Si les données sont stockées dans un ordinateur personnel ou des NAS, le dispositif doit être protégé par un mot de passe.

1.5.3 Rapport et partage des données

Les Rapports doivent être regroupés. Tous les rapports doivent contenir les coordonnées des personnes concernées telles que le nom, le numéro de téléphone ou l'identification. S'il faut établir un rapport sur des personnes en particulier (comme dans les cas de recommandations), le Code Dossier doit être utilisé (ex CMAM1). Celui-ci correspond à un numéro de référence interne n'ayant aucun lien direct avec la personne en question.

Parfois, les donateurs exigent l'intégralité des informations des dossiers. Dans ce cas, les données doivent être envoyées en essayant de réduire autant que possible les destinataires mis en copie (Cc addresses), et le contenu doit être protégé par un mot de passe.

1.5.4 Objectifs spécifiques des Outils IT pour la gestion des données personnelles

Depuis 2017, INTERSOS met au point des plateformes web consacrées à la gestion des dossiers (utilisées en Liban et Irak), pour l'analyse des besoins (Jordanie, Cameroun, Nigeria et RCA) et pour les plaintes.
Toutes les plateformes sont mises au point avec la plateforme cloud Knack, garantissant disponibilité et sécurité. La connexion s'établit à l'aide d'une identification unique (single sign-on) et les utilisateurs sont répertoriés en fonction du principe du besoin de savoir (need-to-know). Ces plateformes garantissent un maximum de confidentialité par rapport à l'objectif principal des applis.

1.5.6 Restrictions

Après avoir consulté le Responsable Protection des données, et d'autres collègues au siège le cas échéant, INTERSOS peut refuser de fournir une réponse et peut limiter ou restreindre sa réponse à une demande ou une objection en vertu de laquelle :

- Il s'agirait d'une mesure nécessaire afin de sécuriser ou de garantir un ou plusieurs des éléments suivants :
    - La sûreté et la sécurité d'INTERSOS, de son personnel ou du personnel de partenaires opérationnels ; ou
    - Les besoins opérationnels dominants et les priorités d'INTERSOS dans l'exercice de son mandat.
- Il y aurait des raisons de croire que la demande est manifestement abusive, frauduleuse ou obstructionniste.

2. Politique de gestion des actifs IT

2.1 A quoi sert la gestion des actifs IT

La politique décrite ci-dessous porte sur l'utilisation responsable des ordinateurs et des systèmes d'information. Cette politique s'applique à l'utilisation d'internet, des e-mails et de tous les équipements des bureaux d'INTERSOS tels que les ordinateurs, ordinateurs portables, tablettes, smartphones, scanners, imprimantes, périphériques de stockage & projecteurs.
La politique et les lignes directrices décrites ici servent à prévenir les dépenses inutiles, les réparations, les défaillances de système des équipements d'INTERSOS et la violation de la Protection des données (voir le chapitre 1 de ce document). De plus, les mesures mentionnées ci-dessous visent également à prévenir une mauvaise utilisation des appareils qui pourrait entraîner un ralentissement de la connexion internet et du réseau ainsi que l'exposition à des virus et à des sites web, photos ou autres, inappropriés sur un lieu de travail. Le non-respect de cette politique peut entraîner des mesures disciplinaires (avertissements verbaux et écrits), la perte d'avantages, l'interdiction d'accéder à ces ressources et, lors des cas les plus graves, un renvoi immédiat.

- Les systèmes de technologie d'Information & Communication sont utilisés pour les besoins de la gestion d'INTERSOS. L'utilisation personnelle est à éviter autant que possible.
- L'accès à Internet de l'Organisation (World Wide Web) doit servir en priorité à des fins professionnelles. INTERSOS se réserve le droit d'accéder aux archives d'utilisation World Wide Web des employés et de les examiner.
- Les employés doivent contacter le Département IT du siège à Rome et obtenir son autorisation avant d'essayer de télécharger ou d'installer un logiciel à partir d'Internet/CD/DVD, à l'exception des mises à jour et des correctifs logiciels (patch) des logiciels standards d'INTERSOS (y compris les logiciels anti-virus).

Afin de garantir la sécurité des informations et la maintenance du réseau, le responsable IT, avec l'autorisation du Secrétaire Général, peut contrôler les appareils, les systèmes et le trafic du réseau à tout moment.

2.2 Principes de gestion des outils IT

2.2.1 E-mails et activités de communications

- INTERSOS a recours au système de communication par e-mail pour la gestion de ses activités. L'accès aux e-mails personnels doit être effectué dans la limite du raisonnable.
- Toute la correspondance par e-mail relative au travail d'INTERSOS doit se faire par le biais de la boîte mail prévue à cet effet.

- Il existe des risques lors de l'envoi ou de l'archivage de messages sur Internet et le Département IT ne peut pas empêcher les piratages ou les atteintes à la sécurité des courriers électroniques.
- Les e-mails envoyés doivent être rédigés de manière respectueuse et correcte. Toute forme de harcèlement via e-mail, par rapport au langage, à la fréquence ou à la taille des messages est interdite. Les politiques de l'organisation interdisant la discrimination et le harcèlement s'appliquent également aux courriers électroniques.
- Les employés ne sont pas autorisés à lire, intercepter, copier, utiliser ou divulguer des courriers électroniques destinés à d'autres personnes sans leur autorisation. Il est formellement interdit d'accéder à la boîte mail d'autres employés sans leur permission.
- Il est formellement interdit d'envoyer des numéros de carte de crédit ou des informations confidentielles similaires concernant des donateurs, grâce à des technologies non chiffrées pour l'utilisateur final, par e-mails et messageries instantanées (chat).
- Il est formellement interdit d'envoyer des messages à des fins commerciales autres que celles d'INTERSOS.

2.2.2 Internet

Les mises en garde et interdictions suivantes doivent être respectées, sans exception.

Il est interdit de :

- Accéder à des sites web et à des media jugés inappropriés ou offensants ;
- Télécharger, diffuser, transmettre, distribuer ou stocker du matériel à caractère obscène ou pornographique dans les appareils ou les systèmes d'INTERSOS. Cela comprend également le matériel à caractère diffamatoire, malveillant, menaçant (ou qui puisse causer toute sorte de tort), raciste, enfreignant les lois sur le contrôle des exportations, contenant des allusions ou des menaces sexuelles, des insultes raciales, ou tout autre commentaire offensant l'âge, le genre, l'orientation sexuelle, l'état civil, les croyances religieuses ou politiques, la nationalité ou le handicap d'une personne;
- Utiliser Internet pour des logiciels en ligne, « peer to peer », torrents, Internet Download Manager etc., qui monopolisent la bande passante d'Internet ;
- Introduire sciemment des programmes malveillants dans le réseau ou le serveur (ex : des vers informatiques, Cheval de Troie, mail bombing etc.)

2.2.3 Équipements et Systèmes ICT

Les mises en garde et les interdictions suivantes doivent être respectées, sans exception.

Il est interdit de :

- Essayer de réparer soi-même les équipements d'INTERSOS ou par l'intermédiaire d'un fournisseur non approuvé. Toutes les réparations et les opérations de maintenance doivent être effectuées par le Département IT ou par une Personne Focale IT ;
- Violer une licence de logiciel ou les copyrights, y compris la distribution de logiciels ;
- Installer des logiciels pirates ou tout logiciel inconnu du Département IT ;
- Utiliser les systèmes d'informations d'INTERSOS à des fins illégales ou non autorisées ou pour accéder à du matériel à caractère obscène ;
- Faire un usage personnel des systèmes d'informations ou des courriers électroniques pour des activités de conseil, d'affaires ou de travail en dehors du cadre d'INTERSOS, sans le consentement écrit du Siège.

2.2.4 Accès aux données

Tous les produits obtenus durant les heures de travail d'INTERSOS sont considérés comme appartenant à INTERSOS et doivent être disponibles à tout moment pour les responsables et la gestion. Cela comprend entre autre la correspondance, les recherches, les rapports, les données et les traductions. Si un employé s'absente pour cause de maladie, ou pour toute autre raison, ou s'il/elle refuse de fournir les informations demandées, l'accès aux informations peut être demandé au Département IT, ou à ses représentants, sur approbation du siège.