PROTECTION DES DONNEES ET ORGANISATIONS HUMANITAIRES CONTRE LES ME NACES NUMERIQUES (UNHCR) SOUS-DELEGATION DE BERTOUA

3ème FORUM NATIONAL SUR LA CYBERSECURITE ET LA LUTTE CONTRE LA CYBERCRIMINALITE

Communauté Urbaine de Bertoua, 11/12/2024

DATA PROTECTION

SECURISATION DES DONNEES DE PROTECTION

Le HCR, comme toute personne morale ou physique peut être victime de la cybercriminalité. Conscient de ce danger permanent et multiforme, le HCR a mis en place, et applique rigoureusement des procédures et mécanismes de sécurisation et d'intégrité de ses programmes et du personnel.

QUELQUES DEFINITIONS ET TYPES DE DONNEES PROTEGEES

- **Données à caractère personnel** désigne toute information relative à une personne identifiée ou identifiable. Elles comprennent par exemple les données biographiques et relationnelles, les photos, les données biométriques, les détails du contact, les constatations de fait concernant les demandes d'asile, les affiliations politiques, le service militaire, ainsi que les documents personnels et les expressions d'opinion (comme dans les évaluations médicales, les évaluations des besoins et d'autres notes pour le dossier).
- Une **personne concernée** désigne une personne physique dont les données personnelles font l'objet d'un traitement.

Nous nous attarderons pour les besoins de cet exposé sur 2 principaux types de données:

- Données numériques (données personnelles démographiques et biométriques) des personnes relevant de la compétence du HCR continues dans PRIMES, e-mails, dossiers d'assistance et de protection, …);
- Données physiques (A Qui De Droit, CIR, dossier physique de protection, …)

MESURES DE PROTECTION DE DONNEES

S’agissant des données numériques:

- Chaque utilisateur du HCR a un compte qui lui permet d’accéder à la base de données et aux différents dossiers de protection et d’assistance qui contient un identifient (user ID) accompagné d’un mot de passe accompagnés d’une authentification MFA;
- Enregistrement et mise a jour des données biométriques dans la base des données ProGres V4 avec un acces sélectif. (seuls les staffs autorisés ont accès a des modules spécifiques selon leurs postes et responsabilités)
- Données sont logées automatiquement sur le cloud (datacenter = structure hébergeant plusieurs serveurs et qui n’est accessible que par Internet).
- Formation du personnel, des réfugiés et des partenaires sur la cybercriminalité et sur la detection des différents types d’attaques et les actions à entreprendre selon chaque type.
- Toute modification dans la base des données ProGres V4 doit être autorisée par un staff dédié et est archivée.
- Système de gestion et audit des utilisateurs de toutes les différentes applications de l’organisation;
- Mise à jour des mots de passe robustes pour accéder à ses comptes de l’organisation tous les 3 mois;
- Les antivirus sur tous les postes d’utilisateurs;
- Les pares-feux (veille);
- Désactivation, suppression des programmes et fichiers des appareils à déclasser.

MESURES DE PROTECTION DE DONNEES

Pour ce qui est des données physiques, nous pouvons citer:

- Utlisation de formulaires sécurisés pour des documents délivrés par le HCR: Attestation de Composition Familiale, Carte d'identité de réfugié, Attestation Tenant Lieu d'Acte de Naissance etc …
- Ces documents produits sont remis directement au titulaire ;
- Existence de salle d'archivage avec accès filtré et sécurisé et les mesures de sécurité incendie ont été prises pour cette salle;
- Destruction des documents délivrés par le HCR au travers des déchiqueteuses (documents expires, documents avec erreurs d'impression, …).

Par ailleurs, en dehors des multiples sensibilisations auprès des pesonnes relevant de notre mandat sur la gratuité d'ABSOLUMENT TOUTES les prestations du HCR, nous collaborons avec les FMOs pour dénoncer et arrêter les cas de falsification des documents délivrés par l'organisation.

LES TECHNIQUES DE TRAITEMENT DES DONNEES DES REFUGIES POUR LA REINSTALLATION

La réinstallation repose sur le traitement des données à caractère personnel des réfugiés. Ces données personnelles sont collectées et traitées dans le but d'évaluer l'éligibilité et l'aptitude d'une personne à la réinstallation, et de faciliter le départ et l'accueil dans le pays de réinstallation. Le traitement des données à caractère personnel dans le cadre du processus de réinstallation comprend :

- Le traitement de données déjà:

  - i) collectées directement par le HCR (par exemple lors de l'enregistrement),

  - ii) reçues de partenaires (par exemple des informations sur la protection) ou

  - iii) générées par le HCR (par exemple les évaluations de la DSR).

- La collecte et la vérification des données par le biais d'un entretien de RST

- Le partage de données avec des tiers impliqués dans le processus de réinstallation (par exemple, le partage d'une demande de réinstallation auprès d'un pays de réinstallation).

- Collaboration et suivi des dossiers entre collègues ou partenaires du HCR, ou avec un pays de réinstallation.

PRINCIPES CLES DE LA PROTECTION DES DONNEES ET DE LA VIE PRIVEE DANS LE CADRE DE LA RST

La *Policy on the Protection of Personal Data (Politique générale sur la protection des données et de la vie privée)* (GDPP) identifie 9 principes clés de protection mais dans le cadre de la RST, nous en examinerons 7:

- **Le principe du traitement équitable et légitime: c**e principe exige que le HCR traite les données à caractère personnel de manière équitable et uniquement sur la base d'un ou de plusieurs des fondements légitimes énoncés au §18 de la GDPP.

- **Le principe de la spécification de l'objectif:** la spécification de l'objectif est le principe selon lequel les données à caractère personnel ne doivent être traitées qu'à des fins spécifiées compatibles avec le mandat et les fonctions du HCR. Cela signifie également que le traitement ultérieur doit être compatible avec le ou les objectifs premiers pour lesquelles les données ont été collectées à l'origine. Le §20 de la GDPP comprend une liste d'objectifs de traitement ultérieur qui sont toujours considérés comme compatibles avec le mandat du HCR, parmi lesquels : « lorsque [le traitement] est nécessaire pour assurer une protection et une assistance à long terme et pour rechercher des solutions… ».

- **Le principe de proportionnalité et de nécessité (minimisation des données):** ce principe est lié au principe de spécification de l'objectif et signifie que la quantité de données à caractère personnel collectées et partagées doit être adéquate, pertinente et limitée à ce qui est nécessaire au regard de la finalité identifiée, et ne pas dépasser cette finalité.

- **Le principe d'exactitude :** il exige que le HCR prenne toutes les mesures raisonnables pour s'assurer que les données à caractère personnel sont exactes et actualisées afin de répondre aux objectifs pour lesquels elles sont traitées. À cette fin, les agents doivent examiner, vérifier et mettre à jour les données à caractère personnel pendant toute la durée de traitement des dossiers.

PRINCIPES CLES DE LA PROTECTION DES DONNEES ET DE LA VIE PRIVEE DANS LE CADRE DE LA RST

- **Le principe de confidentialité** exige que le HCR traite les données à caractère personnel « en tenant dûment compte de la confidentialité, conformément aux règlements, règles, politiques, instructions administratives et autres instruments pertinents établis ou adoptés par le HCR ou les Nations Unies » (§25 de la GDPP). Il convient de noter en particulier l'article 1.2.i) du Statut et règlement du personnel de l'Organisation des Nations Unies, qui stipule que les membres du personnel « ne communiquent à aucun gouvernement, entité, personne ou autre source des informations dont ils ont connaissance du fait de leur position officielle et dont ils savent ou devraient savoir qu'elles n'ont pas été rendues publiques, sauf dans le cadre normal de leurs fonctions ou avec l'autorisation du Secrétaire général ». En outre, le principe 6 du Code de conduite du HCR explique que « la divulgation d'informations sensibles ou confidentielles sans autorisation peut gravement compromettre l'efficacité et la crédibilité du HCR et de son personnel et mettre en danger les personnes sous mandat ». Par ailleurs, lorsque des interprètes sont utilisés dans le cadre des entretiens de RST, ils sont tenus de signer auparavant des déclarations de confidentialité.

- **Le principe de sécurité** impose au HCR d'appliquer des garanties et des procédures organisationnelles, administratives, physiques et techniques adéquates pour assurer la sécurité des données à caractère personnel, notamment contre l'accès et le traitement non autorisés et contre la perte, l'altération, les dommages ou la destruction accidentels. Le respect de ce principe est une condition préalable pour garantir la confidentialité des données à caractère personnel.

- **Le principe de transparence:** Ce principe exige que le HCR traite les données à caractère personnel de manière transparente pour la personne concernée. Ce principe exige que le HCR traite les données à caractère personnel de manière transparente pour la personne concernée. Le principe de transparence permet aux personnes concernées de demander des comptes au HCR et d'exercer un contrôle sur leurs données personnelles. Garantir la plus grande transparence possible dans le traitement des données fait partie de la responsabilité du HCR envers les personnes affectées et doit être considéré comme faisant partie d'une approche de protection globale commençant par l'enregistrement initial et renforcée au fil du temps au cours des différentes interactions avec les personnes déplacées et les apatrides.

QUELQUES NORMES DU HCR EN MATIERE DE PROTECTION DES DONNEES ET DE LA VIE PRIVEE DANS LE CADRE DE LA RST

Les normes de protection des données et de la vie privée de la Partie 2 de la GDPP comprennent l'ensemble des **droits des personnes concernées** suivants à propos du traitement de leurs données à caractère personnel :

- le droit à l'**information** ;
- le droit à l'**accès** ;
- le droit de **rectification** ;
- le droit à l'**effacement** ; et
- le droit d'**opposition**.

Par ailleurs, il est important d'énoncer quelques points clés sur l'application des normes du HCR en matière de protection des données et de la vie privée dans le cadre de la réinstallation.

QUELQUES POINTS CLES SUR L'APPLICATION DES NORMES DU HCR EN MATIERE DE PROTECTION DES DONNEES ET DE LA VIE PRIVEE DANS LE CADRE DE LA RST

- Les données à caractère personnel ne peuvent être traitées qu'à des fins spécifiques compatibles avec le mandat et les fonctions du HCR.
- Le HCR doit informer les réfugiés des types de données à caractère personnel qui doivent être traitées au cours de la procédure de réinstallation, des personnes avec lesquelles leurs données seront partagées et des raisons de ce partage, et expliquer les droits de la personne concernée et la manière dont ils peuvent être exercés.
- Un Formulaire d'enregistrement en vue de la réinstallation ne doit pas contenir de données inutiles ou disproportionnées par rapport à la quantité d'informations requises par les autorités du pays d'accueil.
- Les POS de réinstallation doivent définir des processus garantissant le respect des droits de la personne concernée, notamment en ce qui concerne la réception et la réponse aux réclamations de la personne concernée.
- Les POS doivent tenir compte du fait que les demandes de correction des données à caractère personnel peuvent conduire à des incohérences ou à des allégations de fraude qui devront être traitées conformément à la politique du HCR en matière de lutte contre la fraude commise par des personnes relevant de sa compétence Politique de lutte contre la fraude commise par des personnes relevant de la compétence du HCR et aux lignes directrices opérationnelles correspondantes
- Lorsqu'il s'agit de communiquer sur des cas individuels, il est recommandé d'utiliser les sites SharePoint Team ou Secure File Sharing. Les courriels contenant des données personnelles doivent contenir des numéros proGres et non des noms. Les données personnelles ne doivent jamais figurer dans l'objet d'un courriel.
- Pour garantir la confidentialité, les données à caractère personnel doivent être stockées de manière à n'être accessibles qu'au personnel autorisé, selon le principe du besoin d'en connaître, et à n'être transmises que par des canaux de communication protégés.

BONNES PRATIQUES ET RECOMMANDATIONS

- L**'entretien de réinstallation** est l'une des principales opportunités pour le HCR d'informer les réfugiés de manière accessible sur le traitement de leurs données, sur leur droit à la protection à cet égard et sur la manière dont ils peuvent exercer leurs droits en tant que personnes concernées afin d'agir sur le traitement. La fourniture de ces informations fait partie de l'engagement du HCR à garantir la **redevabilité** à l'égard des populations touchées et constitue une exigence en vertu du cadre de protection des données personnelles et de la vie privée du HCR. Les bureaux doivent donc veiller à ce que les responsables de dossiers soient en mesure d'expliquer aux réfugiés **comment leurs données seront utilisées et partagées** tout au long du processus de réinstallation, conformément au cadre de protection des données personnelles et de la vie privée du HCR.

- Le HCR est souvent amené à partager des données personnelles avec des tiers, y compris, entre autres, des gouvernements, des agences des Nations Unies ou des organisations non gouvernementales. Le partage des données personnelles dans le cadre de la réinstallation se fait, par exemple, par le biais des dossiers de réinstallation soumis aux pays de réinstallation et du suivi de ces dossiers, y compris les mises à jour des données personnelles partagées, La partie 6 de la DPP (qui est plus détaillée que la GDPP quant aux conditions de partage des données à caractère personnel avec des tiers) stipule que, lorsque le partage de données à caractère personnel est susceptible d'être important, répété ou structurel, le HCR doit chercher à signer un accord de partage de données avant le partage, sauf s'il y a des raisons satisfaisantes de ne pas le faire. Ainsi, le HCR a engagé des discussions bilatérales avec plusieurs gouvernements de pays de réinstallation et d'autres entités afin de conclure des accords de partage de données (ASD), étant donné que le processus de réinstallation nécessite un partage régulier de données à caractère personnel.
- Il est important de ne pas partager les données sur les réseaux sociaux (Whatsapp, Messenger, …) mais plutôt utiliser les plateformes telles que Sharepoint,…
- Communiquer nécessairement sur les plateformes internes telles que Microsoft Teams;
- Eviter de laisser traîner des documents contenant les données à caractère personnel des réfugiés, laisser traîner des disques durs;
- Mener des entretiens confidentiels (à l'abri de tout regard extérieur).

Thank you

Questions?