POLITIQUE

relative à la protection des données des personnes relevant de la compétence du HCR

UNHCR
L'Agence des Nations Unies pour les réfugiés

POLITIQUE DE PROTECTION DES DONNÉES

TABLE DES MATIÈRES

1 DISPOSITIONS GÉNÉRALES 6

1.1 OBJET 7

1.2 RAISON D'ÊTRE 7

1.3 PORTÉE 8

1.4 TERMES ET DÉFINITIONS 9

2 PRINCIPES FONDAMENTAUX 14

2.1 PRINCIPES FONDAMENTAUX DU TRAITEMENT DES DONNÉES PERSONNELLES 15

2.2 TRAITEMENT LÉGITIME ET JUSTE 15

2.3 SPÉCIFICATION DES FINALITÉS 16

2.4 NÉCESSITÉ ET PROPORTIONNALITÉ 16

2.5 EXACTITUDE 16

2.6 RESPECT DES DROITS DE LA PERSONNE CONCERNÉE 16

2.7 CONFIDENTIALITÉ 17

2.8 SÉCURITÉ 17

2.9 RESPONSABILITÉS ET SUPERVISION 17

3 DROITS DE LA PERSONNE CONCERNÉE 18

3.1 INFORMATIONS 19

3.2 ACCÈS 20

3.3 CORRECTION ET EFFACEMENT 20

3.4 OPPOSITION 20

3.5 MODALITÉS DES DEMANDES 21

3.6 ENREGISTREMENT ET RÉPONSE DU HCR 21

3.7 LIMITATIONS 23

4 TRAITEMENT DES DONNÉES PAR LE HCR 24

4.1 CONFIDENTIALITÉ DES DONNÉES PERSONNELLES 25

4.2 SÉCURITÉ DES DONNÉES PERSONNELLES 25

4.3 GARANTIR L'EXACTITUDE DES DONNÉES PERSONNELLES 27

4.4 NOTIFICATION D'UNE VIOLATION DE DONNÉES PERSONNELLES 27

4.5 ANALYSE D'IMPACT RELATIVE À LA PROTECTION DES DONNÉES 28

4.6 CONSERVATION 29

5 TRAITEMENT DES DONNÉES EFFECTUÉ PAR DES PARTENAIRES D'EXÉCUTION 30

5.1 CONDITIONS GÉNÉRALES 31

5.2 VÉRIFICATION 31

5.3 ACCORDS DE PARTENARIAT 33

5.4 CAPACITÉS DU PARTENAIRE 33

5.5 CESSATION DU PARTENARIAT 33

6 TRANSFERT DE DONNÉES PERSONNELLES À DES TIERS 34

6.1 CONDITIONS GÉNÉRALES 35

6.2 ACCORDS RELATIFS AU TRANSFERT DES DONNÉES 36

6.3 TRANSFERT AUX ORGANISMES NATIONAUX CHARGÉS DE L'APPLICATION DE LA LOI ET AUX TRIBUNAUX NATIONAUX 36

6.4 ORGANISME INTERNATIONAL CHARGÉ DE L'APPLICATION DE LA LOI, COUR, TRIBUNAL OU AUTRE ORGANISME INTERNATIONAL.....39

6.5 PRIVILÈGES ET IMMUNITÉS.....39

7 RESPONSABILITÉS ET SUPERVISION.....40

7.1 STRUCTURE DES RESPONSABILITÉS ET DE LA SUPERVISION 41

7.2 LE RESPONSABLE DE TRAITEMENT ET LE POINT FOCAL DE LA PROTECTION DES DONNÉES 41

7.3 LE DÉLÉGUÉ À LA PROTECTION DES DONNÉES 43

7.4 BUREAU DE L'INSPECTEUR GÉNÉRAL.....44

7.5 BUREAU DE L'ETHIQUE.....44

1

DISPOSITIONS GÉNÉRALES

1.1 OBJET

La présente politique définit les règles et principes liés au traitement des données personnelles des personnes relevant de la compétence du HCR. Son objectif est de s'assurer que le HCR traite les données personnelles d'une façon qui est conforme aux *Principes directeurs pour la réglementation des fichiers personnels informatisés*[1] adoptés par l'Assemblée générale des Nations Unies en 1990 et à d'autres instruments internationaux relatifs à la protection des données personnelles et à la vie privée des individus. La politique sera complétée par des directives opérationnelles qui donneront des orientations sur sa mise en oeuvre, sa supervision et les responsabilités y afférentes.

1.2 RAISON D'ÊTRE

1.2.1 Dans le cadre de son mandat en matière de protection internationale et de solutions, et aussi en offrant ses bons offices aux États, le HCR est souvent tenu de traiter les données personnelles de personnes relevant de la compétence de l'organisation. Le HCR peut également avoir besoin de partager des données personnelles avec des partenaires d'exécution et/ou des tiers. Il existe des risques inhérents au traitement des données personnelles, comme par exemple la perte ou la divulgation accidentelle ou non autorisée. Compte tenu de la situation particulièrement vulnérable des personnes relevant de la compétence du HCR, la nature de leurs données personnelles est généralement sensible et exige, par conséquent, une gestion minutieuse, conforme à la présente politique. Pour le HCR, la protection adéquate des données personnelles des personnes relevant

1 Assemblée générale des Nations Unies, *Principes directeurs pour la réglementation des fichiers personnels informatisés*, adoptés par Résolution A/Res/45/95 du 14 décembre 1990, en ligne : http://www.un.org/fr/documents/view_doc.asp?symbol=A/RES/45/95.

de sa compétence est par conséquent particulièrement importante et l'Organisation a la responsabilité de les traiter d'une façon qui respecte les principes relatifs à la protection des données.[2]

1.2.2 La politique complète également les dispositions de l'article 1.2 (i) du Statut du personnel ainsi que les engagements du Code de conduite du HCR, et en particulier le Principe 6 relatif à l'obligation incombant au personnel de protéger et d'utiliser de façon responsable les informations auxquelles il a accès.

1.3 PORTÉE

1.3.1 La présente politique s'applique à toutes les données personnelles détenues par le HCR en relation avec des personnes relevant de la compétence du HCR.[3] Le traitement des autres données, par exemple agrégées ou rendues anonymes, n'entre pas dans le champ d'application de la présente politique, mais est couvert, entre autres, par la Politique de classement, de maniement et de divulgation de l'information du HCR.

1.3.2 La présente politique s'applique dans les cas où le traitement est effectué dans un bureau du HCR, par différents bureaux du HCR dans un ou plusieurs pays, ou lorsque les données sont transférées à des partenaires d'exécution ou à des tiers. La politique continuera à s'appliquer même après que les personnes cessent de relever de la compétence du HCR.

---

2 Le Comité exécutif du Programme du Haut-Commissaire a fait référence aux principes de la protection des données dans les Conclusions suivantes : No. 91 (LII) – 2001 (f), en ligne : http://www.unhcr.org/3bd3e1d44.html ; No. 93 (LIII) – 2002 (b) (viii), en ligne : http://www.unhcr.org/3dafdd344.html ; et No. 102 (LVI) – 2005 (v), en ligne : http://www.unhcr.org/43575ce3e.html.

3 HCR, Note relative au Mandat du Haut Commissaire et du Haut Commissariat pour les réfugiés, octobre 2013, en ligne : http://www.refworld.org/docid/5268c9474.html.

1.3.3 Le respect de la présente politique est obligatoire pour l'ensemble des membres du personnel du HCR.

1.4 TERMES ET DÉFINITIONS

Aux fins de la présente Politique, les définitions suivantes s'appliquent :

Consentement

Toute indication éclairée et librement consentie par la personne concernée d'un accord portant sur le traitement de ses données personnelles, qui peut être donnée par le biais d'une déclaration écrite ou orale ou d'une action affirmative claire.

Responsable de traitement

Le membre du personnel du HCR, généralement le représentant d'un bureau de pays du HCR, qui est habilité à superviser la gestion et à définir les finalités du traitement des données personnelles.

Sous-traitant

Tout membre du personnel du HCR, personne physique ou organisation, y compris un partenaire d'exécution ou un tiers, qui procède au traitement des données personnelles au nom du responsable de traitement.

Point focal de la protection des données

En principe, le membre du personnel du HCR chargé de la protection du grade le plus élevé dans un bureau ou une opération de pays du HCR, qui aide le responsable de traitement à assumer ses responsabilités au titre de la présente politique.

Analyse d'impact relative à la protection des données

Outil et processus d'évaluation de l'impact en matière de protection sur les personnes concernées lié au traitement de leurs données personnelles et permettant d'identifier les mesures correctives visant à éviter ou à minimiser cet impact.

Délégué à la protection des données

Le membre du personnel du HCR de la Division de la protection internationale au Siège qui supervise, contrôle et présente des rapports sur le respect de la présente politique. Les fonctions du délégué à la protection des données sont énoncées à la section 7.3.

Personne concernée

La personne dont les données personnelles font l'objet du traitement.

Accord sur le transfert des données

Accord conclu entre le HCR et un partenaire d'exécution ou un tiers stipulant les modalités d'utilisation des données personnelles, en précisant quels éléments des données seront partagés, le mode de transfert, de quelles façons les données peuvent être utilisées, les mesures relatives à la sécurité des données et les autres questions connexes.

Partenaire d'exécution

Organisation établie en tant qu'entité autonome et indépendante vis-à-vis du HCR et que le HCR engage par le biais d'un accord de partenariat de projet dans le but d'entreprendre des activités programmatiques relevant de son mandat.

Données personnelles

Toute donnée liée à une personne qui peut être identifiée à partir de cette donnée, à partir de cette donnée et d'autres informations ou par des moyens raisonnablement susceptibles d'être utilisés en rapport avec cette donnée. Les données personnelles comprennent les données biographiques (« biodata ») telles que le nom, le sexe, la situation matrimoniale, la date et le lieu de naissance, le pays d'origine, le pays d'asile, le numéro d'enregistrement individuel, la profession, la religion et l'ethnicité, les données biométriques[4] telles que la photographie, les empreintes digitales, l'image du visage ou de l'iris, ainsi que tout avis sur la personne, telles que les évaluations du statut et/ou besoins spécifiques.

Violation de données personnelles

Une violation de la sécurité des données conduisant à la destruction, perte, modification accidentelle ou illégale/illégitime, à la divulgation ou à l'accès non autorisé à des données personnelles transférées, stockées ou autrement traitées.

4 Les données biométriques sont des caractéristiques biologiques (anatomiques ou physiologiques) ou comportementales personnelles qui peuvent être utilisées pour établir l'identité d'une personne en les comparant avec des données de référence sauvegardées.

© UNHCR / Dalia Khamissy

Personne relevant de la compétence du HCR

Une personne dont les besoins de protection et d'assistance relèvent du mandat du HCR. Cela inclut les réfugiés, les demandeurs d'asile, les apatrides, les personnes déplacées à l'intérieur de leur propre pays et les rapatriés.

Traitement des données personnelles

Toute opération, ou ensemble d'opérations, automatisée ou manuelle, qui est effectuée sur des données personnelles, incluant sans s'y limiter, la collecte, l'enregistrement, l'organisation, la structuration, le stockage, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, le transfert (sous forme orale, écrite ou informatisée), la diffusion ou d'autres formes de mise à disposition, la correction ou la destruction.

Tiers

Toute personne physique ou morale autre que la personne concernée, le HCR ou un partenaire d'exécution. Les gouvernements nationaux, les organisations internationales gouvernementales ou non gouvernementales, les entités ou des représentants du secteur privé sont quelques exemples de tiers.

2

PRINCIPES FONDAMENTAUX

2.1 PRINCIPES FONDAMENTAUX DU TRAITEMENT DES DONNÉES PERSONNELLES

Le personnel du HCR doit respecter et appliquer les principes fondamentaux suivants lors du traitement des données personnelles :

(i) Traitement légitime et juste

(ii) Spécification des finalités

(iii) Nécessité et proportionnalité

(iv) Exactitude

(v) Respect des droits de la personne concernée

(vi) Confidentialité

(vii) Sécurité

(viii) Responsabilités et supervision

2.2 TRAITEMENT LÉGITIME ET JUSTE

Le traitement des données personnelles ne doit être effectué que sur des bases légitimes et d'une façon juste et transparente. Le HCR ne doit effectuer le traitement des données personnelles que sur une ou plusieurs des bases légitimes suivantes :

(i) Avec le consentement de la personne concernée

(ii) Dans l'intérêt vital ou supérieur de la personne concernée

(iii) Afin de permettre au HCR de s'acquitter de son mandat

(iv) Au-delà du mandat du HCR, afin d'assurer la sûreté et la sécurité des personnes relevant de sa compétence et autres individus

2.3 SPÉCIFICATION DES FINALITÉS

Les données personnelles doivent être collectées à une ou plusieurs finalités spécifiques et légitimes et ne doivent pas être traitées d'une façon qui soit incompatible avec cette/ces finalité(s).

2.4 NÉCESSITÉ ET PROPORTIONNALITÉ

Le traitement des données personnelles doit être nécessaire et proportionné à la(aux) finalité(s) pour la(es)quelle(s) elles sont traitées. Par conséquent, les données qui sont traitées doivent être adéquates et pertinentes au regard de la finalité identifiée, et ne pas excéder cette finalité.

2.5 EXACTITUDE

Les données personnelles doivent être enregistrées de la façon la plus exacte possible et, le cas échéant, être mises à jour de façon à s'assurer qu'elles servent la(es) finalité(s) pour la(es)quelle(s) elles sont traitées.

2.6 RESPECT DES DROITS DE LA PERSONNE CONCERNÉE

Les droits de la personne concernée à l'information, à l'accès, à la correction, à l'effacement et à l'opposition sont abordés dans la section 3 de la présente politique.

2.7 CONFIDENTIALITÉ

Le personnel du HCR doit à tout moment maintenir la confidentialité des données personnelles des personnes relevant de sa compétence, même après que lesdites personnes ne relèvent plus de la compétence du HCR.

2.8 SÉCURITÉ

Afin d'assurer la confidentialité et l'intégrité des données personnelles, des mesures appropriées de sécurité technique et organisationnelle des données doivent être mises en place. La sécurité des données et d'autres questions connexes sont abordées dans la section 4 de la présente politique. Le transfert des données personnelles vers des tiers ne peut être effectué que dans les conditions spécifiées dans la section 6.

2.9 RESPONSABILITÉS ET SUPERVISION

Afin que les responsabilités en matière de traitement des données personnelles soient conformes à la présente politique, le HCR définira une structure des responsabilités et de la supervision, présentée dans la section 7.

3

DROITS DE LA PERSONNE CONCERNÉE

3.1 INFORMATIONS

Lors de la collecte de données personnelles auprès d'une personne concernée, le HCR doit informer la personne concernée des points suivants, sous une forme écrite ou orale, ainsi que d'une manière et dans une langue compréhensibles par la personne concernée :

(i) La(les) finalité(s) précise(s) pour la(les)quelle(s) les données personnelles ou les catégories de données personnelles seront traitées ;

(ii) Si ces données seront transférées à un(des) partenaire(s) d'exécution ou à des tiers ou, le cas échéant, si les données sont collectées par un partenaire d'exécution au nom du HCR ;

(iii) L'importance de fournir des données exactes et complètes ;

(iv) Le devoir de la personne concernée d'informer à tout moment le HCR, et/ou, le cas échéant, les partenaires d'exécution des modifications apportées à sa situation personnelle ;[5]

(v) Toutes les conséquences d'un refus ou d'un manquement à l'obligation de fournir les données personnelles demandées ;

(vi) Le droit de la personne concernée d'accéder à ses données personnelles, de les corriger ou de les effacer ;

(vii) Le droit de la personne concernée de faire opposition à la collecte des données personnelles ;

(viii) Comment déposer une plainte auprès du responsable de traitement et du Bureau de l'Inspecteur général.

5 En particulier les changements dans l'état civil, par exemple les naissances, les décès et les mariages.

3.2 ACCÈS

Sur demande auprès du HCR, la personne concernée peut obtenir :

(i) Confirmation que des données la concernant ont été, sont ou seront traitées ; et

(ii) Des informations sur les données personnelles traitées, la(es) finalité(s) du traitement de ces données et sur le(s) partenaire(s) d'exécution et/ou les tiers à qui ces données ont été, sont ou seront transférées.

3.3 CORRECTION ET EFFACEMENT

3.3.1 La personne concernée peut demander la correction ou l'effacement des données personnelles qui sont inexactes, incomplètes, inutiles ou superflues.

3.3.2 Lorsqu'une personne concernée demande la correction ou l'effacement de ses données personnelles, le HCR doit demander la preuve démontrant qu'elles sont inexactes ou incomplètes.

3.4 OPPOSITION

Sous réserve des restrictions stipulées dans la section 3.7 ci-dessous, une personne concernée peut faire opposition au traitement de ses données personnelles lorsqu'il existe des motifs légitimes précisément liés à sa situation personnelle. Si l'opposition est justifiée, le HCR ne doit plus procéder au traitement des données personnelles concernées.

3.5 MODALITÉS DES DEMANDES

3.5.1 Les demandes d'information concernant l'accès aux données personnelles, leur correction ou leur effacement, ou une opposition, doivent être effectuées par la personne concernée ou son représentant légal autorisé, ou, si c'est un enfant, par un parent ou un tuteur légal. Les demandes doivent être soumises oralement ou par écrit auprès du bureau du HCR, dans le pays où les données sont traitées.

3.5.2 Avant de répondre à toute demande ou opposition, le HCR doit vérifier l'identité de la personne qui a fait la demande ou l'opposition. L'individu est tenu de s'identifier de façon appropriée. Dans le cas d'un représentant légal ou d'un tuteur légal, la preuve de cette autorité légale doit être fournie. Les demandes ou oppositions faites par des parents ou des tuteurs au nom d'enfants doivent être évaluées par rapport à l'intérêt supérieur de l'enfant.

3.6 ENREGISTREMENT ET RÉPONSE DU HCR

3.6.1 Le HCR doit enregistrer le fait d'avoir fourni à la personne concernée les informations prévues à la section 3.1 et les demandes d'accès, de correction, d'effacement ou d'opposition ainsi que les réponses données à ces demandes, conformément aux sections 3.2, 3.3 et 3.4.

3.6.2 Le HCR doit répondre à une demande ou à une opposition conformément à la section 3 dans un délai raisonnable, oralement ou par écrit, ainsi que d'une manière et dans une langue compréhensibles par la personne concernée et/ou, selon le cas, son représentant légal ou tuteur légal.

© UNHCR / M. Abu Asaker

3.7 LIMITATIONS

Après avoir consulté le délégué à la protection des données, et toute autre partie prenante au Siège, le HCR peut refuser de fournir une réponse ou limiter ou restreindre sa réponse à une demande ou à une objection conformes à la section 3 si :

(i) Cela constitue une mesure nécessaire et proportionnée visant à sauvegarder ou à garantir un ou plusieurs des points suivants :

(a) La sûreté et la sécurité du HCR, de son personnel ou du personnel des partenaires d'exécution ;

(b) Les priorités et besoins opérationnels primordiaux du HCR dans le cadre de son mandat.

(ii) Il existe des raisons de considérer que la demande est manifestement abusive, frauduleuse ou visant à faire obstruction à la finalité du traitement.

4

TRAITEMENT DES DONNÉES PAR LE HCR

4.1 CONFIDENTIALITÉ DES DONNÉES PERSONNELLES

4.1.1 Par définition, les données personnelles sont classées comme étant confidentielles. La confidentialité des données personnelles doit être respectée à tout moment par le HCR lors du traitement des données.

4.1.2 Afin d'assurer et de respecter la confidentialité, les données personnelles doivent être rangées et conservées d'une façon qui n'est accessible qu'au personnel autorisé, et ne doivent être transférées qu'en utilisant des moyens de communication protégés.

4.2 SÉCURITÉ DES DONNÉES PERSONNELLES

4.2.1 Le HCR doit assurer et mettre en oeuvre un haut niveau de sécurité des données qui est adapté aux risques que constituent la nature et le traitement des données personnelles, à la disponibilité et à la qualité des équipements nécessaires, aux coûts et à la faisabilité opérationnelle.

4.2.2 Les mesures de sécurité des données du HCR ont pour objet de protéger les données personnelles contre les risques de destruction, de perte, de modification accidentelle ou illégale/illégitime, de divulgation ou d'accès non autorisé à des données personnelles.

4.2.3 Compte tenu de la technologie disponible et des coûts de la mise en oeuvre, le HCR doit mettre en place les mesures organisationnelles et techniques appropriées afin de s'assurer que le traitement satisfait aux exigences de la présente politique. Il doit notamment veiller à mettre en place des outils et des technologies renforçant la protection des données et permettant aux sous-traitants de mieux protéger les données personnelles (« respect de la vie privée dès la conception et par défaut »).

4.2.4 Les mesures organisationnelles comprennent :

(i) L'établissement de procédures opérationnelles standard ;

(ii) L'organisation de la formation du personnel à la protection et à la sécurité des données ; et

(iii) La conduite d'analyses d'impact relatives à la protection des données (section 4.5).

4.2.5 Les mesures techniques comprennent :

(i) La préservation de la sécurité physique des locaux, des équipements portables, des dossiers et des enregistrements concernant des cas individuels ;

(ii) La préservation de la sécurité des systèmes informatiques et des technologies de l'information, par exemple, le contrôle de l'accès (les mots de passe, l'accès progressif), le contrôle des utilisateurs, le contrôle du stockage, le contrôle des données ajoutées, le contrôle de la communication et du transport (par ex. le cryptage).

4.2.6 Dans les situations de détérioration de la sécurité qui font courir des risques sérieux de violations des données personnelles, le HCR doit prendre toutes les mesures nécessaires et possibles pour éviter de telles violations des données personnelles en relocalisant, ou, en dernier recours, en détruisant les dossiers concernant des cas individuels, numérisés ou sur papier, qui contiennent des données personnelles, afin d'éviter tout préjudice que pourraient subir les personnes concernées.

4.3 GARANTIR L'EXACTITUDE DES DONNÉES PERSONNELLES

4.3.1 Le HCR peut corriger ou effacer les données personnelles conservées dans ses systèmes qui sont inexactes, incomplètes, inutiles ou superflues.

4.3.2 Le HCR doit mettre à jour les enregistrements de données personnelles lorsque cela s'avère nécessaire et les vérifier de manière régulière.

4.3.3 Lorsque des données personnelles sont corrigées ou effacées dans les systèmes du HCR, le HCR devra en informer l'ensemble des partenaires d'exécution et/ou des tiers auxquels les données personnelles pertinentes ont été transférées dès que raisonnablement possible.

4.4 NOTIFICATION D'UNE VIOLATION DE DONNÉES PERSONNELLES

4.4.1 Dès que le personnel du HCR prend connaissance d'une violation de données personnelles, il est tenu d'en informer dès que possible le responsable de traitement et d'enregistrer la violation de façon appropriée.

4.4.2 Si une violation de données personnelles est susceptible de causer à la personne concernée des blessures ou des atteintes personnelles, le responsable de traitement doit déployer tous les efforts possibles pour communiquer à la personne concernée la violation de données personnelles et prendre sans délai indu les mesures correctives appropriées. Dans de tels cas, le responsable de traitement doit également informer le délégué à la protection des données de la violation des données personnelles.

4.4.3 La notification doit décrire :

(i) La nature de la violation de données personnelles, y compris les catégories et le nombre de personnes concernées et d'enregistrements de données concernés ;

(ii) Les conséquences négatives et prévisibles de la violation de données personnelles ; et

(iii) Les mesures prises ou proposées pour atténuer et traiter les impacts négatifs possibles de la violation de données personnelles.

4.5 ANALYSE D'IMPACT RELATIVE À LA PROTECTION DES DONNÉES

4.5.1 Lors de l'élaboration de nouveaux systèmes, projets ou politiques ou avant de conclure des accords sur le transfert des données avec des partenaires d'exécution ou des tiers qui peuvent avoir un impact négatif sur la protection des données personnelles des personnes relevant de la compétence du HCR, le HCR doit procéder à une analyse d'impact relative à la protection des données (AIPD). Une AIPD doit être effectuée lorsque la collecte et le traitement ou le transfert de données personnelles est susceptible d'être important, répété ou structurel (c'est-à-dire lorsque les données sont partagées avec un partenaire d'exécution ou un tiers pendant une période donnée).

4.5.2 Une AIPD comprend une description générale du système, du projet, de la politique ou des dispositions relatives au partage de données impliquant un traitement de données personnelles qui sont envisagés, une analyse des risques auxquels sont exposés les droits des personnes concernées compte tenu des circonstances et de la nature des données personnelles traitées, des mesures de protection et de toutes

les mesures nécessaires en place ou proposées pour s'assurer du respect de la présente Politique.

4.5.3 Les responsables de traitement sont responsables, le cas échéant, de l'organisation et de la mise en oeuvre des AIPD. Les AIPD sont normalement effectuées au niveau des pays sauf s'il est décidé que l'AIPD doit être effectuée au niveau régional ou mondial en raison de la portée du système ou des dispositions à prendre.

4.5.4 Les responsables de traitement doivent tenir le délégué à la protection des données pleinement informé de toute AIPD effectuée sous leur responsabilité et doivent lui transmettre un exemplaire de l'AIPD.

4.6 CONSERVATION

4.6.1 Les données personnelles qui ne sont pas enregistrées dans les dossiers concernant des cas individuels ne sont pas conservées plus longtemps que nécessaire à la(aux) finalité(s) pour la(es)quelle(s) elles ont été collectées.

4.6.2 Tous les dossiers concernant des cas individuels, ouverts ou clos, sont considérés comme des enregistrements permanents, et doivent, par conséquent, être conservés de façon permanente, conformément à la politique en matière de recherche et d'accès aux archives du HCR.[6]

6 Politique du HCR en matière de recherche et d'accès aux archives, en ligne : http://www.unhcr.org/fr/archives-dossiers.html et http://www.unhcr.org/3b03896a4.html.

5

TRAITEMENT DES DONNÉES EFFECTUÉ PAR DES PARTENAIRES D'EXÉCUTION

5.1 CONDITIONS GÉNÉRALES

Lorsque la collecte et le traitement des données personnelles constituent l'une des responsabilités des partenaires d'exécution, les données sont collectées et traitées au nom du HCR. Pour ces raisons, les partenaires d'exécution doivent respecter et mettre en oeuvre des normes et principes fondamentaux de protection des données personnelles identiques ou similaires à ceux qui sont stipulés dans la présente politique (en particulier les sections 2, 3 et 4). Cette condition est applicable lorsque le HCR a l'intention de transférer des données personnelles à des partenaires d'exécution, mais aussi lorsque des partenaires d'exécution collectent des données personnelles pour exercer les activités convenues.

5.2 VÉRIFICATION

Quel que soit l'accord de partenariat, avant de transférer des données personnelles à un partenaire d'exécution ou d'impliquer un partenaire d'exécution dans la collecte et le traitement de données personnelles, le HCR doit vérifier que le traitement des données personnelles effectué par le partenaire d'exécution satisfait aux normes et principes fondamentaux de la présente politique. Cette vérification peut faire partie d'une analyse d'impact relative à la protection des données.

© UNHCR / Frederic Noy

5.3 ACCORDS DE PARTENARIAT

Le HCR exige des partenaires d'exécution qu'ils respectent la présente politique par le biais d'un engagement qui ressort de la signature des accords de partenariat. Ces accords doivent également spécifier la(es) finalité(s) du traitement des données personnelles ainsi que la base légitime du traitement.

5.4 CAPACITÉS DU PARTENAIRE

Le HCR peut être appelé à aider les partenaires d'exécution à développer ou à renforcer leurs capacités afin qu'ils puissent respecter les normes et principes fondamentaux de la protection des données stipulés dans la présente politique. Cette aide peut être apportée en rapport avec l'établissement ou l'ajustement de politiques, la mise en oeuvre de formations ou l'instauration de mesures techniques et organisationnelles.

5.5 CESSATION DU PARTENARIAT

Après la cessation d'un partenariat, toutes les données personnelles collectées dans le cadre de ce partenariat doivent être restituées au HCR. Les accords de partenariat peuvent prévoir des exceptions, en particulier lorsqu'il existe des raisons légitimes de ne pas restituer les données, notamment le consentement des personnes concernées.

6

TRANSFERT DE DONNÉES PERSONNELLES À DES TIERS

6.1 CONDITIONS GÉNÉRALES

6.1.1 Le HCR peut transférer des données personnelles à des tiers à condition que les tiers assurent un niveau de protection des données identique ou similaire à celui stipulé dans la présente politique.

6.1.2 Compte tenu des risques potentiels pour la protection des données qu'impliquent les transferts à des tiers, le HCR doit prêter une attention particulière aux principes fondamentaux suivants de la présente politique :

(i) Le transfert doit s'appuyer sur une ou plusieurs bases légitimes ;

(ii) Le transfert doit répondre à une ou plusieurs finalité(s) spécifique(s) et légitime(s) ;

(iii) Les données personnelles devant être transférées sont appropriées, pertinentes, nécessaires et n'excédant pas la (les) finalité(s) pour la(les)quelle(s) elles sont transférées ;

(iv) La personne concernée a été informée, soit au moment de la collecte, conformément à la section 3.1, soit ultérieurement, du transfert de ses données personnelles, sauf si une ou plusieurs des restrictions stipulées à la section 3.7 est applicable ;

(v) Le tiers respecte la confidentialité des données personnelles qui lui sont transférées par le HCR. Qu'un accord relatif au transfert des données ait ou non été signé entre le HCR et le tiers, le HCR doit chercher à obtenir un accord écrit du tiers spécifiant que la confidentialité des données personnelles sera respectée à tout moment. Afin d'assurer et de respecter la confidentialité, les données personnelles doivent être rangées et conservées de façon à ce qu'elles ne soient accessibles qu'au personnel autorisé et à ce qu'elles ne soient transférées que par le biais de moyens de communication protégés ;

(vi) Le tiers maintient un haut niveau de sécurité qui protège les données personnelles contre les risques de destruction, de perte, de modification accidentelle ou illégale/illégitime, de divulgation ou d'accès non autorisé aux données.

6.1.3 En outre, le HCR doit s'assurer que le transfert des données personnelles n'a pas d'impact négatif sur

(i) la sûreté et la sécurité du personnel du HCR et/ou du personnel des partenaires d'exécution ; et/ou sur

(ii) le fonctionnement efficace des opérations du HCR ou qu'il ne compromet pas le mandat du HCR, par exemple en entraînant une perte du climat de confiance entre le HCR et les personnes relevant de sa compétence ou une détérioration de l'image du HCR en tant qu'organisation indépendante, humanitaire et apolitique.

6.1.4 Avant d'accepter de transférer des données personnelles à un tiers, le HCR doit évaluer le niveau de protection des données proposé par le tiers. Dans le cadre de cette évaluation, le responsable de traitement doit évaluer, entre autres, les lois et réglementations applicables, les règlements et les politiques internes du tiers, les obligations ou engagements contractuels spécifiques visant à respecter des cadres spécifiques en matière de protection des données, l'efficacité de leur mise en oeuvre ainsi que les moyens techniques et organisationnels de sécurité des données mis en place. Conformément à la section 4.5, le responsable de traitement peut avoir besoin de mener une AIPD.

6.2 ACCORDS RELATIFS AU TRANSFERT DES DONNÉES

6.2.1 Sauf s'il existe des raisons satisfaisantes de ne pas le faire, avant de transférer des données personnelles à un tiers, le responsable de traitement doit chercher à conclure un accord relatif au transfert des données, ou, selon le cas, à incorporer

des clauses relatives à la protection des données dans des accords plus larges, en particulier lorsque les transferts de données sont susceptibles d'être importants, répétés ou structurels, c'est-à-dire lorsque le(s) même(s) type(s) de données est(sont) partagé(s) avec le même tiers pendant une période donnée.

6.2.2 Les accords relatifs au transfert des données doivent, entre autres:

(i) évoquer la(es) finalité(s) du transfert des données, les éléments de données spécifiques qui doivent être transférés ainsi que les mesures de protection des données et de sécurité des données qui doivent être mises en place ;

(ii) exiger du tiers qu'il s'assure que les mesures de protection des données et de sécurité des données respectent la présente politique ; et

(iii) stipuler les mécanismes de consultation, supervision, de responsabilisation et d'examen mis en place pour surveiller le transfert pendant la durée de vie de l'accord.

6.2.3 Le délégué à la protection des données et le Service des affaires juridiques (LAS) doivent examiner et accepter tous les accords relatifs au transfert des données. Les exemplaires des accords finaux doivent être remis au délégué à la protection des données.

6.3 TRANSFERT AUX ORGANISMES NATIONAUX CHARGÉS DE L'APPLICATION DE LA LOI ET AUX TRIBUNAUX NATIONAUX

6.3.1 Dans les circonstances appropriées, le HCR peut transférer des données personnelles à un organisme national chargé de l'application de la loi ou à un tribunal national. Ces transferts

peuvent être effectués sur demande de l'organisme chargé de l'application de la loi ou du tribunal, ou à l'initiative du HCR. Les transferts peuvent concerner des personnes faisant l'objet d'une enquête pour une infraction pénale qu'elles sont soupçonnées d'avoir commise, ou être liés à une(des) victime(s) ou un(des) témoin(s) d'une infraction pénale.

6.3.2 Parallèlement aux conditions générales du transfert de données personnelles à des tiers (section 6.1, à l'exception du point 6.1.2 (iv)), le HCR ne peut collaborer à de telles demandes et transférer des données personnelles à un organisme national chargé de l'application de la loi ou à un tribunal national que si les conditions suivantes sont remplies :

(i) Le transfert est nécessaire à des fins de détection, de prévention, d'investigation ou de poursuite engagée pour infraction pénale grave, en particulier pour éviter qu'un individu ou le public ne soit exposé à un risque immédiat et substantiel pour sa sûreté et sa sécurité ;

(ii) L'organisme national chargé de l'application de la loi ou le tribunal national qui fait la demande est compétent en matière de détection, de prévention, d'investigation ou de poursuite concernant l'infraction en question ;

(iii) Le transfert aidera considérablement l'organisme chargé de l'application de la loi ou le tribunal dans la réalisation de ces objectifs et les données personnelles ne peuvent pas être obtenues auprès d'autres sources ;

(iv) Le transfert n'interfère pas de façon disproportionnée avec le droit à la vie privée ou à d'autres droits de l'Homme de la personne concernée ou d'une autre personne relevant de la compétence du HCR ; et

(v) Dans le cas de données relatives à des victimes et témoins, leur consentement au transfert a été obtenu.

6.3.3 Préalablement au transfert de données personnelles à un organisme national chargé de l'application de la loi ou à un tribunal national, il sera nécessaire de recueillir les avis du Délégué à la protection des données, en consultation avec l'Unité de la protection et de la sécurité nationale de la Division de la protection internationale, le LAS et le(s) Bureau(x) concerné(s).

6.4 ORGANISME INTERNATIONAL CHARGÉ DE L'APPLICATION DE LA LOI, COUR, TRIBUNAL OU AUTRE ORGANISME INTERNATIONAL

Les demandes de transfert de données personnelles effectuées par la Cour pénale internationale, les juridictions pénales internationales *ad hoc*, les commissions d'enquête mandatées par l'ONU et les organismes internationaux similaires doivent être transmises à la Division de la protection internationale (délégué à la protection des données, Unité de la protection et de la sécurité nationale et, selon le cas, l'Unité de liaison pour les droits de l'Homme) et au LAS.

6.5 PRIVILÈGES ET IMMUNITÉS

Le transfert de données personnelles ne porte pas préjudice aux privilèges et immunités du HCR accordés en vertu de la *Convention sur les privilèges et immunités de l'Organisation des Nations Unies* de 1946 et ne doit pas être considéré comme tel. Les privilèges et immunités du HCR et des membres de son personnel existent quel que soit l'accord de coopération conclu avec le gouvernement d'un pays. Toute question concernant les privilèges et immunités doit être adressée au LAS.

7

RESPONSABILITÉS ET SUPERVISION

7.1 STRUCTURE DES RESPONSABILITÉS ET DE LA SUPERVISION

La structure des responsabilités et de la supervision mentionnée à la section 2.9 comprendra les principaux acteurs suivants :

(i) Un délégué à la protection des données au sein de la Division de la protection internationale, au siège du HCR,

(ii) Des responsables de traitement dans chaque bureau / opération de pays, et

(iii) Des points focaux de la protection des données dans les bureaux/opérations de pays.

7.2 LE RESPONSABLE DE TRAITEMENT ET LE POINT FOCAL DE LA PROTECTION DES DONNÉES

7.2.1 Le responsable de traitement est responsable de la mise en oeuvre et de la supervision du traitement des données personnelles relevant de son domaine de responsabilité. Par conséquent, il assume la principale responsabilité du respect de la politique. À cette fin, le responsable de traitement doit désigner un point focal de la protection des données. En principe, le point focal de la protection des données est le membre du personnel du HCR en charge de la protection du bureau/opération de pays ayant le grade le plus élevé.

7.2.2 Avec l'assistance du point focal de la protection des données, le responsable de traitement doit mettre en oeuvre la présente politique en, notamment :

(i) Déterminant la base légitime et les finalités légitimes et spécifiques applicables du traitement des données ;

(ii) Assurant la mise en oeuvre des mesures organisationnelles et de sécurité ainsi qu'en évaluant la sécurité des données assurée par les tiers ;

(iii) Établissant des procédures internes, par exemple sous la forme de procédures opérationnelles standard de la protection des données, couvrant tous les aspects pertinents de la présente politique, en particulier le respect des droits de la personne concernée et les mesures visant à assurer la confidentialité et la sécurité des données ;

(iv) S'assurant que les aspects touchant à la protection des données et à la sécurité des données sont inclus de façon appropriée dans les accords conclus avec les partenaires d'exécution ;

(v) Négociant et concluant des accords de transfert de données avec des tiers, si cela s'avère nécessaire ou approprié.

7.2.3 Si cela s'avère nécessaire, le responsable de traitement et/ou le point focal de la protection des données doit/doivent chercher à recueillir l'avis du délégué à la protection des données concernant les questions relatives à l'application et à l'interprétation de la présente politique.

7.3 LE DÉLÉGUÉ À LA PROTECTION DES DONNÉES

7.3.1 Le HCR nommera un délégué à la protection des données qui travaillera au sein de la Division de la protection internationale, au siège du HCR, et dont les tâches consisteront à :

(i) Conseiller, soutenir et former à la protection des données et à la présente politique ;

(ii) Tenir les inventaires des informations fournies par les responsables de traitement et les points focaux de la protection des données, notamment les accords de transfert de données, les cas précis de partage des données du HCR avec des tiers, les analyses d'impact relative à la protection des données, les notifications de violations de données et les plaintes des personnes concernées ;

(iii) Activement encourager les responsables de traitement et les autres acteurs pertinents à prendre les mesures visant au respect de la présente politique ;

(iv) Surveiller et rendre compte du respect de la présente politique ;

(v) Assurer la liaison avec le LAS en tant que de besoin et conformément à la présente politique.

7.3.2 Par l'intermédiaire du Directeur de la Division de la protection internationale, le délégué à la protection des données soumettra chaque année un rapport sur la protection des données au Haut Commissaire adjoint pour la protection.

7.4 BUREAU DE L'INSPECTEUR GÉNÉRAL

La présente politique n'affecte pas les fonctions prévues par le mandat du Bureau de l'inspecteur général (IGO), notamment celles qui consistent à recevoir les plaintes pour faute disciplinaire présumée, par exemple pour violation de la confidentialité ou fraude, et à mener des investigations sur de telles fautes.[7] Ce faisant, l'IGO complète la structure de surveillance et de respect établie par la présente politique.

7.5 BUREAU DE L'ETHIQUE

À l'appui de la présente politique, le Bureau de l'éthique fournira des conseils sur les pratiques et normes en matière d'éthique et contribuera à atténuer les risques liés au traitement des données personnelles grâce à l'application du Code de conduite du HCR, et de la Politique relative à la protection des personnes contre les représailles (politique en matière de dénonciation d'abus).

7 Des informations sur les fonctions du BIG et sur la procédure à suivre pour déposer une plainte sont disponibles à l'adresse suivante: http://www.unhcr.org/pages/52e11b746.html.

© UNHCR / Jared Kohler

UNHCR
L'Agence des Nations
Unies pour les réfugiés

© UNHCR/HCP/2015/6