MANUEL DE PROTECTION DES DONNEES DE L'OIM

Organisation internationale pour les migrations

L'OIM est attachée au principe selon lequel des migrations humaines et ordonnées profitent aux migrants et à la société. En tant qu'organisation intergouvernementale, l'OIM agit avec ses partenaires de la communauté internationale afin d'aider à résoudre les problèmes opérationnels que pose la migration ; de faire mieux comprendre les questions migratoires ; d'encourager le développement économique et social grâce à la migration ; et de préserver la dignité humaine et le bien-être des migrants.

Editeur : Organisation internationale pour les migrations
17, route des Morillons
1211 Genève 19
Suisse
Tél : +41 22 717 91 11
Fax : +41 22 798 61 50
Courriel : hq@iom.int
Internet : http://www.iom.int

Illustration de la page de couverture : © Yvonne Lee-www.allegoric.co.uk

MANUEL DE PROTECTION DES DONNEES DE L'OIM

Organisation internationale pour les migrations

AVANT-PROPOS

La protection des données est un domaine du droit en constante évolution. En effet, la croissance rapide des technologies de l'information et le fait que les données sont transmissibles et facilement accessibles par voie numérique posent des problèmes de protection de la vie privée. L'augmentation des cas de vol ou de perte de données, et l'utilisation et la divulgation non autorisées ou inappropriées de données à caractère personnel de plus en plus fréquentes soulèvent des questions quant à la bonne application des lois et politiques. En outre, le recours à des techniques de pointe pour gérer la migration et la fraude aux documents cause de multiples difficultés en matière de protection des données et de droits de l'homme. Ces préoccupations sont plus sérieuses encore lorsqu'une divulgation par inadvertance peut nuire à la sécurité des personnes ou la mettre en danger. Que les mouvements soient réguliers ou irréguliers, toute donnée à caractère personnel communiquée dans un but précis doit être traitée avec toutes les précautions voulues afin de protéger les intérêts des personnes concernées et de façon que celles-ci soient pleinement conscientes des conséquences éventuelles pour leurs droits humains.

Les normes internationales de collecte et de traitement des données à caractère personnel sont universellement reconnues. Cependant, l'absence d'un instrument international contraignant fait l'objet d'un intense débat. A la 31e Conférence internationale des commissaires à la protection des données et à la vie privée, un certain nombre d'Etats ont adopté une résolution qui recommande une convention universelle et reconnaît que la protection des données et le respect de la vie privée sont des droits fondamentaux attachés à toute personne, quels que soient sa nationalité ou son lieu de résidence. L'OIM espère que cette publication contribuera aux discussions menées à l'échelle nationale et internationale.

Malgré les nombreux ouvrages sur la question, il existe peu de directives sur la protection des données à caractère personnel dans le contexte de la migration. L'OIM est heureuse d'apporter une première contribution aux discussions en cours sur la protection des données, et encourage une mobilisation plus grande sur cette question importante. En 2007, elle avait examiné des projets d'enregistrement dans 26 bureaux extérieurs. Il était apparu qu'il était effectivement nécessaire de normaliser le traitement des données à caractère personnel dans toute l'Organisation. La politique de l'OIM en matière de protection des données s'inspire des normes internationales pertinentes, notamment des principes de base relatifs à la protection des données reconnus par de nombreux Etats, mais s'appuie aussi sur des recherches consacrées aux politiques et procédures appliquées dans d'autres organisations. Les principes relatifs à la protection des données de l'OIM entendent aider le personnel de l'Organisation à prendre les précautions raisonnables qui s'imposent pour préserver la confidentialité des données à caractère personnel et garantir que les droits et les intérêts des bénéficiaires de l'OIM sont dûment protégés. La politique de protection des données suivie par l'OIM est en place depuis mai 2009, et chaque jour apporte son lot d'enseignements. Bien que la présente publication soit destinée à un usage interne, elle peut être utile à d'autres organisations œuvrant dans des contextes similaires.

Pour terminer, nous remercions l'auteur, Ruzayda Martens, d'avoir élaboré la stratégie de l'OIM relative à la protection des données et d'avoir fait en sorte que cette question soit dûment prise en considération dans l'action de l'OIM.

Richard Perruchoud

REMERCIEMENTS

L'auteur tient à remercier ses collègues de l'OIM, présents et passés, qui ont ouvert la voie au projet de protection des données dans le cadre des applications technologiques en matière de gestion de la migration (TAMM), élaboré conjointement par le Département de la gestion des migrations, la Division Technologie de l'information et communications et le Département du droit international de la migration et des affaires juridiques. Ce projet a bénéficié de l'expérience et du savoir-faire d'un grand nombre de collègues, tant des bureaux extérieurs que du Siège. Je remercie sincèrement l'équipe du projet, le comité directeur et les membres du groupe de travail qui, malgré un calendrier chargé, ont pris le temps d'apporter leurs contributions aux diverses étapes du projet.

Tout d'abord, je souhaite remercier les membres de l'équipe du projet : Shpëtim Spahiya, pour sa contribution et son soutien, grâce auxquels nous avons pu achever le projet dans les délais, et Chiara Frattini, Jacqueline Straccia et Elif Celik pour leurs recherches.

Je remercie aussi les membres du comité directeur : Yorio Tanimura, Jillyanne Redpath-Cross et Bernardo Mariano, pour leurs orientations éclairées et leurs inestimables contributions.

Toute ma gratitude va également aux membres du groupe de travail : Nicholas Theotocatos, Norbert Wühler, Monica Halil, Walter Brill, Sarah Craggs, Delbert Field, Lea Matherson, Jobste Koheler, Christopher Gascon, Elizabeth Dunlap, Dyane Epstein, Goran Grujovic, Chintana Meegamarachchi, Mariko Tomiyama, Teresa Zakaria et Jesus Sarol. Mes remerciements vont également à Jonathan Martens, Miwa Takahashi, Ashraf El-Nour, Richard Scott, Mio Sato, Amy Mahoney, Daniel Redondo, Ricardo Cordero, Tanja Brombacher, Mark Brown, Nasim Faruk, William Barriga, Gloria Ko, Patrick Corcoran, Abye Makonnen, Ramiro Nochez-McNutt, Anna Eva Randicetti et Robert Villamor, qui m'ont livré de précieux commentaires.

Enfin, je remercie Richard Perruchoud pour son soutien indéfectible, et mes collègues du Bureau des affaires juridiques pour les efforts qu'ils déploient afin de promouvoir la protection des données dans leur travail quotidien.

Ruzayda Martens[1]

[1] Juriste, OIM Genève. Les Directives en matière de protection des données ont été élaborées pour faciliter l'application des treize principes relatifs à la protection des données de l'OIM. Les opinions, constatations, interprétations et conclusions exprimées dans ces Directives sont celles de l'auteur, qui est seul responsable d'erreurs éventuelles.

INTRODUCTION

La mission de l'OIM, qui consiste à faciliter les mouvements migratoires, à comprendre les défis que pose la migration et à respecter la dignité humaine et le bien-être des migrants, nécessite de recueillir et de traiter des données à caractère personnel. La stratégie de protection des données de l'OIM vise à sauvegarder les intérêts des bénéficiaires de l'OIM ainsi que ceux de l'Organisation.

Il est de la plus haute importance de protéger les données pour garantir l'échange et le stockage en toute sécurité des données à caractère personnel, ainsi que leur traitement confidentiel. Il y a lieu de veiller systématiquement à la protection des données dans l'ensemble de l'Organisation pour renforcer les interventions et les systèmes de l'OIM.

Déclaration de l'OIM relative à la protection des données

> « **L'OIM prendra toutes les précautions raisonnables et nécessaires pour protéger la confidentialité des données à caractère personnel et l'anonymat des personnes concernées. Toutes les informations personnelles seront recueillies, utilisées, transférées et stockées en toute sécurité, conformément aux principes de l'OIM en matière de protection des données**. »

Objectifs clés :

- ../ Respecter la vie privée et répondre aux attentes des personnes concernées.
- ../ Protéger l'intégrité et la confidentialité des données à caractère personnel.
- ../ Prévenir toute divulgation inutile et inappropriée de données à caractère personnel.
- ../ Mettre en place des garanties institutionnelles détaillées régissant le traitement des données à caractère personnel.
- ../ Améliorer la compréhension de notions essentielles et des normes internationales régissant la protection des données.
- ../ Donner des directives opérationnelles pour mettre en œuvre les principes et les lignes directrices de l'OIM concernant les données.

La présente publication contient des orientations visant à protéger les données à caractère personnel dans le contexte de l'aide aux migrants. Elle comprend trois parties : la partie I, qui énonce les 13 principes relatifs à la protection des données de l'OIM ; la partie II, qui contient des lignes directrices détaillées relatives à la protection des données, ordonnées selon ces 13 principes ; et la partie III, qui renferme des modèles et des listes de vérification.

> Cet ouvrage est conçu comme un document vivant pouvant être adapté et révisé en fonction des besoins opérationnels émergents, de nouvelles orientations, et d'une mise à niveau ou d'une amélioration des systèmes de l'OIM.
>
> Les mesures de protection des données énoncées dans le présent document devront être appliquées avec souplesse, selon les conditions dans lesquelles un projet est mis en œuvre.

Le Bureau des affaires juridiques (LEG) au Siège de l'OIM est l'interlocuteur désigné pour toutes les questions relatives à la protection des données et peut assurer des formations à l'intention du personnel de l'OIM et de parties prenantes.

PARTIE I : Principes relatifs à la protection des données de l'OIM

1. COLLECTE LICITE ET LOYALE

Les données à caractère personnel doivent être obtenues à l'aide de procédés licites et loyaux au su de la personne concernée ou avec son consentement.

2. FINALITE DETERMINEE ET LEGITIME

La ou les finalités de la collecte et du traitement de données à caractère personnel doivent être déterminées et légitimes, et être connues de la personne concernée au moment de la collecte. Des données à caractère personnel ne seront utilisées qu'en vue de la ou des finalités déterminées, sauf si la personne concernée consent à une autre utilisation ou si ladite utilisation est compatible avec la ou les finalités déterminées initiales.

3. QUALITE DES DONNEES

Les données à caractère personnel demandées et obtenues doivent être adéquates, pertinentes et non excessives au regard de la ou des finalités déterminées pour lesquelles elles sont collectées et traitées. Les responsables du traitement des données prendront toutes les dispositions raisonnables pour que les données à caractère personnel soient exactes et à jour.

4. CONSENTEMENT

Le consentement doit être obtenu au moment de la collecte ou dès que possible ultérieurement, compte dûment tenu de l'état de santé et de la capacité juridique de certains groupes et personnes vulnérables. Si des circonstances exceptionnelles ne permettent pas d'obtenir le consentement, le responsable du traitement des données veillera au moins à ce que la personne concernée dispose des connaissances suffisantes pour comprendre et saisir la ou les finalités déterminées pour lesquelles les données à caractère personnel sont recueillies et traitées.

5. TRANSFERT A DES TIERS

Des données à caractère personnel ne seront transférées à des tiers qu'avec le consentement exprès de la personne concernée, pour une finalité déterminée, et avec la garantie que des mesures suffisantes ont été prises pour protéger la confidentialité desdites données et garantir le respect des droits et des intérêts de la personne concernée. Ces trois conditions de transfert doivent être garanties par écrit.

6. CONFIDENTIALITE

La confidentialité des données à caractère personnel doit être préservée à toutes les étapes du processus de collecte et de traitement des données, et sera garantie par écrit. Tous les membres du personnel de l'OIM et les personnes représentant des tiers qui sont autorisés à avoir accès à des données à caractère personnel et à les traiter sont tenus à la confidentialité.

7. ACCES ET TRANSPARENCE

Les personnes concernées auront la possibilité de vérifier leurs données à caractère personnel et pourront y accéder pour autant que la ou les finalités déterminées pour lesquelles elles ont été recueillies et traitées ne s'en trouvent pas compromises. Les responsables du traitement des données veilleront à l'application d'une politique générale d'ouverture à l'égard de la personne concernée en l'informant des faits nouveaux, des pratiques et des politiques concernant les données à caractère personnel.

8. SECURITE DES DONNEES

Les données à caractère personnel doivent être conservées en lieu sûr, tant sur le plan technique qu'organisationnel, et seront protégées par des mesures raisonnables et suffisantes contre toute modification non autorisée, falsification, destruction illégale, perte accidentelle, divulgation abusive ou transfert indu. Les mesures de protection énoncées dans les politiques et directives pertinentes de l'OIM s'appliqueront à la collecte et au traitement des données à caractère personnel.

9. CONSERVATION DES DONNEES A CARACTERE PERSONNEL

Les données à caractère personnel seront conservées aussi longtemps que nécessaire ; elles seront détruites ou rendues anonymes dès que la ou les finalités déterminées pour lesquelles elles ont été recueillies et traitées auront été atteintes. Elles pourront toutefois être conservées pendant une période déterminée additionnelle si l'intérêt de la personne concernée l'exige.

10. APPLICATION DES PRINCIPES

Ces principes s'appliqueront aux dossiers électroniques et papier de données à caractère personnel, et pourront être complétés par des mesures de protection additionnelles selon, entre autres, la sensibilité des données à caractère personnel. Ils ne s'appliqueront pas aux données à caractère non personnel.

11. PROPRIETE DES DONNEES A CARACTERE PERSONNEL

L'OIM est propriétaire des données à caractère personnel recueillies directement auprès des personnes concernées ou recueillies pour le compte de l'OIM, sauf accord contraire conclu par écrit avec un tiers.

12. SURVEILLANCE, RESPECT ET RECOURS INTERNES

Un organe indépendant sera nommé pour surveiller l'application de ces principes et examiner les plaintes. Des correspondants pour la protection des données seront désignés pour apporter leur concours à la surveillance et à la formation. Des mesures seront prises pour remédier à toute collecte ou tout traitement illicite de données, ainsi qu'à toute atteinte aux droits et intérêts de la personne concernée.

13. EXCEPTIONS

Toute intention de déroger à ces principes doit être soumise au préalable, pour approbation, au Bureau des affaires juridiques de l'OIM ainsi qu'à l'unité ou au département compétent au Siège de l'OIM.

PARTIE II : Lignes directrices en matière de protection des données

Les présentes lignes directrices visent à faire en sorte que les principes de l'OIM relatifs à la protection des données (« principes de l'OIM ») soient appliqués de façon à respecter le droit des personnes à la protection de leurs données à caractère personnel, et à tenir compte de la nécessité, pour l'OIM, de recueillir, d'utiliser et de divulger des données à caractère personnel dans l'accomplissement de son mandat dans le domaine de la migration.

Etant donné la grande diversité des activités menées par l'OIM, les questions relatives à la protection des données doivent être prises en considération à toutes les étapes, depuis l'élaboration et la mise en œuvre des projets, jusqu'à l'évaluation et l'établissement des rapports.

1. Comment appliquer ces lignes directrices

Les lignes directrices en matière de protection des données doivent être appliquées de pair avec les autres politiques et lignes directrices pertinentes de l'OIM. Elles expliquent comment incorporer la protection des données dans les pratiques actuelles de collecte, de stockage, d'utilisation, de divulgation et d'élimination des données à caractère personnel.

Elles sont complétées par des encadrés attirant l'attention sur des aspects à prendre en considération, ainsi que par des modèles et des listes de vérification conçus pour aider les responsables du traitement des données à identifier les facteurs clés dont il faut tenir compte aux diverses étapes du traitement des données.

Encadré 1 : Considérations éthiques

../ Respecter la vie privée et la dignité des personnes concernées.

../ Garantir la sécurité et l'absence de discrimination.

../ Protéger la confidentialité des données à caractère personnel.

../ Prévenir la divulgation non autorisée et l'utilisation inappropriée de données à caractère personnel.

2. Terminologie

Qu'est-ce que la protection des données ?

La protection des données désigne l'application systématique d'un ensemble de mesures institutionnelles, techniques et matérielles qui garantissent le droit au respect de la vie privée en ce qui concerne la collecte, le stockage, l'utilisation et la divulgation de données à caractère personnel[2].

Toute personne a droit au respect de sa vie privée[3]. Le droit au respect de la vie privée est un droit universel qui n'est pas réservé aux ressortissants d'un pays et qui n'établit pas de distinction entre étrangers en situation régulière ou irrégulière. Dans sa volonté

de respecter la dignit® humaine et le bien-°tre des migrants et dôautres b®n®ficiaires, lôOIM sôemploie ¨ faire en sorte que les donn®es ¨ caract¯re personnel soient trait®es en toute prudence et confidentialit® Une utilisation inappropri®e ou la divulgation non autoris®e de donn®es ¨ caract¯re personnel peut entra´ner toutes sortes de risques, tels que des violences physiques, la discrimination ou la marginalisation sociale. Une approche normalis®e de la protection des donn®es dans lôensemble de lôOIM permettra de bien g®rer les strat®gies visant ¨ prot®ger les b®n®ficiaires ainsi que lôOrganisation elle-m°me. Les principes de lôOIM constituent un cadre pour la protection des donn®es et r®gissent le traitement de tous types de donn®es ¨ caract¯re personnel se rapportant aux b®n®ficiaires de lôOIM.

[2] Cette d®finition de la protection des donn®es a ®®adapt®e aux besoins de lôOIM et ®tablit une distinction entre la protection des donn®es et la s®curit®des donn®es (voir le glossaire).

[3] Les principes de lôOIM sont fond®s sur les normes et instruments internationaux pertinents. Voir, ¨ lôannexe A, la liste des instruments internationaux et r®gionaux qui r®gissent le droit au respect ¨ la vie priv®e et ¨ la protection des donn®es, et ¨ lôannexe B, une liste de lois nationales relatives ¨ la protection des donn®es.

Qu'en est-il des données à caractère personnel concernant le personnel de l'OIM?

Bien que les principes de l'OIM soient axés sur les bénéficiaires de l'Organisation, ils servent de référence pour la protection des données dans l'ensemble de l'Organisation.

Qui sont les personnes concernées ?

Ce sont des personnes qui peuvent être identifiées directement ou indirectement grâce à un ou plusieurs éléments précis, tels qu'un nom, un numéro d'identification, des conditions matérielles, ou des caractéristiques physiques, mentales, culturelles, économiques ou sociales.

Tous les bénéficiaires identifiés ou identifiables visés par les activités de l'OIM sont considérés comme des personnes concernées.

Qu'est-ce que des données à caractère personnel ?

Les données à caractère personnel s'entendent de toute information pouvant être utilisée pour identifier ou léser des personnes concernées.

Lorsqu'ils traitent des données à caractère personnel, les responsables du traitement des données doivent toujours tenir compte des méthodes sophistiquées susceptibles d'être utilisées pour identifier des personnes concernées.

Qu'est-ce que des méthodes sophistiquées ?

Ce sont des moyens extraordinaires mis en œuvre pour obtenir un accès non autorisé à des données à caractère personnel, qui exigent du temps, des efforts, des ressources et une détermination démesurés.

Les méthodes sophistiquées varieront selon la sensibilité des données à caractère personnel et la nature de l'activité de l'OIM. Les données à caractère personnel pouvant être utilisées pour menacer la vie de personnes concernées, de membres du personnel de l'OIM ou de personnes représentant des tiers autorisés sont à considérer comme étant hautement sensibles.

Encadré 2 : Liste de données à caractère personnel

- **Données biographiques :** nom, date de naissance, état civil, adresse ou dernier lieu de résidence, profession, téléphone et courriel, âge, langue, sexe, orientation sexuelle, race, origine ethnique ou sociale, nationalité, religion, culture, opinions politiques ou autres convictions, appartenance à un groupe, incapacité physique ou mentale et état de santé ;
- **Données biométriques et génétiques :** empreintes digitales, reconnaissance de l'iris, morphologie de la main, traits du visage, reconnaissance vocale et échantillons d'ADN ;
- **Données de base :** passé familial, histoire du ménage, relations avec les proches, les membres de la communauté et l'entourage ;
- **Conditions matérielles :** expérience d'atteintes aux droits de l'homme, renseignements concernant le transit, notamment l'itinéraire emprunté, études, expérience professionnelle, adresse professionnelle, et noms et coordonnées des membres du personnel de l'OIM ou des personnes représentant des tiers autorisés qui réalisent des entretiens et recueillent les données à caractère personnel ;
- **Images et enregistrements :** portraits ou photographies, images télévisées, vidéos, enregistrements vocaux et numériques, radiographies, échographies et autres images médicales ;
- **Pièces justificatives :** rapports médicaux, rapports psychologiques, rapports des numéros d'urgence, rapports de police ou autres rapports officiels ou officieux ;
- **Documents personnels :** dossier médical, documents comptables, coordonnées bancaires, extrait du casier judiciaire et activités délictueuses ;
- **Pièces justificatives :** originaux ou copies des passeports, cartes d'identité ou cartes de sécurité sociale, certificats de naissance, permis temporaires, permis de conduire, visas, certificats de mariage, diplômes scolaires, dossiers universitaires, certificats médicaux, titres de propriété, contrats de travail ou offres de recrutement.

Note : Cette liste n'est pas exhaustive et entend simplement donner un aperçu des catégories de données à caractère personnel collectées et traitées dans le cadre des activités de l'OIM.

EXEMPLE :

Des liens avec le crime organisé peuvent justifier l'utilisation de méthodes de suivi très élaborées pour identifier et localiser des personnes victimes de la traite.

Avant toute collecte de donn®es, les responsables du traitement des donn®es ®valueront leur degr® de sensibilit®, afin dôarr°ter les mesures de protection, les contr¹les dôacc¯s et les mesures de s®curit® ¨ appliquer dôun bout ¨ lôautre du cycle de traitement des donn®es.

Le degr® de sensibilit® de donn®es ¨ caract¯re personnel d®pend de la nature du projet de lôOIM, du type dôactivit® men®e par lôOrganisation, et des circonstances dans lesquelles les donn®es sont recueillies et trait®es. Il sôagit notamment des ®l®ments suivants :

- la situation du pays ;
- le groupe de population vis® ou la personne concern®e ;
- les comportements sociaux ou culturels ;
- les ®ventuelles atteintes ¨ lôint®grit® physique ; et
- la discrimination pouvant r®sulter dôune divulgation.

Encadr®3 : Evaluation de la sensibilit®

> Sensibilit® ®lev®e ;
> Sensibilit® mod®r®e ;
> Sensibilit® faible.

Consid®rations cl®s

0 Risque de pr®judice pour la personne concern®e ;
0 Risque de discrimination ;
0 Risque de pr®judice pour dôautres personnes concern®es ;
0 Risque de pr®judice pour le personnel de lôOIM et pour des personnes repr®sentant un tiers autoris®

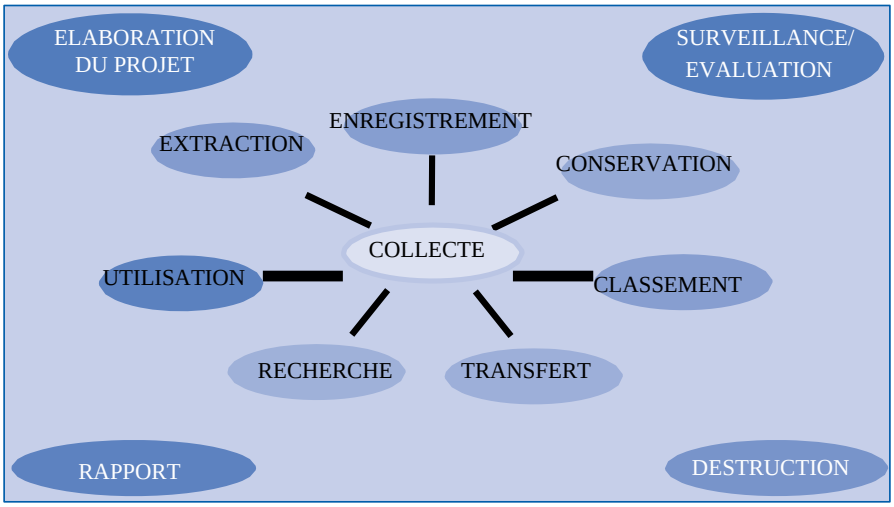
Il est important de mettre en ®vidence le niveau de sensibilit® des dossiers ®lectroniques et des dossiers papier.

Qu'est-ce que le traitement des données ?

Lôexpression ç traitement des donn®es è est un terme g®n®rique d®signant toutes les activit®s li®es ¨ lôutilisation de donn®es ¨ caract¯re personnel.

Les principes de lôOIM sôappliquent de la m°me mani¯re ¨ toutes les phases du traitement des donn®es.

Phases du traitement des donn®es



Note : *Le traitement des données n'est pas nécessairement un processus continu commençant par la collecte pour s'achever à la destruction des données, mais consiste souvent en un ensemble d'activités menées en parallèle à différentes étapes.*

Les responsables du traitement des données veilleront à ce que les donateurs, les partenaires de l'OIM, les partenaires d'exécution et les tiers soient informés de l'attachement de l'OIM à la protection des données à caractère personnel. Cela permettra de stimuler la coopération et de faciliter la mise en œuvre des principes de l'OIM. Les responsables du traitement des données incorporeront les principes de l'OIM dans les propositions de projet afin de pourvoir aux besoins de financement concernant :

- Les mesures de sécurité des données ;
- Les matériels et/ou logiciels informatiques ;
- Les capacités du personnel ; et
- Les formations.

On ne saurait trop insister sur l'importance de la formation. Celle-ci doit cibler les membres du personnel de l'OIM et les tiers autorisés, ainsi que les donateurs, les partenaires de l'OIM, les partenaires d'exécution et les autres parties prenantes (voir aussi le Principe 12).

Qu'est-ce qu'une évaluation du rapport risques/avantages ?

L'évaluation du rapport risques/avantages s'entend du processus consistant à soupeser les risques et les avantages liés au traitement des données.

Une évaluation du rapport risques/avantages[4] doit être effectuée avant toute collecte de données, et porter sur le contenu, la méthode de collecte, et les moyens mis en œuvre pour saisir, stocker puis utiliser les données à caractère personnel.

Les responsables du traitement des données doivent systématiquement mettre en balance la probabilité d'un préjudice et les avantages escomptés, et veiller à ce que les avantages l'emportent largement sur les risques éventuels.

Les risques dépendent de la probabilité qu'ils se produisent et de la gravité du préjudice. Même s'ils sont inévitables, les risques peuvent être réduits ou gérés. Des mesures de précaution et de protection et des solutions de rechange réalistes doivent être prévues dans les stratégies d'élaboration de projets ainsi que dans le processus de collecte de données, afin de réduire l'éventualité d'un préjudice ou d'en limiter la gravité ou la durée.

Que faire si les risques l'emportent sur les avantages ? *Des mesures adaptées de maîtrise des risques doivent être prises pour supprimer ou réduire la probabilité que le risque ne se produise. Si celui-ci est trop élevé, les responsables du traitement des données doivent interrompre le traitement des données.*

Encadré 4 : Indicateurs d'action selon le risque

> Risque élevé : inacceptable ;
> Risque modéré : prudence ;
> Risque faible : poursuite de l'activité.

0 Risque élevé → Abandon immédiat de l'activité jusqu'à la mise en œuvre de mesures de réduction du risque.
0 Risque modéré → Prudence et surveillance permanente et, au besoin, arrêt de l'activité pour mettre en œuvre des mesures de réduction du risque.
0 Risque faible → Poursuite de l'activité et surveillance permanente du rapport risques/avantages.

[4] L'évaluation du rapport risques/avantages n'est pas une évaluation technique valable en toutes circonstances. Il s'agit plutôt d'un jugement de valeur qui, souvent, dépend de divers facteurs, dont les comportements sociaux, culturels et religieux dominants du groupe de population cible ou de la personne concernée.

Il est important d'évaluer constamment les risques et les avantages tout au long du cycle de traitement des données parce que le rapport risques/avantages peut changer au fil du temps.

Les mesures de maîtrise des risques peuvent être les suivantes :

../ ***Elimination*** : Eliminer le risque est le meilleur moyen, et le plus sûr, de le réduire.

../ ***Remplacement*** : Si le risque ne peut être éliminé, le mieux est de remplacer l'activité risquée par une autre qui l'est moins.

../ ***Limitation*** : Une surveillance stricte peut contribuer à réduire au minimum le risque de préjudice.

../ ***Réduction*** : Des précautions supplémentaires permettent de réduire la probabilité d'un préjudice.

../ ***Formation*** : La sensibilisation sur les lieux de collecte peut faciliter l'identification et la gestion des risques.

../ ***Surveillance*** : Une surveillance permanente peut faciliter l'identification de mesures de protection appropriées pour réduire les risques au minimum.

Que faire si le rapport risques/avantages change après la collecte de données ?

Les responsables du traitement des données doivent évaluer les nouveaux risques par rapport aux avantages et étudier des possibilités de rechange réalistes. En l'absence de solutions de rechange, tout doit être mis en œuvre pour réduire les risques et leurs effets dommageables au minimum. Si le risque élevé subsiste, le traitement des données doit être suspendu.

Les responsables du traitement des données continueront à soupeser les risques et les avantages tout au long du cycle de traitement des données.

Encadré 5 : Effectuer une évaluation du rapport risques/avantages

../ Déterminer si les limites au principe de la protection de la vie privée et de la confidentialité sont acceptables au regard des attentes raisonnables des personnes concernées. Il est nécessaire d'entrer en contact avec elles afin de déterminer leurs attentes raisonnables.

../ Etablir si le projet de l'OIM est suffisamment important pour justifier des restrictions aux droits et intérêts des personnes concernées. L'importance du projet de l'OIM doit être déterminée sur la base du mandat de l'OIM et des circonstances entourant le projet de l'OIM comme, par exemple, la protection des personnes concernées, les mesures exigées par la communauté internationale, l'intérêt général, les atteintes aux droits de l'homme, des catastrophes naturelles, etc..

../ Etablir si les risques en matière de sécurité, de santé et de discrimination sont raisonnables par rapport aux avantages, et dans quelle mesure ces risques peuvent être réduits au minimum.

../ Tenir compte des circonstances particulières et des vulnérabilités des personnes concernées, et promouvoir la prise en considération du sexe, de l'âge, de la langue, et des comportements sociaux, culturels ou religieux du groupe de population cible ou de chacune des personnes concernées.

../ Veiller à ce que des garanties appropriées soient incluses dans le processus de collecte des données, afin de protéger les droits et le bien-être des personnes concernées susceptibles d'être exposées à la coercition ou à l'intimidation comme, par exemple, les mineurs, les détenus, les femmes enceintes, les personnes physiquement ou mentalement handicapées, ou les personnes concernées qui peuvent être défavorisées sur le plan économique ou éducatif.

../ Réexaminer régulièrement l'équilibre entre les risques et les avantages, afin de tenir compte de l'éventualité d'une modification du rapport risques/avantages.

../ Prévoir une formation adaptée pour le personnel de l'OIM et ceux qui participent à la collecte de données, et veiller à ce qu'ils connaissent les mesures de maîtrise des risques afin de réduire la probabilité d'un préjudice.

../ Analyser les effets des flux de données à caractère personnel sur les droits et les intérêts des personnes concernées tout au long du cycle de traitement des données.

Note : Lors de la mise en œuvre des mesures de sécurité des données, le responsable du traitement des données veillera à ce qu'elles réduisent les risques au minimum et maximisent les avantages.

Evaluation des risques à différentes phases du traitement des données : illustration

Collecte des données :
Les responsables du traitement des données doivent évaluer les risques pour la sûreté et la sécurité afin de déterminer la nature et l'étendue des données à caractère personnel devant être recueillies auprès de populations touchées par un conflit, par exemple lors de l'attribution d'abris, de la distribution de nourriture et de l'organisation des camps. Après avoir réalisé une évaluation objective, ils doivent faire le nécessaire pour réduire la probabilité qu'un risque survienne, et veiller à ce que les avantages continuent de l'emporter sur les risques. Les membres du personnel de l'OIM doivent être informés des précautions à prendre pour réduire la probabilité d'un préjudice, et le processus de collecte des données doit faire l'objet d'une surveillance constante.

Conservation des données :
Après l'enregistrement, il y a lieu de tenir compte des avantages d'un stockage des données à caractère personnel sur les sites et des risques liés à une divulgation non autorisée, pour garantir le stockage des données dans un lieu sûr. L'accès au site de stockage doit être limité aux personnes autorisées, et des mesures appropriées de sécurité des données doivent être prises pour prévenir le vol ou une divulgation non autorisée.

Qui sont les responsables du traitement des données ?

Les responsables du traitement des données sont des personnes habilitées à déterminer la façon dont les données à caractère personnel sont traitées.

Un projet de l'OIM peut requérir l'intervention d'un ou de plusieurs responsables du traitement des données, selon la nature et l'ampleur du projet, les ressources disponibles, les capacités du personnel, les stratégies de gestion du projet, les finalités déterminées de la collecte et du traitement des données, et les conditions de transfert, entre autres.

Les responsables du traitement des données peuvent être :

- les chefs de mission ;
- les administrateurs de projet ;
- les concepteurs de projet ;
- des personnes désignées ;
- des personnes représentant un tiers autorisé.

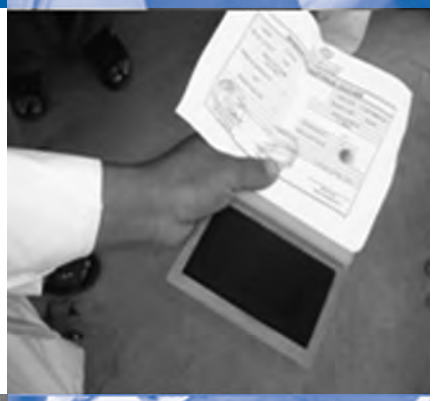
EXEMPLE :
Le représentant autorisé d'un établissement de recherche devient responsable du traitement des données dès le transfert de données à caractère personnel. Il est alors habilité à prendre les décisions requises pour réaliser les finalités déterminées de la recherche, telles qu'énoncées dans le contrat de transfert.

Les responsables du traitement des données doivent toujours se mettre dans la peau de la personne concernée et se poser la question suivante :

« Comment une personne raisonnable, dans la situation de la personne concernée, réagirait-elle à ces pratiques de collecte et de traitement des données ? »

1

PRINCIPE 1 : COLLECTE LICITE ET LOYALE



PRINCIPE 1 : COLLECTE LICITE ET LOYALE

Les données à caractère personnel doivent être obtenues à l'aide de procédés licites et loyaux au su de la personne concernée ou avec son consentement.

Les deux critères de licéité et de loyauté apparaissent dans tous les principes de l'OIM et ne sont pas limités à la collecte de données à caractère personnel. Une large place est accordée ici à la phase de la collecte car il s'agit de la première étape du traitement des données au cours de laquelle des données à caractère personnel sont utilisées.

3. Licéité

La collecte et le traitement de données à caractère personnel doivent être conformes aux principes de l'OIM, qui sont fondés sur les normes et instruments internationaux pertinents. La conformité avec la législation nationale régissant la protection des données ne doit pas être automatique.

La conformité ou non avec la législation nationale relative à la protection des données dépendra des circonstances de l'espèce et de la compatibilité de la loi en question avec les principes et lignes directrices de l'OIM. LEG doit être consulté au cas par cas, notamment en cas de conflit, d'incohérences ou de doute.

Le respect de la législation nationale relative à la protection des données ne doit pas aller à l'encontre des privilèges et immunités de l'Organisation. Ceux-ci varient d'un pays à l'autre, selon l'accord de statut conclu par l'OIM avec le gouvernement.

Il y a lieu de consulter systématiquement LEG avant de contracter des obligations qui pourraient avoir des effets sur le statut de l'OIM en tant qu'organisation intergouvernementale dans un pays donné[5].

EXEMPLE :

Il peut arriver qu'un contrat conclu avec un donateur exige le respect des normes nationales ou supranationales de protection des données. Tel est, de plus en plus souvent, le cas des contrats conclus avec l'Union européenne. Au cours de la phase d'examen du contrat, LEG relèvera toute obligation en matière de protection des données et, selon les circonstances, donnera des orientations sur la marche à suivre.

Concrètement, il appartient aux responsables du traitement des données de :

- S'informer sur les normes internationales en vigueur et la législation nationale relative à la protection des données du pays dans lequel a lieu l'intervention.
- Vérifier la compatibilité de la législation nationale relative à la protection des données avec les principes et lignes directrices de l'OIM.
- Sensibiliser les gouvernements, les donateurs, les partenaires de l'OIM, les partenaires d'exécution, les agents (fournisseurs de services/consultants) et d'autres tiers, et stimuler la coopération avec eux.
- Evaluer la capacité juridique et l'aptitude des personnes concernées à donner leur consentement.
- Tenir compte des contraintes pratiques risquant d'empêcher l'obtention du consentement.
- Toujours consulter LEG.

Encadré 6 : Considérations juridiques

- Conformité avec le droit international des droits de l'homme ;
- Lois nationales ou supranationales portant atteinte aux principes de l'OIM ;
- Privilèges et immunités de l'OIM dans le pays dans lequel elle intervient, s'il y a lieu ;
- Dispositions relatives au consentement et à la confidentialité incluses dans les formulaires d'entretien, d'enregistrement et de demande, ainsi que dans les contrats de transfert ;
- Principes pertinents de l'OIM repris dans les contrats écrits conclus avec les agents (fournisseurs de services/consultants), les donateurs, les partenaires de l'OIM, les partenaires d'exécution, les organismes publics, les institutions universitaires et d'autres tiers.

[5] Les privilèges et immunités de l'Organisation ayant un rapport avec la protection des données/le droit national sont, entre autres, l'immunité à l'égard de toute procédure judiciaire (immunité de juridiction), et l'inviolabilité des archives de l'OIM et de tous les documents qu'elle détient ou possède, où qu'ils se trouvent.

4. Loyauté

La quantité de données à caractère personnel doit être limitée à ce qui est nécessaire pour atteindre la finalité déterminée de la collecte et du traitement des données.

Elle dépendra :

- de l'urgence et de la sécurité légitime du projet de l'OIM ; et
- de la proportionnalité entre la quantité de données à caractère personnel collectées et les objectifs du projet de l'OIM.

L'application de ces deux critères variera d'un cas à l'autre, selon la sensibilité des données à caractère personnel et le contexte dans lequel celles-ci sont collectées et traitées.

La collecte de données à caractère personnel doit toujours répondre au « besoin d'en connaître ».

Avant toute collecte, les responsables du traitement des données détermineront :

- les catégories de données à caractère personnel qui sont nécessaires pour atteindre la finalité déterminée initiale ; et
- les catégories additionnelles requises pour une utilisation prévisible, qui sont compatibles avec la finalité déterminée initiale et susceptibles d'être nécessaires au cours du cycle de traitement des données[6].

Encadré 7 : Considérations en matière de loyauté

- Limiter la quantité de données à caractère personnel au strict minimum, en tenant compte de l'urgence et de la nécessité légitime du projet de l'OIM, et en évaluant le rapport de proportionnalité entre la quantité de données à caractère personnel collectées et les objectifs du projet de l'OIM.
- Susciter une attente légitime de confidentialité en indiquant et en expliquant clairement :
  - les finalités déterminées de la collecte et du traitement des données ;
  - l'utilisation prévisible, les flux internes au sein de l'OIM, les méthodes de stockage et toutes les divulgations prévisibles à des tiers.
- Maximiser la loyauté en tenant compte des comportements sociaux, culturels et religieux, ainsi que des problèmes environnementaux.
- Veiller à ce que les méthodes de collecte tiennent compte des sexospécificités, des particularités culturelles, et des sensibilités liées à l'âge.
- Réduire au minimum le degré d'intrusion en utilisant la méthode de collecte la moins importune.
- Informer les personnes concernées et les parties prenantes du projet des principes de l'OIM.

Note : Toujours privilégier la sincérité et la coopération.

Pour satisfaire à l'exigence de loyauté, il faut de solides garanties de confidentialité d'un bout à l'autre du processus de collecte des données, et les personnes concernées doivent être clairement informées de la finalité déterminée initiale, des finalités déterminées additionnelles et de toute divulgation prévisible.

5. Processus de collecte

Les données à caractère personnel doivent être collectées aussi rapidement que possible, sans intimidation et dans le respect de la sécurité et de la dignité des personnes concernées.

[6] Les finalités déterminées doivent être clairement définies selon la portée et les objectifs du projet particulier de l'OIM. L'utilisation prévisible doit être définie en fonction de l'aide pouvant être apportée à la personne concernée tout au long du cycle de traitement des données.

Communication permanente

La communication avec les personnes concernées doit être encouragée à toutes les étapes du processus de collecte des données. Cela sensibilisera l'ensemble de la communauté au projet de l'OIM et éveillera sa confiance.

Egalité de traitement

Les sexospécificités, les particularités culturelles et les sensibilités liées à l'âge doivent être prises en considération dans le processus de collecte des données, et les mêmes règles doivent s'appliquer à chacune des personnes concernées.

Des différences de traitement peuvent se justifier lorsqu'il est nécessaire d'évaluer les besoins de certaines personnes concernées, et pour expliquer correctement le processus de collecte des données aux personnes concernées.

Les enquêteurs qui demandent et collectent des données à caractère personnel doivent, en tout temps, respecter leur caractère confidentiel. Dans la mesure du possible, ces données doivent être recueillies directement auprès de la personne concernée, c.-à-d. directement auprès des femmes et des hommes, des filles et des garçons.

Des facteurs sociaux, culturels, religieux, linguistiques, environnementaux ou liés à l'âge ou à la santé, ou une simple impossibilité pratique peuvent toutefois faire obstacle à un échange direct entre l'enquêteur et la personne concernée.

Dans ces cas exceptionnels, les données à caractère personnel peuvent être recueillies auprès de proches, de membres autorisés de la communauté ou de l'entourage. En cas de conflit entre le représentant et la personne concernée, l'opinion de la personne concernée prévaudra. En tout état de cause, l'intérêt supérieur de la personne concernée reste primordial.

EXEMPLE :

Lorsque de nombreuses données à caractère personnel sont collectées, des discussions en groupe pourraient, par exemple, permettre d'identifier plus facilement les diverses croyances, idées et opinions collectives du groupe de population visé. Ces discussions peuvent servir un double objectif : renforcer l'adhésion au principe de protection des données et améliorer la véracité et la qualité des données à caractère personnel.

EXEMPLE :

En tenant dûment compte de l'unité familiale, il pourrait être utile, pour évaluer les besoins et définir des méthodes de collecte appropriées, de séparer les membres d'un grand groupe de population cible en fonction de l'âge et du sexe. Une fois que les paramètres ont été définis et les besoins évalués, la procédure de collecte doit être équitable et loyale.

EXEMPLE :

Lors de catastrophes naturelles, des données à caractère personnel peuvent être recueillies auprès de représentants autorisés, tels que le chef de famille ou d'autres chefs familiaux ou communautaires. Les données à caractère personnel recueillies auprès de représentants doivent toutefois être vérifiées avec la personne concernée dès que le danger imminent s'est éloigné et qu'il est possible d'organiser des réunions de communautés ou des contrôles sur place.

Si des circonstances exceptionnelles empêchent les personnes concernées d'être présentes sur le lieu de collecte de données, des mesures seront prises pour qu'elles puissent valider leurs données à caractère personnel dès que possible.

Méthode de collecte des données

Les données à caractère personnel doivent être recueillies dans un environnement sûr. Les responsables du traitement des données doivent faire le nécessaire pour ne pas accentuer les vulnérabilités individuelles et les risques potentiels.

La méthode de collecte des données variera selon :

- le contexte particulier ;
- le type de projet de l'OIM ;
- l'aide requise ;
- la stratégie de gestion du projet ;
- les capacités du personnel ; et
- les ressources disponibles.

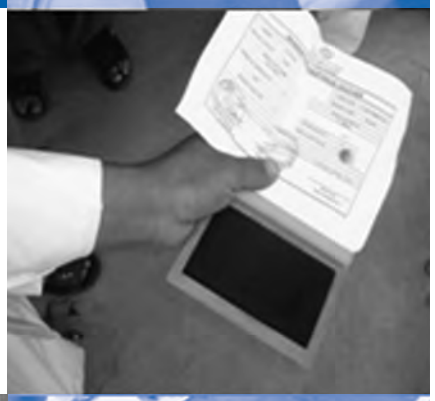
Les responsables du traitement des données choisiront la méthode de collecte la mieux à même d'améliorer l'utilité des données à caractère personnel collectées et de protéger leur caractère confidentiel.

EXEMPLE :

Dans les situations d'urgence, il est rare que des données à caractère personnel soient recueillies au début de la crise. Lorsque commence la collecte, quatre phases peuvent être distinguées : 1) la planification, l'organisation et l'information des migrants ; 2) la distribution de jetons nécessaires pour obtenir une carte d'enregistrement ; 3) la collecte d'informations détaillées et de documents, et la délivrance de cartes d'enregistrement ; et 4) l'analyse, la vérification et la mise à jour des informations. Selon le contexte, la stratégie de gestion du projet, les ressources disponibles et les capacités du personnel, des kits d'enregistrement mobiles peuvent être utilisés pour saisir des données sur place au cours de la troisième phase.

2

PRINCIPE 2 :
FINALITE DETERMINEE ET LEGITIME



PRINCIPE 2 : FINALITE DETERMINEE ET LEGITIME

La ou les finalités de la collecte et du traitement de données à caractère personnel doivent être déterminées et légitimes, et être connues de la personne concernée au moment de la collecte. Des données à caractère personnel ne seront utilisées qu'en vue de la ou des finalités déterminées, sauf si la personne concernée consent à une autre utilisation ou si ladite utilisation est compatible avec la ou les finalités déterminées initiales.

La collecte de données à caractère personnel doit être effectuée de manière réfléchie, et la finalité déterminée de la collecte et du traitement des données doit être clairement expliquée aux personnes concernées.

6. Finalité déterminée et légitime

La finalité déterminée doit être clairement énoncée et justifiée par la nécessité de répondre au besoin légitime du projet de l'OIM. Ce besoin légitime doit être défini par le responsable du traitement des données compte tenu des objectifs du projet de l'OIM et des intérêts que celui-ci cherche à promouvoir.

Des données à caractère personnel ne doivent servir qu'à atteindre la ou les finalités déterminées, et ne sauraient être utilisées ultérieurement pour des finalités totalement différentes sans le consentement de la personne concernée.

Cette restriction est un élément fondamental de la protection des données, qui vise à promouvoir le principe de loyauté et prévenir toute « dérive fonctionnelle », à savoir toute autre utilisation de données à caractère personnel qui s'écarte de la finalité énoncée initialement et des attentes de la personne concernée.

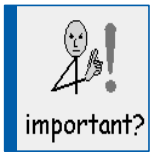
La finalité initiale et les finalités additionnelles prévisibles doivent être définies et décrites avant la collecte des données, ce qui permettra aux responsables du traitement des données de reconnaître les catégories de données à caractère personnel requises.

La finalité déterminée doit toujours apporter une valeur ajoutée, et des données à caractère personnel doivent être utilisées dans l'intérêt de la dignité et de l'autonomie des personnes concernées.

EXEMPLE :

L'utilisation de données biométriques doit être limitée à la finalité énoncée. La finalité déterminée de la sécurité nationale ne doit pas conduire à une utilisation arbitraire de données biométriques, qui pourrait engendrer des discriminations injustifiées ou limiter le droit des migrants de circuler librement et en toute légalité.

Les personnes concernées doivent être informées des conséquences éventuelles d'un refus de communiquer certaines catégories de données à caractère personnel, y compris des incidences possibles d'un tel refus sur les services et l'aide qui pourraient leur être fournis.



Les formulaires d'entretien, d'enregistrement ou de demande doivent comprendre une clause qui énonce les finalités déterminées, et le contenu des formulaires doit être clairement expliqué aux personnes concernées au moment de la collecte des données[7].

[7] Voir le Modèle 1.2 pour une autorisation type du bénéficiaire pour participer à des projets de l'OIM.

Il y a lieu de signaler aux personnes concernées toute modification ultérieure apportée à la finalité déterminée initiale en raison de circonstances imprévues.

La mesure dans laquelle la finalité déterminée a changé permet de décider s'il suffit d'en informer les personnes concernées pour poursuivre les activités de traitement des données.

../ ***Changement minime*** : Malgré le changement, le traitement des données reste compatible avec la finalité déterminée initiale.

../ ***Changement important*** : La poursuite du traitement des données requiert le consentement ultérieur de la personne concernée. Dans ces conditions, les responsables du traitement des données ne continueront à traiter que les données à caractère personnel des personnes concernées qui ont consenti à la nouvelle finalité déterminée.

EXEMPLE :

S'il est impossible de contacter la personne concernée, toutes les dispositions raisonnables doivent être prises pour communiquer de manière générale tout changement important au groupe de population cible, par exemple à la faveur d'une campagne publique, d'un message radiophonique, d'une publication sur Internet ou d'une distribution de brochures.

7. Finalités secondaires compatibles

La notion de finalité secondaire compatible renvoie à l'utilisation de données à caractère personnel pour des finalités se rattachant à la finalité déterminée initiale.

Ces finalités sont fondées sur la nécessité d'atteindre la finalité déterminée initiale et recouvrent des finalités imprévues qui sont étroitement liées à la finalité déterminée initiale.

Il y a lieu d'informer les personnes concernées que leurs données à caractère personnel pourraient être utilisées et divulguées pour des finalités connexes visant à atteindre la finalité déterminée initiale.

Contrôle de compatibilité

Ce contrôle consiste à déterminer s'il est raisonnable de supposer que les personnes concernées s'attendent à ce que leurs données à caractère personnel soient utilisées de la façon envisagée, même si l'utilisation envisagée n'a pas été exposée au moment de la collecte des données.

Pour qu'il y ait compatibilité, il doit exister un lien raisonnable et direct entre la finalité déterminée initiale et la finalité secondaire.

Les finalités secondaires compatibles qui apparaissent pendant la période de conservation des données sont, entre autres :

../ ***Des finalités lo stiques t administratives,*** nécessaires pour réaliser la finalité déterminée initiale.

../ ***L'externalisation d'activités de projet*** à des tiers qui entretiennent déjà des relations avec l'OIM, par exemple la communication de données à caractère personnel à des fournisseurs de services non prévus.

../ ***La fourniture d'une aide continue*** par une unité/un département de l'OIM dans l'intérêt de la même personne concernée.

Encadré 8 : Considérations en matière de compatibilité

- Attentes raisonnables des personnes concernées ;
- Rapport entre la finalité déterminée initiale et la finalité secondaire ;
- Nature et portée des données à caractère personnel utilisées ou divulguées en vue de la finalité secondaire ;
- Conséquences pour les droits et les intérêts des personnes concernées ;
- Mesure dans laquelle des garanties appropriées protégeraient la confidentialité des données à caractère personnel et l'anonymat de la personne concernée.

Note : Toujours veiller à limiter la quantité de données à caractère personnel utilisées et divulguées en vue de finalités secondaires à ce qui est nécessaire pour mener l'activité connexe spécifique indispensable pour atteindre la finalité déterminée initiale.

../ ***Le repérage de mouvements migratoires,*** s'il est nécessaire pour déterminer l'opportunit d'une assistance de la part de l'OIM.

../ ***L'analyse détaillée des antécédents,*** si elle est nécessaire pour identifier les vulnérabilités des personnes concernées.

../ ***La recherche et l'analyse en matière de migration*** qui promeuvent l'expertise de l'OIM concernant les questions de migration et qui entrent dans l'une des catégories de recherche sur la migration énumérées plus loin.

EXEMPLE :

L'analyse des antécédents spécifiques et le repérage des mouvements migratoires d'une personne concernée pour savoir si elle a bénéficié de multiples projets de retour volontaire assisté constitueraient une finalité secondaire compatible.

8. Continuum de l'aide

La notion de continuum de l'aide s'entend de l'utilisation ultérieure de données à caractère personnel dans l'intérêt de la même personne concernée.

Ces finalités additionnelles doivent être définies et expliquées aux personnes concernées au moment de la collecte des données.

Au moment de la collecte des données, les responsables du traitement des données doivent s'efforcer d'obtenir le consentement de la personne concernée à un continuum de l'aide.

En l'absence de consentement, la question doit être renvoyée à LEG et à l'unité/au département compétent de l'OIM, surtout si les responsables du traitement des données ont de bonnes raisons de croire que l'utilisation de données à caractère personnel pour une finalité ultérieure serait nécessaire pour protéger la vie ou la sécurité de la personne concernée.

9. Recherche compatible

Rapprochement des données

Le rapprochement des données s'entend de la comparaison électronique de deux ensembles ou plus de données à caractère personnel recueillies pour des finalités déterminées différentes.

Le rapprochement de données interne, au sein de l'Organisation, peut être autorisé si le consentement a été obtenu au moment de la collecte des données ou s'il est compatible avec les finalités déterminées initiales pour lesquelles les données à caractère personnel ont été recueillies et traitées.

Les responsables du traitement des données doivent toujours :

- évaluer la faisabilité du rapprochement des données proposé ;
- analyser les incidences potentielles sur les principes de l'OIM ; et
- mettre en place les garanties nécessaires pour limiter l'accès, l'utilisation et la divulgation de données à caractère personnel.

EXEMPLE :

Si le système MiMOSA (Application relative aux systèmes opérationnels et de gestion des migrants) est utilisé pour comparer et clarifier des données à caractère personnel non concordantes, le rapprochement de données interne doit être limité à l'élucidation des écarts entre les deux ensembles de données indépendants.

Les applications de bases de données centrales qui servent au stockage de données à caractère personnel recueillies dans le cadre de projets indépendants de l'OIM doivent faire l'objet d'une surveillance stricte afin de garantir des contrôles d'accès stricts et d'empêcher toute utilisation abusive de données à caractère personnel à des fins de rapprochement de données arbitraire.

Des données à caractère personnel ne peuvent être communiquées à des tiers aux fins de rapprochement, sauf disposition contractuelle expresse, auquel cas toutes les parties contractantes se conforment strictement aux principes de l'OIM.

Recherche sur la migration au sein de l'OIM

L'utilisation, par l'OIM, de données à caractère personnel à des fins de recherche sur la migration et d'analyse peut être autorisée pendant la période de conservation des données, à condition que les responsables du traitement des données fixent des conditions strictes d'accès et de divulgation.

Les catégories de recherches par l'OIM sur la migration[8] énoncées ci-après sont réputées compatibles avec les principes de l'OIM, et ne requièrent donc pas le consentement ultérieur de la personne concernée.

- Approfondir la compréhension des réalités migratoires et analyser les causes profondes de la migration.
- Promouvoir des pratiques exemplaires et préserver la dignité humaine et le bien-être des migrants.
- Encourager le développement social et économique en vue de maximiser les avantages de la migration.
- Offrir des conseils spécialisés aux parties prenantes et faciliter la coopération sur les questions de migration.
- Aider à relever les défis opérationnels croissants que pose la gestion des migrations.

EXEMPLE :

Pour dégager les tendances migratoires dans une région géographique donnée, l'administrateur de projet de l'OIM chargé d'une nouvelle recherche/enquête doit demander au responsable du traitement des données à caractère personnel compétent l'autorisation d'accéder à des données à caractère personnel et de les utiliser. Après avoir évalué le rapport risques/avantages, celui-ci décidera s'il y a lieu d'autoriser cet accès. Si les avantages l'emportent sur les risques, le responsable du traitement des données mettra en place des contrôles d'accès appropriés et des restrictions quant à l'utilisation future des données, opposables aux membres du personnel de l'OIM non autorisés.

Concrètement, il y a lieu de procéder comme suit :

> Le chercheur de l'OIM soumet une demande précisant l'objet de la recherche sur la migration au responsable du traitement des données associé au projet de l'OIM pour lequel des données à caractère personnel avaient été initialement recueillies et traitées.
> Le responsable initial du traitement des données réalise une évaluation du rapport risques/avantages pour savoir s'il y a lieu ou non d'autoriser l'accès aux données à caractère personnel et leur utilisation.
> Le responsable initial du traitement des données détermine si la demande de recherche entre dans les catégories de recherche sur la migration précitées, ce qui lui permet d'être considérée comme une finalité « compatible » ne nécessitant pas le consentement de la personne concernée.
> La confidentialité des données à caractère personnel et l'anonymat des personnes concernées doivent être préservés en cas de publication des conclusions des travaux de recherche et d'analyse.

10. Finalité de recherche additionnelle

Toute finalité de recherche additionnelle qui n'entre pas dans les catégories de recherche sur la migration précitées requiert le consentement ultérieur de la personne concernée, si celui-ci n'a pas été obtenu au moment de la collecte de données.

Si des finalités de recherche additionnelles sont connues avant la collecte des données, elles doivent être mentionnées dans les formulaires d'entretien, d'enregistrement et de demande.

Les conditions de transfert énoncées au Principe 5 s'appliquent à tout projet de recherche additionnel qui utilise des données à caractère personnel recueillies dans le cadre d'un projet de l'OIM donné et qui n'entre pas dans les catégories de recherche sur la migration précitées. Par ailleurs, de tels projets de recherche additionnels sont soumis à l'approbation du responsable du traitement des données associé au projet de l'OIM pour lequel les données à caractère personnel avaient été initialement recueillies et traitées, ainsi qu'à celle de l'unité/du département compétent de l'OIM.

Encadré 9 : Considérations en matière de recherche

- Réduire les dommages corporels ainsi que la détresse sociale et psychologique au minimum.
- Garantir l'honnêteté et la transparence.
- Décrire clairement la nature de la recherche, le rôle escompté des personnes concernées, et les modalités de recherche retenues.
- Considérer les personnes concernées comme des sujets de recherche autonomes.
- Décrire de manière claire et intelligible la finalité déterminée de la recherche et les objectifs plus larges.
- Obtenir le consentement volontaire exprès lors de la collecte des données ou dès que la finalité déterminée de la recherche a été identifiée. Si possible, le consentement sera donné par écrit.
- Préserver la confidentialité des données à caractère personnel et l'anonymat des personnes concernées en cas de publication des conclusions des travaux de recherche et d'analyse.
- Promouvoir le recours à des mesures garantissant la sécurité des données qui s'accordent avec les modalités de recherche adoptées.
- Veiller à la protection des données d'un bout à l'autre du projet de recherche.

Les responsables du traitement des données associés à des projets de recherche veilleront à ce que le thème de la recherche soit clair et à ce que les principes de l'IOM ne soient pas mis en péril. Des modalités de recherche appropriées seront adoptées en concertation avec l'Unité de recherche au Siège pour éviter que les méthodes utilisées pour garantir la confidentialité des données ne nuisent à l'exactitude et à la validité de l'étude.

[8] Ces catégories sont définies en regard de la stratégie et des objectifs de l'OIM. Pour plus d'informations, voir l'édition 2010 de *Migration Initiatives*, OIM, Genève.

Le *Manuel de recherche de l'OIM*[9] donne des orientations sur les principes éthiques à prendre en compte lors de la recherche, de la mise en œuvre de stratégies de gestion de projets, et de la rédaction de rapports de projet.

Les chercheurs intégreront la protection des données dans les modalités de recherche afin de prévenir les risques et les éventuelles violations de la confidentialité pouvant résulter, entre autres, de recherches comportementales, sociales, biomédicales ou épidémiologiques.

Il peut être utile de désigner des personnes chargées de superviser les propositions de recherche et de veiller à leur conformité avec les normes éthiques liées aux diverses activités de l'OIM.

EXEMPLE :

Diverses disciplines sont régies par des principes éthiques. Par exemple, la déontologie médicale exige la confidentialité du rapport médecin-patient ; l'aide directe aux victimes de la traite requiert un traitement et des soins individualisés ; la déontologie des médias exige d'être exact et de valider ses sources ; quant à l'éthique de la recherche, elle exige de prévenir les conséquences néfastes qui pourraient résulter d'une participation à une étude.

Propositions de recherche

L'analyse aux fins d'élaboration de propositions de recherche doit, si possible, être limitée à des données anonymes. L'utilisation de données à caractère personnel dans le cadre de stratégies d'élaboration de projets exige le consentement exprès des personnes concernées, sauf si cette utilisation est compatible avec la finalité déterminée initiale ou les finalités déterminées ultérieures pour lesquelles le consentement a été obtenu.

Les membres du personnel de l'OIM et les tiers autorisés qui effectuent des recherches en utilisant des données à caractère personnel recueillies par l'OIM ou en son nom doivent signer un formulaire de confidentialité.

Un engagement de confidentialité est une garantie nécessaire qui vise à :

- protéger l'anonymat des personnes concernées ;
- préserver la confidentialité des données à caractère personnel ; et
- faire en sorte que des éléments identifiables ne soient pas utilisés à des fins arbitraires.

Le consentement exprès de la personne concernée est requis en cas de divulgation de données à caractère personnel à des tiers qui ne sont pas associés à des projets de recherche[10].

EXEMPLE :

Les donateurs et les partenaires de l'OIM associés à des projets de recherche doivent être informés des principes de l'OIM pendant la phase d'élaboration des projets, de façon que les projets de recherche soient assortis de garanties appropriées et que les clauses contractuelles ne nuisent pas à la protection des données.

Recherche d'intérêt général

Des recherches d'intérêt général qui ne faisaient pas partie de la finalité déterminée initiale et ne relèvent pas des catégories de recherche sur la migration précitées sont soumises à l'approbation de LEG et de l'unité/du département compétent de l'OIM, qui soupèseront divers éléments pour déterminer si l'intérêt général auquel contribuerait la promotion de la recherche l'emporte dans une large mesure sur le droit au respect de la vie privée et de la confidentialité des données à caractère personnel.

[9] Pour plus d'informations sur l'éthique de la recherche, voir l'édition 2004 du *Manuel de recherche de l'OIM*, OIM, Genève.

Publications de recherche

La présentation et le contenu des publications de recherche doivent rendre impossible l'identification des personnes concernées. La divulgation d'analyses et de travaux de recherche sera, dans la mesure du possible, limitée aux données anonymes. A moins que les personnes concernées n'acceptent expressément d'être identifiées, leur anonymat doit être préservé.

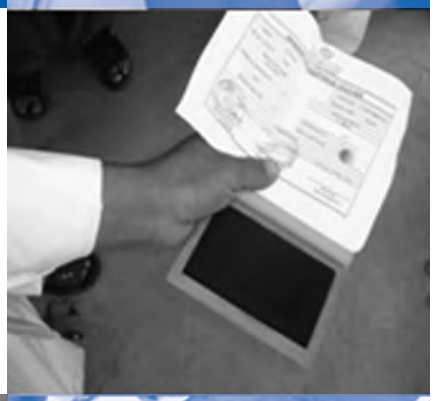
EXEMPLE :

Toutes les mesures nécessaires doivent être prises pour empêcher de remonter à la source de la recherche. Par exemple, les noms peuvent être protégés par des pseudonymes, et d'autres éléments identifiables peuvent être remplacés par des données fictives.

[10] La divulgation à des tiers doit être limitée au strict minimum. Voir le Principe 5 pour un aperçu des trois conditions applicables au transfert à des tiers : le consentement exprès de la personne concernée, la finalité déterminée du transfert, et des garanties appropriées.

3

PRINCIPE 3 : QUALITE DES DONNEES



PRINCIPE 3 : QUALITE DES DONNEES

Les données à caractère personnel demandées et obtenues doivent être adéquates, pertinentes et non excessives au regard de la ou des finalités déterminées pour lesquelles elles sont collectées et traitées. Les responsables du traitement des données prendront toutes les dispositions raisonnables pour que les données à caractère personnel soient exactes et à jour.

La quantité et la qualité des données à caractère personnel doivent être suffisantes pour atteindre les finalités déterminées. La quantité de données à caractère personnel recueillies ne doit pas excéder ce qui est objectivement nécessaire pour atteindre les finalités déterminées.

La nécessité objective dépend :

- des objectifs du projet particulier de l'OIM ;
- de la nature et de la portée des données à caractère personnel requises pour atteindre les finalités déterminées ; et
- des attentes des personnes concernées.

Des catégories additionnelles de données à caractère personnel peuvent être recueillies si leur utilisation ultérieure est compatible avec la finalité déterminée initiale, ou si le consentement a été obtenu pour une finalité déterminée future. La finalité déterminée future doit être fondée sur un continuum d'aide au profit de la personne concernée.

EXEMPLE :

Si la collecte de données sur les études et les antécédents professionnels n'est pas nécessaire pour traiter des demandes de retour volontaire assisté, elle peut toutefois être utile en cas d'aide supplémentaire à la réintégration, telle que la formation professionnelle.

11. Mesures visant à garantir l'exactitude des données

L'exactitude est de rigueur tout au long du cycle de traitement des données, et elle doit être vérifiée lors des phases de collecte, d'enregistrement, d'extraction, d'utilisation et de divulgation. La fréquence de vérification des données à caractère personnel dépendra des capacités du personnel et d'une formation régulière, de façon que les données à caractère personnel soient correctement enregistrées aux différentes étapes de leur traitement.

EXEMPLE :

Les données à caractère personnel stockées dans la base de données du module de lutte contre la traite (CTM) doivent être corrigées par le personnel autorisé du bureau extérieur de l'OIM intéressé, sur instruction du responsable du traitement des données. Le personnel de l'OIM chargé de la gestion de la base de données CTM doit être informé de tout changement important.

Le bureau extérieur de l'OIM associé à la collecte et au traitement de données à caractère personnel restera le point de repère en cas de changements importants, si les données à caractère personnel sont stockées dans un dépôt central de bases de données.

Il incombe aux responsables du traitement des données de créer une « culture du contrôle minutieux » car un mauvais enregistrement de données à caractère personnel peut avoir des incidences sur la fourniture de services. Des dispositions raisonnables seront prises pour réduire au minimum la possibilité de prendre une décision sur la base de données inappropriées et erronées.

EXEMPLE :

Si un pays d'accueil impose des restrictions fondées sur l'état de santé, l'enregistrement erroné de la sérologie VIH pourrait avoir des incidences sur la procédure d'approbation des demandes de réinstallation.

Les moyens permettant de vérifier l'exactitude des données sont notamment :

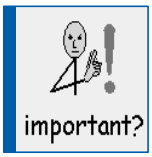
../ ***La surveillance*** de la procédure de collecte.

../ ***La validation*** des catégories de données à caractère personnel.

../ ***La double vérification,*** avant l'enregistrement et lors de la conversion des documents papier en fichiers électroniques.

../ ***La vérification préalable,*** avant l'utilisation et la divulgation.

../ ***L'établissement de rapports réguliers et la surveillance permanente,*** d'un bout à l'autre du cycle de traitement des données.



Afin de surveiller régulièrement la qualité des données, des listes de vérification doivent être distribuées au personnel de l'OIM et aux tiers autorisés qui traitent des données à caractère personnel[11].

Intégrité et véracité

L'exactitude va de pair avec l'intégrité et la véracité des données à caractère personnel. Les enquêteurs doivent être formés pour pouvoir vérifier que les catégories de données à caractère personnel fournies par les personnes concernées sont vraies et correctes.
Si possible, des séances d'information seront organisées avant la collecte de données pour sensibiliser les enquêteurs à l'importance d'obtenir et d'enregistrer des données à caractère personnel exactes, et pour que la participation des personnes concernées au processus de collecte de données ne les expose pas à des risques physiques, à des actes d'intimidation ou à d'autres menaces qui les amèneraient à communiquer de fausses informations.

Encadré 10 : Mesures raisonnables permettant de garantir l'exactitude des données

- Assurer aux personnes concernées que leurs données à caractère personnel seront traitées avec le plus grand soin et en toute confidentialité.
- Expliquer les conséquences qu'entraîne la communication de données à caractère personnel incorrectes.
- Vérifier la véracité et l'exactitude des données au moment de leur collecte.
- Examiner les catégories de données à caractère personnel et en vérifier l'exactitude lors de l'extraction des données.
- Vérifier l'exactitude des données à caractère personnel avant leur utilisation et leur divulgation.
- Examiner le format et le support des dossiers électroniques et transférer les données sur un support compatible.
- Se concerter avec l'informaticien compétent pour mettre à jour le matériel et/ou les logiciels.
- Examiner le dispositif de stockage et le volume des dossiers papier, et envisager de les scanner si c'est économiquement rentable.
- Effectuer des évaluations trimestrielles ou annuelles de l'exactitude des données, selon la durée du projet de l'OIM.
- Réaliser l'inventaire des dossiers papier et électroniques.

Note : Créer une « culture du contrôle minutieux » et toujours permettre aux personnes concernées de mettre à jour et de rectifier à tout moment leurs données à caractère personnel.

Mises à jour

Les responsables du traitement des données doivent offrir aux personnes concernées la possibilité de mettre à jour, à tout moment, leurs données à caractère personnel. Toute modification importante de données à caractère personnel doit être consignée avec exactitude dans les dossiers papier et électroniques. Dès qu'il a connaissance d'une modification importante de données à caractère personnel, le responsable du traitement des données en informera tout membre du personnel de l'OIM et tout tiers autorisé traitant des données à caractère personnel.

EXEMPLE :

Afin de permettre les mises à jour, les personnes concernées pourraient être invitées à communiquer, dans un délai imparti, tout ajout, changement ou rectification dans leurs données à caractère personnel, par exemple en distribuant des brochures, en diffusant un message sur Internet ou en informant oralement les personnes concernées de leur droit à rectification ou modification.

Compatibilité technologique

Les dossiers électroniques doivent être conservés sous les formats les plus récents, les plus courants et les plus fiables. Des supports électroniques obsolètes peuvent entraîner une altération du contenu des données à caractère personnel, voire la perte de données pour cause d'obsolescence technologique. Les supports électroniques, les matériels et/ou les logiciels doivent être régulièrement mis à jour et être conformes aux normes de l'OIM en matière de technologie de l'information et des communications (ITC).

Les responsables du traitement des données vérifieront régulièrement les supports électroniques pour s'assurer que les données à caractère personnel sont conservées sous un format lisible. Les bandes électroniques, les disquettes, les applications Flash Media et les bases de données obsolètes doivent être mises à niveau dans une version récente compatible avec la dernière technologie de l'information utilisée dans le bureau extérieur de l'OIM concerné.

EXEMPLE :

Conformément aux normes ITC, les bureaux extérieurs de l'OIM devront inscrire au budget des crédits pour la mise à niveau du matériel et/ou des logiciels pendant la quatrième année du cycle de vie du bien informatique.

Toutes les versions obsolètes doivent être détruites dès lors qu'elles ne sont plus nécessaires. Les dossiers électroniques seront régulièrement vérifiés afin de réduire le risque d'erreur humaine, et les responsables du traitement des données corrigeront sans retard les divergences et les inexactitudes.

Les responsables du traitement des données préserveront l'intégrité des dossiers électroniques en concertation avec l'informaticien compétent.

[11] Voir la liste de vérification 1 contenant un modèle de liste de vérification concernant la qualité des données.

Stockage sûr des dossiers papier

Pour protéger l'intégrité des données à caractère personnel, tous les dossiers papier et les justificatifs seront stockés en sécurité et sous clé dans un coffre, une armoire, un tiroir ou une pièce afin d'en prévenir la détérioration, la falsification, la manipulation ou le vol. Les données à caractère personnel qui sont archivées ou conservées à des fins de sauvegarde seront réputées exactes dès lors qu'elles sont exactes au moment de leur stockage.

EXEMPLE :

En cas de déménagement ou de fermeture d'un bureau, un inventaire pourrait être l'occasion d'apposer sur les documents papier la mention « confidentiel » et de s'assurer que tous les documents électroniques sont chiffrés pour qu'ils puissent être transférés en toute sécurité au personnel autorisé des bureaux régionaux de l'OIM ou du Siège, ou dans les nouveaux locaux.

Cession de données à caractère personnel

La cession et la circulation de données à caractère personnel feront l'objet d'une surveillance rigoureuse, afin que la qualité et la confidentialité des données soient protégées à tout moment.

Les responsables du traitement des données dresseront l'inventaire des supports électroniques et des dossiers papier utilisés pour conserver des données à caractère personnel.

Un tel inventaire facilitera la cession de données à caractère personnel à de nouveaux responsables du traitement des données, ainsi que la définition de stratégies de gestion en vue de l'adoption des mesures techniques et organisationnelles nécessaires pour permettre la circulation sûre et rapide de données à caractère personnel. Cet inventaire peut aussi servir aux informaticiens compétents lorsqu'ils mettent à niveau les supports électroniques, les bases de données, ainsi que les matériels et/ou logiciels.

12. Mesures permettant de garantir la pertinence des données

Les responsables du traitement des données vérifieront régulièrement si certaines catégories de données à caractère personnel sont nécessaires et pertinentes. Des données à caractère personnel inappropriées, obsolètes ou sans intérêt doivent être détruites après consultation de l'unité/du département compétent de l'OIM.

Pour déterminer la pertinence des données, il est possible de séparer les « données actives » des « données inactives ».

Des motifs suffisants doivent être invoqués pour justifier la pertinence et la conservation de « données inactives », et doivent figurer dans les rapports de projet ou dans les rapports soumis aux fins de contrôle.

EXEMPLE :

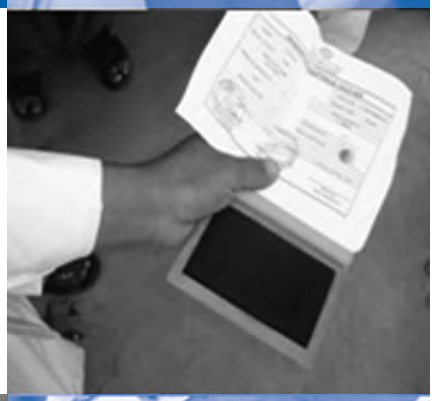
Des « données inactives » pourraient être conservées pendant une période déterminée afin d'examiner le bien-fondé de demandes d'indemnisation. Au terme du délai prescrit, ces « données inactives » doivent être détruites si elles sont sans intérêt ou obsolètes.

Encadré 11 : Détermination de la pertinence

- Des inexactitudes ont-elles altéré la qualité de données à caractère personnel ?
- Des mises à jour ou des changements importants ont-ils rendu inutiles les données à caractère personnel initialement enregistrées ?
- Dans quelle mesure les données initialement enregistrées peuvent-elles encore apporter une valeur ajoutée aux objectifs du projet de l'OIM, et vaut-il la peine de continuer à les conserver ?
- La situation de la personne concernée a-t-elle changé, et les nouveaux éléments rendent-ils les données initialement enregistrées obsolètes et sans intérêt ?
- Est-il possible de séparer les « données actives » des « données inactives », et suffisamment de temps s'est-il écoulé au point que les « données inactives » ne présentent plus d'intérêt ?
- Les données sans intérêt et inutiles peuvent-elles être utilisées à des fins statistiques ou de recherche compatibles avec la finalité déterminée pour laquelle les données à caractère personnel avaient été collectées ?

4

PRINCIPE 4 : CONSENTEMENT



PRINCIPE 4 : CONSENTEMENT

Le consentement doit être obtenu au moment de la collecte ou dès que possible ultérieurement, compte dûment tenu de l'état de santé et de la capacité juridique de certains groupes et personnes vulnérables. Si des circonstances exceptionnelles ne permettent pas d'obtenir le consentement, le responsable du traitement des données veillera au moins à ce que la personne concernée dispose des connaissances suffisantes pour comprendre et saisir la ou les finalités déterminées pour lesquelles les données à caractère personnel sont recueillies et traitées.

Les personnes concernées ont le droit de décider quand et à qui elles souhaitent communiquer leurs données à caractère personnel. Le consentement de la personne concernée doit être obtenu au moment de la collecte des données, sauf circonstances exceptionnelles justifiant qu'elle en ait, au minimum, connaissance.

Les responsables du traitement des données veillent à ce que les enquêteurs communiquent suffisamment d'informations aux personnes concernées pour qu'elles puissent parfaitement comprendre et saisir la finalité déterminée pour laquelle les données à caractère personnel sont recueillies et traitées. Il sera considéré que la connaissance des personnes concernées est suffisante dès lors que tous les faits pertinents liés à la finalité déterminée, à l'utilisation et à la divulgation des données à caractère personnel leur ont été clairement expliqués.

13. Capacité à donner son consentement

La capacité à donner son consentement s'entend de l'aptitude à comprendre les conséquences d'un tel acte.

Pour que le consentement soit valable, les personnes concernées doivent avoir la capacité de donner leur consentement. Les personnes concernées présentant un handicap mental et les enfants doivent être interrogés en présence de leur tuteur ou de leurs parents et, en cas d'absence de ceux-ci, il y a lieu de consulter LEG. Toute question liée à la capacité doit être soumise à LEG et à l'unité/au département compétent, qui indiqueront les mesures à prendre selon les circonstances.

Formes du consentement

La nature des données à caractère personnel et les circonstances entourant le projet particulier de l'OIM déterminent la forme du consentement qui doit être donné au moment de la collecte des données.

Encadré 12 : Considérations en matière de consentement

- Déterminer la capacité juridique, sociale et culturelle des personnes concernées.
- Tenir compte de la capacité physique et mentale à donner son consentement.
- Soumettre à LEG les questions de capacité juridique avant la collecte de données.
- Etablir une représentation cartographique du flux interne de données à caractère personnelle au sein de l'OIM et des divulgations prévisibles à des tiers tout au long du cycle de traitement des données.
- Promouvoir l'obtention d'un consentement exprès sous forme écrite.
- Insérer une clause de consentement dans les formulaires existants d'entretien, d'enregistrement et de demande, ou utiliser un formulaire de consentement distinct au moment de la collecte des données.
- Distribuer des messages d'information lorsque des données à caractère personnel sont recueillies auprès d'importants groupes de population cibles.
- Prévoir des feuilles de signatures collectives lors de la saisie des données électroniques sur le terrain.
- Expliquer les procédures d'accès et de plainte (voir le Principe 7 : Accès et transparence).
- Communiquer les coordonnées de l'OIM aux personnes concernées au moment de la collecte des données.

Note : Les enquêteurs doivent être suffisamment formés. Le sexe, l'âge, la diversité linguistique et le niveau d'alphabétisation doivent toujours être pris en considération.

../ Consentement exprès : Déclaration orale ou signature manuscrite des personnes concernées indiquant qu'elles ont clairement compris et saisi les conséquences d'un consentement exprès donné à la collecte et au traitement de données.

../ Consentement implicite : Aucune déclaration orale ni signature manuscrite n'est obtenue mais, par leur action ou leur inaction, les personnes concernées indiquent sans ambiguïté qu'elles participent volontairement au projet de l'OIM.

../ Consentement par procuration : Consentement oral ou écrit donné dans des circonstances exceptionnelles au nom des personnes concernées par des proches, un membre autorisé de la communauté ou de l'entourage.

La forme du consentement doit être indiquée dans les formulaires d'entretien, d'enregistrement et de demande ou dans les dossiers électroniques.

Dans la mesure du possible, les responsables du traitement des données chercheront à obtenir un consentement exprès par écrit. Les empreintes digitales ou une croix suffisent si les personnes concernées sont illettrées ou incapables d'apposer leur signature.

La teneur du formulaire de consentement[12] et les conséquences d'une signature doivent être clairement expliquées, dans des termes qui permettent à la personne concernée de pleinement saisir et comprendre les finalités déterminées pour lesquelles les données à caractère personnel sont recueillies et traitées.

Le consentement donné pour la finalité déterminée initiale, des finalités déterminées additionnelles ou une divulgation à des tiers doit être consigné avec exactitude pour permettre aux responsables du traitement des données de vérifier que le consentement a été effectivement obtenu au moment de la collecte des données.

Le consentement doit être clairement indiqué dans les bases de données en cas de conversion des dossiers papier en dossiers électroniques.

EXEMPLE :

Si des dossiers papier sont numérisés manuellement aux fins de stockage dans une base de données, les cases de consentement doivent indiquer précisément la forme du consentement et les catégories de finalités déterminées pour lesquelles le consentement a été obtenu.

14. Consentement éclairé

Il y a consentement éclairé quand la personne concernée accepte que ses données à caractère personnel soient recueillies après avoir pris en considération tous les faits pertinents liés à la collecte et au traitement des données.

Les responsables du traitement des données doivent toujours tenir compte des éventuels obstacles linguistiques et des différents niveaux d'alphabétisation.

La méthode utilisée pour diffuser des informations aux personnes concernées doit viser à une bonne compréhension, et tout renseignement nécessaire et pertinent doit être mis à disposition sur les lieux de collecte, par exemple au moyen d'affiches bien visibles ou par une large diffusion de brochures.

EXEMPLE :

Des feuilles imprimées de format A3 sur lesquelles est indiquée la finalité déterminée de la collecte et du traitement des données peuvent être affichées sur les murs ou les arbres. Les affiches d'information doivent être clairement expliquées aux personnes concernées. Au besoin, des mégaphones, microphones, cassettes audio ou autres moyens de projection de la voix seront utilisés.

Au moment de la collecte, les éléments suivants doivent être clairement expliqués aux personnes concernées :

- les finalités déterminées et les finalités connexes ;
- les finalités déterminées additionnelles, si elles sont connues ;
- les flux internes nécessaires au sein de l'OIM ;
- les procédures d'accès, de correction et de plainte ; et
- toutes les divulgations prévisibles à des tiers (y compris les donateurs et les partenaires de projet).

L'obtention du consentement au moment de la collecte, en vue de divulgations prévisibles à des tiers ou de finalités déterminées additionnelles, permet de résoudre d'éventuelles difficultés pratiques liées à l'obtention du consentement à une date ultérieure.

[12] Voir le Modèle 1.1 pour un exemple de formulaire de consentement.

Refus du consentement

Tous les faits pertinents connus des responsables du traitement des données doivent être communiqués aux personnes concernées, notamment l'intérêt de donner son consentement, les risques en cas de refus du consentement, ainsi que toute conséquence négative qui pourrait résulter d'une divulgation à des tiers.

Si les personnes concernées refusent expressément de donner leur consentement, elles doivent être informées des conséquences d'un tel refus, y compris des effets éventuels en matière d'aide. Si la personne concernée décide néanmoins, en toute connaissance de cause, de refuser de donner son consentement, la collecte de données doit s'interrompre en ce qui la concerne.

Les personnes concernées conservent le droit de retirer leur consentement à toutes les étapes du processus de collecte des données. Dans la mesure du possible, les responsables du traitement des données respecteront les souhaits des personnes concernées, et toutes les données à caractère personnel les concernant seront détruites une fois le consentement retiré.

EXEMPLE :

Dans des circonstances exceptionnelles, des données à caractère personnel peuvent être recueillies auprès du chef de famille. Si l'épouse est en désaccord avec son conjoint, qui avait donné son consentement en son nom, les enquêteurs la rassureront quant aux principes de l'OIM et lui expliqueront les avantages liés au consentement. Si l'épouse persiste dans son refus de donner son consentement, le traitement des données prend fin, et toutes les informations sur cette personne concernée doivent être détruites.

EXEMPLE :

Un déplacement forcé consécutif à un conflit armé ou à une catastrophe naturelle peut laisser des milliers de personnes dans le dénuement. Dans pareille situation, il peut être impossible d'obtenir un consentement en temps voulu. En l'absence de consentement, les personnes concernées doivent à tout le moins être informées des raisons pour lesquelles leurs données à caractère personnel sont recueillies. Une fois le danger imminent passé, les enquêteurs peuvent obtenir le consentement, par exemple par le biais d'une campagne d'information ou la diffusion de feuilles de signatures collectives.

15. La connaissance comme condition minimale

La connaissance ne peut tenir lieu de condition minimale que si des circonstances exceptionnelles le justifient. Les responsables du traitement des données soupèseront toujours les risques et les avantages pour déterminer si la collecte de données peut être effectuée uniquement sur la base de la connaissance des personnes concernées.

Les personnes concernées doivent toujours être informées de la finalité déterminée de la collecte de données, même lorsque des circonstances exceptionnelles ne permettent pas de donner un consentement en temps voulu.

Dans pareille situation, les responsables du traitement des données doivent chercher à obtenir le consentement des personnes concernées dès que cela est raisonnablement possible.

16. Consentement par procuration

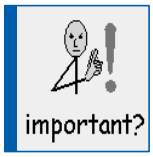
Le consentement par procuration s'entend du consentement oral ou écrit donné au nom de la personne concernée par un représentant autorisé.

Les responsables du traitement des données doivent toujours tenir compte des contraintes sociales, culturelles, religieuses ou environnementales susceptibles d'empêcher les personnes concernées de donner leur consentement.

Dans ces cas, le consentement du chef de famille peut tenir lieu de consentement par procuration. Les responsables du traitement des données informeront toutefois, par des moyens appropriés, tous les membres de la famille des finalités déterminées pour lesquelles leurs données à caractère personnel sont demandées et collectées.

EXEMPLE :

Il peut arriver que des personnes concernées n'aient pas la capacité sociale de donner leur consentement en raison d'une croyance culturelle selon laquelle les anciens représentent toujours les intérêts des membres de la famille. Si les particularités culturelles le permettent, des enquêteurs de même sexe que les personnes concernées expliqueront la finalité déterminée de la collecte de données, afin que chacune d'elles comprenne la finalité et l'utilisation prévue de ses données à caractère personnel.



Le consentement par procuration n'est permis que dans des circonstances exceptionnelles, lorsqu'il est impossible ou inapproprié d'obtenir directement le consentement de la personne concernée.

17. Personnes concernées vulnérables

On entend par personne concernée vulnérable toute personne qui n'a pas la capacité juridique, sociale, physique ou mentale de donner son consentement.

Les responsables du traitement des données doivent toujours respecter la vulnérabilité de certains groupes de population cibles et de certaines personnes concernées. La vulnérabilité dépendra des circonstances.

Le respect de la vulnérabilité suppose de trouver un équilibre entre les normes sociales, culturelles et religieuses du groupe auquel appartiennent les personnes concernées et de veiller à ce que chacune d'elles soit traitée sur un pied d'égalité dans le processus de collecte de données.

Encadré 13 : Respect de la vulnérabilité

- Valoriser les sexospécificités et les particularités liées à l'âge et à la culture.
- Mener des discussions de groupe thématiques.
- Encourager des séances d'information avant et après la collecte des données.
- Veiller à ce que des mesures appropriées soient en place pour protéger les droits et le bien-être des membres de groupes vulnérables et des personnes vulnérables.

Les critères de vulnérabilité sont notamment :

../ ***La présence de caractéristiques particulières,*** telles que l'illettrisme, le handicap, l'âge, etc. ;
../ ***Le lieu de résidence,*** tel qu'un lieu de détention, un camp de réinstallation, un endroit éloigné, etc. ;
../ ***Des facteurs environnementaux ou autres,*** tels qu'un environnement inhabituel, ou une langue et des concepts incompréhensibles, etc. ;
../ ***La situation dans les relations avec autrui,*** telle que l'appartenance à un groupe minoritaire ou à une secte, etc. ;
../ ***Des normes sociales, culturelles et religieuses*** au sein des familles, des communautés ou d'autres groupes auxquels appartiennent les personnes concernées.

17. Personnes concernées vulnérables

On entend par personne concernée vulnérable toute personne qui n'a pas la capacité juridique, sociale, physique ou mentale de donner son consentement.

Les responsables du traitement des données doivent toujours respecter la vulnérabilité de certains groupes de population cibles et de certaines personnes concernées. La vulnérabilité dépendra des circonstances.

Le respect de la vulnérabilité suppose de trouver un équilibre entre les normes sociales, culturelles et religieuses du groupe auquel appartiennent les personnes concernées et de veiller à ce que chacune d'elles soit traitée sur un pied d'égalité dans le processus de collecte de données.

Encadré 13 : Respect de la vulnérabilité

- Valoriser les sexospécificités et les particularités liées à l'âge et à la culture.
- Mener des discussions de groupe thématiques.
- Encourager des séances d'information avant et après la collecte des données.
- Veiller à ce que des mesures appropriées soient en place pour protéger les droits et le bien-être des membres de groupes vulnérables et des personnes vulnérables.

Les critères de vulnérabilité sont notamment :

../ ***La présence de caractéristiques particulières,*** telles que l'illettrisme, le handicap, l'âge, etc. ;
../ ***Le lieu de résidence,*** tel qu'un lieu de détention, un camp de réinstallation, un endroit éloigné, etc. ;
../ ***Des facteurs environnementaux ou autres,*** tels qu'un environnement inhabituel, ou une langue et des concepts incompréhensibles, etc. ;
../ ***La situation dans les relations avec autrui,*** telle que l'appartenance à un groupe minoritaire ou à une secte, etc. ;
../ ***Des normes sociales, culturelles et religieuses*** au sein des familles, des communautés ou d'autres groupes auxquels appartiennent les personnes concernées.

18. Souci des sexospécificités

Le souci des sexospécificités consiste à reconnaître les différences et les inégalités entre les sexes et à promouvoir les intérêts, les besoins et les priorités des hommes et des femmes, comme des filles et des garçons.

En encourageant le souci des sexospécificités, les responsables du traitement des données doivent tenir compte des normes sociales, culturelles et religieuses au sein du groupe auquel appartiennent les personnes concernées.

Les enquêteurs des deux sexes doivent être suffisamment formés pour réaliser l'équilibre entre le souci des sexospécificités et les dynamiques de pouvoir au sein des structures familiales, afin de prévenir toute répercussion négative que pourrait avoir la participation au processus de collecte des données.

EXEMPLE :

Après avoir évalué la dynamique des pouvoirs au sein du groupe de population cible, les responsables du traitement des données feront en sorte que, dans la mesure du possible, les femmes soient interrogées séparément par des enquêteurs femmes formées à être attentives à la dynamique des pouvoirs, aux rôles dévolus par la société aux deux sexes, à la violence familiale, etc..

Egalité de participation

La participation active des personnes concernées doit être encouragée à tous les stades du processus de collecte des données afin de leur permettre de s'exprimer librement lorsqu'elles prennent des décisions qui ont une incidence sur leur vie. Dans la mesure du possible, les enquêteurs animeront des groupes de discussion indépendants pour expliquer la finalité déterminée pour laquelle des données à caractère personnel sont demandées et recueillies.

Femmes et filles

Le principe même d'un consentement éclairé peut être battu en brèche par certaines normes en matière de relations entre les sexes, qui souvent exposent les femmes et les filles à l'influence excessive de leur mari, de leur père, de leur famille et des chefs de leur communauté. Les responsables du traitement des données adopteront une démarche proactive, de façon à ce que les données à caractère personnel soient demandées et recueillies directement auprès des femmes et des filles.

Il arrive souvent que les adolescentes soient particulièrement vulnérables dans des situations de migration, en raison du rôle d'adulte qu'elles assument et de la marginalisation sociale résultant de la maternité. Le rôle particulier des femmes et des filles et les facteurs de risque liés à la participation au processus de collecte des données doivent être identifiés avant la collecte des données, pour que des mesures appropriées soient prises pendant la collecte des données.

19. Enfants

Aux fins des principes de l'OIM, les enfants s'entendent des personnes concernées de moins de 18 ans[13].

Légalement, l'enfant n'a pas la capacité de donner son consentement. Les parents ou tuteurs doivent donner leur consentement en son nom et défendre à tout moment son intérêt supérieur.

Le consentement donné par les parents ou les tuteurs peut être invalidé si les responsables du traitement des données ont des raisons suffisantes de penser que ceux-ci agissent contrairement à l'intérêt supérieur de l'enfant. Dans ces cas, il y a lieu de prendre acte du conflit et demander conseil à LEG.

EXEMPLE :
S'il existe un doute sur l'implication d'un parent dans des activités inacceptables, telles que la traite d'enfants, le cas doit être soumis à l'unité/au département compétent de l'OIM et à LEG pour conseils.

Intérêt supérieur de l'enfant

L'intérêt supérieur de l'enfant est capital dans toute décision le concernant.

Les responsables du traitement des données doivent toujours anticiper les conséquences néfastes que peuvent avoir la collecte et le traitement de données à caractère personnel concernant un enfant. Le cas échéant, ils se concerteront avec les partenaires de l'OIM pour défendre l'intérêt supérieur de l'enfant.

Les incidences des conflits, la pauvreté et le VIH/sida ont affaibli le rôle traditionnel de l'enfant dans certaines communautés et accru sa vulnérabilité à l'exploitation et aux abus.

Les responsables du traitement des données détermineront si un enfant a besoin d'un traitement spécial à la suite d'un traumatisme, surtout lorsqu'il a fait l'objet d'exploitation et de violences sexuelles, ou lorsqu'il a été victime d'un conflit armé ou y a participé.

EXEMPLE :
L'aide sociopsychologique aux enfants peut permettre d'établir un compte rendu précis des antécédents, qui sera nécessaire pour porter assistance aux enfants non accompagnés.

Points de vue et opinions de l'enfant

Les enquêteurs doivent être suffisamment formés pour comprendre les besoins différents des filles et des garçons, ainsi que les éventuelles structures familiales parallèles.

[13] L'OIM considère qu'aux fins de protection de l'enfant, 18 ans est la limite d'âge supérieure. Les protections prévues par la Convention relative aux droits de l'enfant de 1989 s'appliquent à toute personne de moins de 18 ans, même si le droit national fixe l'âge de la majorité plus bas.

Les points de vue et opinions de l'enfant doivent être respectés à tout moment[14].

L'importance attachée aux points de vue et aux opinions de l'enfant dépendra de l'âge et du degré de maturité de celui-ci.

Il y a lieu d'encourager la participation de l'enfant. Les données seront recueillies dans un cadre adapté à celui-ci et, si possible, par un enquêteur du même sexe.

EXEMPLE :

Lors de l'entretien avec l'enfant, la finalité déterminée de la collecte de données doit lui être expliquée avec des mots simples et à l'aide de concepts adaptés à son âge, à son stade de développement et à ses origines culturelles, afin de lui faciliter la compréhension de la situation.

Tutelle

L'OIM ne peut assumer la tutelle d'un enfant en l'absence des parents ou du tuteur, même à la demande d'autorités légitimes.

En l'absence des parents ou des tuteurs, l'affaire doit être transmise à LEG.

En coordination avec LEG, les responsables du traitement des données envisageront des procédures appropriées, dans le pays d'origine et/ou d'accueil, en vue de désigner un tuteur. Si nécessaire, ils consulteront les partenaires de l'OIM spécialisés dans la protection de l'enfance.

Les cas spéciaux doivent être soumis à LEG pour orientation, de même que les projets où l'on escompte un nombre important de foyers dirigés par des enfants, orphelins ou adolescents exerçant un rôle d'adulte, ainsi que les cas de mineurs non accompagnés et d'enfants séparés accompagnés d'adultes assurant la tutelle pendant la durée du voyage.

[14] Selon l'article 12 de la Convention de 1989 relative aux droits de l'enfant, « [un] enfant qui est capable de discernement [a] le droit d'exprimer librement son opinion sur toute question l'intéressant, les opinions de l'enfant étant dûment prises en considération eu égard à son âge et à son degré de maturité. » Ce principe est réaffirmé dans les instruments suivants : Principes directeurs relatifs aux enfants associés aux forces armées et aux groupes armés (Paris, 2007) ; Observation générale n° 6 du Comité des droits de l'enfant relative au traitement des enfants non accompagnés et des enfants séparés en dehors de leurs pays d'origine (2005) ; Principles for ethical reporting on children, élaborés par le Fonds des Nations Unies pour l'enfance (UNICEF) et disponibles à l'adresse : http://www.unicef.org/media/media_tools_guidelines.html ; Guide de références de l'UNICEF sur la protection des enfants victimes de la traite en Europe (2006) ; Enfants réfugiés : principes directeurs concernant la protection et l'assistance, élaborés par le Haut-Commissariat des Nations Unies pour les réfugiés (1994) ; Principes directeurs du HCR relatifs à la détermination de l'intérêt supérieur de l'enfant (2008).

20. Personnes âgées

Les besoins spéciaux des personnes âgées doivent être pris en considération lors de l'évaluation des besoins des groupes de population cibles.

Les responsables du traitement des données évalueront les handicaps physiques et mentaux ainsi que les besoins sanitaires et psychosociaux des personnes âgées, afin qu'elles bénéficient de mesures adaptées.

EXEMPLE :

Lors de la distribution de l'aide alimentaire, des points d'enregistrement séparés pourraient être ménagés pour les personnes âgées.

Les enquêteurs doivent être suffisamment formés pour veiller à ce que les personnes âgées ne soient pas négligées pendant le processus de collecte des données.

21. Incapacité mentale

Légalement, les personnes concernées présentant une incapacité mentale ne peuvent donner leur consentement parce qu'elles risquent de ne pas comprendre et saisir pleinement les conséquences d'un tel acte. Ce sont les tuteurs qui doivent donner leur consentement en leur nom. En l'absence de tuteur, les responsables du traitement des données prendront acte de l'incapacité mentale et demanderont conseil à LEG sur les mesures à prendre en fonction des circonstances.

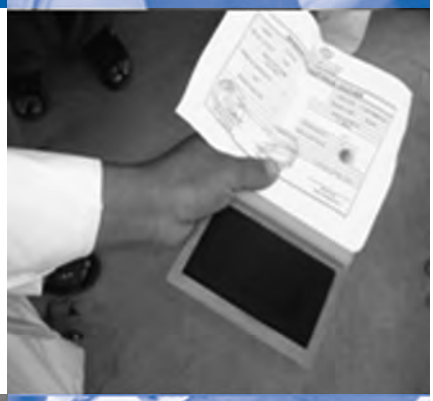
22. Incapacité physique

Des solutions de rechange doivent être prévues pour les personnes concernées présentant une incapacité physique ou dont la mobilité est réduite, qui ne peuvent se rendre sur les lieux de collecte des données.

EXEMPLE :

L'amputation d'un bras/d'une main ou la déficience d'un de ces membres peut être un obstacle au consentement écrit. Dans ces cas, les signatures par procuration ou le consentement oral doivent être consignés dans les formulaires d'entretien, d'enregistrement et de demande.

5



PRINCIPE 5 : TRANSFERT A DES TIERS

PRINCIPE 5 : TRANSFERT A DES TIERS

Des données à caractère personnel ne seront transférées à des tiers qu'avec le consentement exprès de la personne concernée, pour une finalité déterminée, et avec la garantie que des mesures suffisantes ont été prises pour protéger la confidentialité desdites données et garantir le respect des droits et des intérêts de la personne concernée. Ces trois conditions de transfert doivent être garanties par écrit.

La communication de données à caractère personnel à des tiers doit être strictement régie par une obligation contractuelle écrite pour éviter qu'elle ne :

- porte atteinte aux principes de l'OIM ;
- compromette la confidentialité des données à caractère personnel ; ou
- aille à l'encontre des attentes raisonnables des personnes concernées.

Registre des divulgations

Les responsables du traitement des données tiennent un registre de toutes les divulgations à des tiers.

Sur demande et dans la mesure du possible, les personnes concernées recevront un extrait du registre des divulgations concernant leurs données à caractère personnel.

Le registre des divulgations contiendra les éléments suivants :

- nom des responsables du traitement des données ;
- finalité déterminée du transfert ;
- date du transfert ; et
- description des catégories de données à caractère personnel ayant été divulguées.

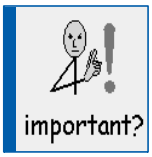
Encadré 14 : Tiers prévisibles

- Membres du personnel de l'OIM étrangers au projet de l'OIM pour lequel les données à caractère personnel ont été initialement collectées et traitées.
- Agents, tels que fournisseurs de services, consultants et chercheurs, qui recueillent des données à caractère personnel pour le compte de l'OIM.
- Donateurs, partenaires de l'OIM et partenaires d'exécution.
- Organismes publics dans les pays d'origine et d'accueil.
- Autorités de police et entités gouvermentales.
- Autres tiers, tels que médias, établissements universitaires, milieux d'affaires, entreprises privées, organisations non gouvernementales (ONG) ou non enregistrées, organisations internationales, et institutions des Nations Unies.

Note : Toujours veiller à ce que les tiers acceptent expressément par écrit les principes de l'OIM. En l'absence d'engagement à respecter les principes de l'OIM, il y a lieu d'en référer à LEG.

23. Consentement exprès

Le transfert à des tiers de données à caractère personnel est subordonné au consentement exprès de la personne concernée, et toutes les mesures raisonnables doivent être prises pour obtenir ce consentement sous forme écrite.



Le transfert à des tiers prévisibles doit être prévu avant la collecte des données.

De la sorte, il sera inutile d'obtenir le consentement au moment du transfert. Si des motifs raisonnables le justifient, il est possible de tenir compte de difficultés pratiques à obtenir le consentement exprès au moment du transfert. Ces cas exceptionnels doivent être soumis à LEG, qui avisera au cas par cas.

24. Finalité déterminée du transfert

La demande de transfert de données à caractère personnel doit être claire et précise, et indiquera la nature et les catégories des données à caractère personnel requises ainsi que la méthode de transfert à utiliser. Toute divulgation à des tiers doit être fondée sur le « besoin d'en connaître », et seules certaines catégories précises de données à caractère personnel pourront être communiquées pour atteindre la finalité déterminée de la demande de transfert.

25. Garanties suffisantes

Les garanties suffisantes pour protéger la confidentialité des données à caractère personnel et les droits et intérêts des personnes concernées seront examinées à la lumière des risques et des avantages d'un transfert éventuel. Les responsables du traitement des données feront preuve de diligence raisonnable, compte tenu de toutes les circonstances qui entourent le transfert éventuel.

Les éléments de diligence raisonnable sont notamment :

- ../ les risques potentiels et réels auxquels sont exposées les personnes concernées en cas de transfert ;
- ../ la nature des données à caractère personnel requises ;
- ../ la finalité déterminée pour laquelle des données à caractère personnel sont demandées ;
- ../ la durée du traitement escompté des données à caractère personnel ;
- ../ le type d'entité qui demande le transfert et ses relations avec l'OIM ;
- ../ le droit applicable au tiers ;
- ../ la garantie que la confidentialité des données à caractère personnel est respectée, et que les droits et intérêts des personnes concernées sont protégés pendant et après le transfert.

Le transfert de données à caractère personnel doit toujours être régi par un contrat écrit.

Encadré 15 : Indicateurs à prendre en compte en vue d'un contrat de transfert écrit

- 0 Nommer les parties contractantes.
- 0 Le cas échéant, examiner les dispositions législatives et réglementaires nationales relatives à la protection des données applicables au tiers.
- 0 Evaluer la situation dans le pays, le respect des droits de l'homme et la sécurité des personnes concernées.
- 0 Déterminer s'il est nécessaire de communiquer des données à caractère personnel ou si des données globales anonymes répondent à la finalité déterminée de la demande de transfert.
- 0 Indiquer la nature et les catégories de données à caractère personnel demandées, et veiller à ce que la quantité de données à caractère personnel soit limitée à ce qui est nécessaire pour atteindre la finalité déterminée du transfert.
- 0 Définir la méthode de transfert, préciser les conditions du transfert, et veiller à ce que la procédure soit sûre et sécurisée.
- 0 Toujours conserver les dossiers originaux des données à caractère personnel, et fournir une copie des données à caractère personnel nécessaires pour répondre à la demande de transfert.
- 0 Insister sur l'importance de préserver la confidentialité des données à caractère personnel et l'anonymat des personnes concernées, et envisager des mesures de protection supplémentaires pour les personnes vulnérables.
- 0 Insérer des clauses de confidentialité/protection des données, joindre la liste des principes de l'OIM relatifs à la protection des données, en précisant qu'elle fait partie intégrante du contrat.
- 0 Divulguer les données à caractère personnel uniquement aux personnes autorisées, et limiter toute utilisation et divulgation ultérieure à des tiers qui ne sont pas mentionnés dans le contrat de transfert écrit.
- 0 Indiquer les mesures nécessaires pour garantir la sécurité des données et les contrôles d'accès.
- 0 Indiquer la période de conservation et la méthode de destruction à utiliser lorsque la finalité déterminée du transfert aura été atteinte.
- 0 Préciser si l'OIM souhaite rester une source anonyme.
- 0 Préciser à qui appartiennent les données à caractère personnel et quelles sont les conditions de leur destruction, et souligner les privilèges et immunités de l'OIM, s'il y a lieu.

Note : Toujours demander conseil à LEG et à l'unité/au département compétent de l'OIM.

Les responsables du traitement des données soupèseront les risques et les avantages avant de divulguer des données, afin de déterminer si le tiers veillera à ce que des mesures comparables de protection des données soient prises pendant et après le transfert[15].

26. Méthode de transmission

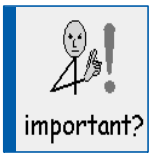
En cas de transfert de données à caractère personnel, des mesures appropriées seront prises pour protéger leur transmission aux tiers. La méthode de transmission doit être adaptée à la nature et à la sensibilité des données à caractère personnel.

Les méthodes de transmission sécurisées conjuguent les procédés suivants :

../ ***Cryptage*** : Toute transmission électronique de données à caractère personnel à des tiers doit, dans la mesure du possible, être cryptée.

../ ***Indicateurs de confidentialité*** : Des courriels contenant des données à caractère personnel ne seront envoyés qu'en cas de « besoin d'en connaître ». Ils devront être signalés comme confidentiels à l'aide d'applications de courrier électronique, telles que celle proposée par Microsoft Outlook, permettant de signaler le degré de sensibilité du courriel.

../ ***Service de messagerie/pli recommandé*** : Tout CD crypté ou dossier papier confidentiel doit toujours être envoyé par messagerie privée ou, à tout le moins, par courrier recommandé, et l'enveloppe doit clairement porter la mention « confidentiel ».



Les systèmes de cryptage les plus performants[16] doivent être utilisés pour protéger le transfert de données à caractère personnel à des tiers.

27. Divulgation

Tout contrat de transfert écrit[17] sera soumis à LEG pour approbation. Sauf convention contraire, l'OIM se réservera le droit de divulguer des données à caractère personnel au cas par cas.

Services de police

Les services de police s'entendent des autorités nationales ou internationales investies du pouvoir d'assurer ou de faciliter l'application de la loi.

EXEMPLE :

Dans l'hypothèse où EUROPOL demanderait à consulter des données à caractère personnel concernant des victimes de la traite dans le but de lutter contre la traite dans l'Union européenne, le transfert de données à caractère personnel obéirait aux trois conditions strictes que sont le consentement exprès, la finalité déterminée du transfert, et l'application de mesures de protection suffisantes.

Toute demande de consultation de données à caractère personnel ou d'accès à des bénéficiaires de l'OIM de la part de services de police nationaux ou internationaux doit, au préalable, faire l'objet d'une concertation avec LEG et l'unité/le département compétent de l'OIM. La divulgation de données à caractère personnel aux fins d'enquête et de poursuites pénales est soumise à l'approbation de l'OIM et de la personne concernée. Selon la nature du projet de l'OIM, toute relation existante entre l'OIM et des services de police sera portée à la connaissance des personnes concernées au moment de la collecte de données.

[15] Les principes pertinents de l'OIM doivent figurer dans les contrats écrits afin de défendre les droits et intérêts des personnes concernées.

[16] Les responsables de traitement des données doivent se concerter avec l'informaticien compétent et consulter les tiers avant le transfert des données, de manière à disposer de systèmes de décryptage compatibles.

[17] Voir le Modèle 2 pour des clauses contractuelles types en cas de transfert à des tiers.

Agents

Les agents sont des personnes ou des entités habilitées à agir au nom du responsable du traitement des données pendant toute la durée du traitement des données.

EXEMPLE :
Une société privée mandatée pour mener des activités d'enregistrement peut être considérée comme un agent agissant au nom de l'OIM.

Les agents contribuent à la réalisation des finalités déterminées pour lesquelles les données à caractère personnel sont recueillies et traitées. Ils sont directement autorisés par l'OIM à apporter leur concours aux activités nécessaires à la réalisation de ces finalités. Les responsables du traitement des données veillent à ce que les personnes concernées aient connaissance des indispensables divulgations aux agents prévus, ainsi que des divulgations éventuelles aux agents qui n'étaient pas prévus au moment de la collecte des données.

Les relations entre l'OIM et les agents doivent être strictement régies par des dispositions contractuelles écrites obligeant ceux-ci à se conformer aux principes de l'OIM et aux instructions du responsable du traitement des données[18]. La propriété des données à caractère personnel revient normalement à l'OIM. Les restrictions quant à leur utilisation et divulgation future à l'égard d'autres tiers, ainsi que la destruction des données à caractère personnel, seront clairement définies dans le contrat de service[19].

Partenaires d'exécution

Les partenaires d'exécution sont des entités qui oeuvrent aux côtés de l'OIM à la réalisation d'une activité de projet de l'OIM.

EXEMPLE :
Lorsque le Haut-Commissariat des Nations Unies pour les réfugiés (HCR) et l'OIM collaborent pour réinstaller un réfugié, ils peuvent être les partenaires d'exécution d'un projet conjoint.

La libre circulation des données à caractère personnel pourra être autorisée avec des entités ayant des relations officielles avec l'OIM, à condition que le transfert soit prévu au moment de la collecte des données et accepté par la personne concernée. Avant le transfert, toutefois, les responsables du traitement des données s'assureront que l'entité en question continue de satisfaire aux conditions de protection applicables au transfert.

Partenaires de l'OIM

Les partenaires de l'OIM sont des parties prenantes avec lesquelles un accord avait été conclu antérieurement aux fins d'activités menées en coopération et en coordination avec l'OIM.

EXEMPLE :
Des réunions stratégiques seront organisées pour faire connaître les principes de l'OIM aux gouvernements hôtes, aux organismes des Nations Unies, aux organisations internationales, aux ONG et aux membres de groupes de population cibles associés aux opérations de secours et à la gestion des camps.

Les responsables du traitement des données se mettront en relation avec toutes les parties prenantes pour qu'elles connaissent l'attachement de l'OIM à la protection des données. Cela facilitera la coopération en vue de la mise en œuvre des principes de l'OIM.

[18] Voir le Modèle 2 pour des clauses contractuelles types à insérer dans les contrats conclus avec des agents.

[19] Voir le Modèle 2 pour des clauses types sur la protection des données, la confidentialité, la propriété et la destruction à insérer dans les contrats.

Donateurs

Les donateurs sont des personnes ou des entités qui contribuent au financement d'un projet de l'OIM.

Les responsables du traitement des données veilleront à ce que les relations avec les donateurs ne portent pas atteinte aux principes de l'OIM. Une bonne façon de faire connaître ces principes consiste à les incorporer dans les propositions de projet au titre des considérations de politique générale de l'OIM. Sauf exigence contraire du donateur, l'OIM affirmera son droit de propriété sur les données à caractère personnel et insérera une clause de propriété dans les mémorandums d'accord et les accords passés avec les donateurs[20]. Les rapports aux donateurs ne comprendront aucune donnée à caractère personnel ni aucune photographie de personnes concernées vulnérables, sauf accord écrit préalable de l'intéressé.

Si les trois conditions de transfert sont remplies, les modalités et conditions du transfert devront être clairement définies dans le contrat écrit.

Les accords écrits conclus avec des tiers devront comporter des clauses relatives à la propriété des données et au respect des principes de l'OIM (voir aussi le Principe 11).

Médias

Le personnel de l'OIM et les tiers autorisés n'évoqueront pas devant les médias de cas précis permettant d'identifier des personnes concernées[21].

Tout commentaire sera limité aux questions de politique générale, sauf si la divulgation de données à caractère personnel a été autorisée[22]. Cette règle est particulièrement importante dans le cas de personnes concernées vulnérables, telles que les enfants, les personnes déplacées par la force, les victimes ou victimes présumées de la traite, et les victimes de violences physiques et sexuelles.

EXEMPLE :
Sans autorisation préalable, il y a lieu de ne pas communiquer aux journalistes de noms, de situations, de photographies ni de renseignements précis sur des victimes de conflit armé.

Toutes les personnes concernées ont le droit de garder l'anonymat en ce qui concerne la couverture médiatique, et les médias doivent être encouragés à protéger l'identité des personnes concernées. Toute demande de médias visant à rencontrer des bénéficiaires de l'OIM ou à consulter leurs données à caractère personnel sera coordonnée à l'avance avec la Division Médias et communication et le secteur de service compétent au Siège de l'OIM. Elle sera examinée au cas par cas, compte tenu de la sensibilité du dossier, du niveau de risque encouru ainsi que de la sécurité et de l'intérêt supérieur de la personne concernée.

---

[20] Voir le Modèle 2 pour une clause type relative à la propriété/propriété intellectuelle.

[21] Pour de plus amples informations, prière de contacter la Division Médias et communication, au Siège de l'OIM.

[22] En fonction de la sensibilité des données à caractère personnel, les coordonnées des membres du personnel de l'OIM ou des représentants de tiers ne doivent pas être communiquées aux médias sans autorisation préalable. Voir le Modèle 1.4 pour un formulaire d'autorisation type concernant les médias, destiné aux personnes concernées.

Si le bénéficiaire est une victime de la traite, d'autres éléments encore doivent être pris en considération, dont des mesures supplémentaires de protection de la confidentialité et de l'anonymat. Le principe directeur de la protection des victimes est de « ne pas nuire »[23], ce qui suppose de protéger le bénéficiaire face aux médias lorsque les relations avec eux risquent de nuire à sa sécurité ou à sa réadaptation. En outre, l'OIM devra disposer d'un délai suffisant pour examiner la demande et, s'il y a lieu, pour désigner une personne répondant aux conditions requises et disposée à rencontrer les médias.

L'OIM doit toujours veiller à être libre de décider s'il y a lieu ou non de faciliter l'accès. Si elle donne son accord, le consentement écrit préalable du bénéficiaire devra être obtenu, et la finalité déterminée de la demande ainsi que les risques particuliers et les conséquences éventuelles d'un échange avec les médias seront clairement exposés. Par ailleurs, l'OIM signera avec le média un accord qui énonce clairement les règles de protection requises, notamment l'obligation de respecter strictement les principes de l'OIM, ainsi que les conditions précises d'accès aux données telles qu'exposées dans la Note d'orientation sur l'accès des médias aux bénéficiaires de l'OIM victimes de la traite[24].

Sans préjudice de l'indépendance éditoriale, l'OIM vérifiera et approuvera les versions finales des séquences audio et vidéo des témoignages avant leur distribution, diffusion ou impression. Il est nécessaire que l'enregistrement reçoive l'approcation préalable de l'OIM, pour garantir la protection de l'image et de la voix du bénéficiaire, et du lieu où il se trouve.

Sauf consentement préalable de la personne concernée, les visages doivent être floutés, l'identité et le lieu cachés, et une voix hors champ prévue dans le reportage. Ces précautions revêtent une importance particulière pour les cas très sensibles et les personnes concernées vulnérables, qui peuvent être en danger.

28. Photographies, documents vidéo ou audio et images numériques

Les photographies, documents vidéo ou audio et images numériques représentant des personnes concernées dans le but de faire connaître et de promouvoir les activités de l'OIM seront, dans toute la mesure du possible, soumis au consentement des personnes concernées. Les personnes concernées seront informées de la nature et du but de la séance photo ou du document vidéo, ainsi que de son insertion dans l'iconothèque de l'OIM et de son utilisation ultérieure dans le cadre de l'action de l'OIM[25].

Dans les cas extrêmement sensibles, le consentement écrit préalable de la personne concernée est requis et, s'il y a lieu, l'identité et le lieu seront cachés et les visages floutés.

EXEMPLE :

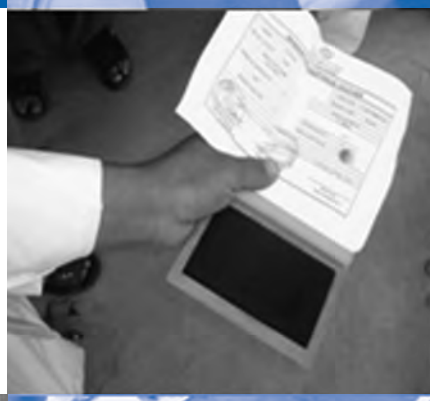
Les visages des personnes victimes de la traite n'apparaîtront pas à la télévision ou dans des publications, sauf si ces personnes y ont expressément consenti par écrit.

[23] Pour de plus amples informations sur la protection des victimes, voir le manuel intitulé *The IOM Handbook on Direct Assistance for Victims of Trafficking*, OIM, Genève (2007).

[24] Pour une assistance concernant la « Note d'orientation sur l'accès des médias aux bénéficiaires de l'aide de l'OIM victimes de la traite », contacter la Division de l'aide aux migrants au Département de la gestion des migrations, au Siège de l'OIM.

[25] Voir le Modèle 1.3 contenant un formulaire type de consentement à la prise de photographies.

6



PRINCIPE 6 :
CONFIDENTIALITE

PRINCIPE 6 : CONFIDENTIALITE

La confidentialité des données à caractère personnel doit être préservée à toutes les étapes du processus de collecte et de traitement des données, et sera garantie par écrit. Tous les membres du personnel de l'OIM et les personnes représentant des tiers qui sont autorisés à avoir accès à des données à caractère personnel et à les traiter sont tenus à la confidentialité.

La confidentialité des données à caractère personnel et l'anonymat des personnes concernées doivent être respectés tout au long du cycle de traitement des données.

29. Engagement de confidentialité

La confidentialité concerne le traitement des données à caractère personnel que la personne concernée a communiquées à l'OIM dans le cadre d'une relation de confiance, dans l'espoir qu'elles ne seront pas divulguées d'une manière incompatible avec ses souhaits.

La confidentialité doit être un outil au service de la coopération et garantir la véracité des données à caractère personnel communiquées. Une clause type relative à la protection des données[26] sera incorporée dans les formulaires d'entretien, d'enregistrement et de demande existants, ou un formulaire de confidentialité distinct sera utilisé au moment de la collecte des données afin de renforcer l'attachement de l'OIM au principe de confidentialité.

EXEMPLE :

Si, en raison de leur méfiance, des personnes concernées ne livrent que des informations partielles, cela peut avoir des incidences sur l'ensemble des services d'aide que l'OIM pourrait leur fournir. Les personnes concernées doivent être rassurées au sujet de l'attachement de l'OIM à la confidentialité, ce qui favorisera un climat de confiance propice à la fourniture d'informations véridiques et exactes.

Toute limitation au principe de confidentialité sera expliquée aux personnes concernées au moment de la collecte des données.

L'attachement de l'OIM à la confidentialité doit être promu par des séances d'information et des formations à l'intention, entre autres, des membres du personnel de l'OIM, des agents (fournisseurs de services/consultants), des partenaires d'exécution, des partenaires de l'OIM, des donateurs, des pays dans lesquels intervient l'Organisation et des pays hôtes.

30. Précautions de confidentialité

Les membres du personnel de l'OIM, les agents, les donateurs, les partenaires de l'OIM, les partenaires d'exécution et les tiers autorisés doivent tous être informés de la confidentialité des données à caractère personnel avant toute collecte, utilisation ou divulgation.

Les responsables du traitement des données prendront toutes les précautions voulues au moment d'autoriser la divulgation de données à caractère personnel car un manquement à la confidentialité peut engendrer toutes sortes de problèmes de protection, parmi lesquels des atteintes ou des menaces d'atteinte à la vie, un traitement discriminatoire ou la détention.

EXEMPLE :

Les personnes concernées doivent avoir connaissance de l'existence d'accords sur la communication d'informations ou d'exigences de donateurs qui obligent à divulguer certaines catégories de données à caractère personnel à des partenaires d'exécution et aux pays associés à des projets de rapatriement ou de réinstallation.

[26] Voir le Modèle 2.2 pour un exemple de clause type relative à la protection des données à incorporer, s'il y a lieu, dans les formulaires d'entretien, d'enregistrement et de demande. La clause type relative à la protection des données doit figurer dans les contrats conclus avec les agents (fournisseurs de services/consultants), les partenaires d'exécution, les partenaires de l'OIM, les donateurs et les autres tiers.

Personnel de l'OIM

Tous les membres du personnel – permanents, temporaires, bénévoles – de l'OIM sont tenus à la confidentialité.

L'engagement à respecter et préserver la confidentialité des données à caractère personnel doit être garanti par écrit.

Les clauses types de l'OIM relatives à la protection des données et à la confidentialité seront incorporées dans tous les contrats de travail, pour que les données à caractère personnel soient protégées à tout moment. L'engagement à respecter la confidentialité restera valable après la cessation de service.

Les responsables du traitement des données veilleront à ce qu'un formulaire de confidentialité[27] soit signé par tous les membres du personnel autorisés à traiter des données à caractère personnel, en particulier dans les cas très sensibles. Cela vise les informaticiens, les commis à la saisie des données, les stagiaires, les chercheurs, les interprètes officiels et officieux, les conseillers désignés, les médecins et les consultants.

Le traitement de données à caractère personnel très sensibles peut exiger des garanties plus strictes. Dans ces cas, l'unité/le département compétent doit être consulté.

Tiers autorisés

Toute personne représentant un tiers autorisé est tenue à la confidentialité même après l'expiration ou la résiliation des contrats écrits. Les contrats écrits conclus avec des tiers agissant pour le compte de l'OIM, tels que, en autres, des fournisseurs de services, des consultants, des chercheurs et des interprètes, mentionneront clairement l'obligation de garantir la confidentialité des données à caractère personnel et de traiter ces données conformément aux principes de l'OIM.

Encadré 16 : Considérations en matière de confidentialité

- Organiser des formations continues pour le personnel et les agents de l'OIM, et encourager des formations conjointes pour les fournisseurs de services, les partenaires d'exécution, les partenaires de l'OIM et les donateurs.
- Faire preuve d'ouverture et de transparence, et encourager une relation de confiance avec les personnes concernées.
- Donner aux personnes concernées l'assurance que l'OIM est déterminée à traiter leurs données à caractère personnel de manière confidentielle.
- Expliquer aux personnes concernées la portée et les limites de la confidentialité, au moment de la collecte des données.
- Encourager un « climat de confidentialité » au sein du bureau et dans les relations avec tous les tiers autorisés.
- Veiller à ce que les données à caractère personnel soient gérées avec le plus grand soin et en toute confidentialité tout au long de leur traitement.
- Autoriser toutes les divulgations par écrit, et veiller à ce que les membres du personnel de l'OIM et les tiers comprennent l'importance de la confidentialité.
- Garantir la confidentialité en veillant à ce que les formulaires de confidentialité soient signés.
- Limiter strictement l'accès aux membres autorisés du personnel de l'OIM et aux personnes représentant des tiers autorisés.
- Tenir un registre d'accès aux catégories de données à caractère personnel divulguées.
- Indiquer la mention « Confidentiel » sur toute correspondance électronique et papier, et veiller à ce que les destinataires soient sélectionnés avec discernement.
- Surveiller l'élimination des documents imprimés et autres documents papier contenant des données à caractère personnel.

Note : En cas de doute, s'adresser à l'unité/au département compétent de l'OIM et à LEG.

EXEMPLE :

Le traitement de données à caractère personnel très sensibles, telles que les données médicales, peut obliger à limiter leur accès à certaines catégories de personnel de l'OIM, à les conserver sous un format codé, et à les transmettre au moyen d'outils de cryptage de haut niveau.

[27] Voir le Modèle 3 pour un exemple de formulaire de confidentialité type à l'intention des membres du personnel de l'OIM, des stagiaires et des consultants qui traitent des données à caractère personnel.

Les responsables du traitement des données veilleront à ce que tous les tiers acceptent la condition de confidentialité avant le transfert de données à caractère personnel. Une clause de confidentialité[28] figurera dans les contrats de transfert écrits conclus avec les partenaires d'exécution, les partenaires de l'OIM, les donateurs et les autres tiers qui demandent à accéder à des données à caractère personnel.

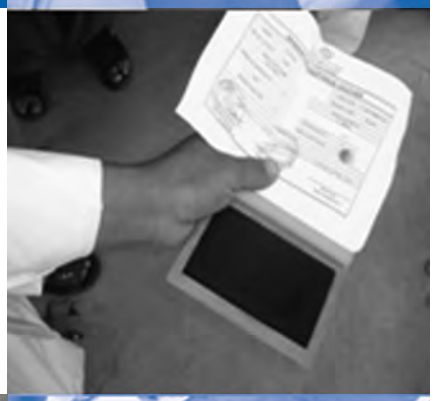
Les responsables du traitement des données s'assureront que la clause de confidentialité s'applique à l'OIM en tant que source de l'information[29], au cas où l'Organisation souhaite rester anonyme dans une publication.

Tout contrat de transfert écrit comportera une clause de confidentialité qui s'appliquera au-delà de la durée du contrat.

[28] Voir le Modèle 2 pour une clause de confidentialité type.

[29] Voir le Modèle 2.1 pour une clause de confidentialité type concernant la source de l'information.

7



PRINCIPE 7 : ACCES ET TRANSPARENCE

PRINCIPE 7 : ACCES ET TRANSPARENCE

Les personnes concernées auront la possibilité de vérifier leurs données à caractère personnel et pourront y accéder pour autant que la ou les finalités déterminées pour lesquelles elles ont été recueillies et traitées ne s'en trouvent pas compromises. Les responsables du traitement des données veilleront à l'application d'une politique générale d'ouverture à l'égard de la personne concernée en l'informant des faits nouveaux, des pratiques et des politiques concernant les données à caractère personnel.

L'élaboration des politiques et les pratiques doivent être transparentes, et les procédures d'accès, de rectification et de plainte relativement simples.

31. Plaintes

Afin de permettre le dépôt de plaintes relatives à la protection des données, les coordonnées du bureau extérieur pertinent de l'OIM doivent, à tout le moins, être communiquées aux personnes concernées au moment de la collecte des données. L'adresse postale, l'adresse électronique et les numéros de téléphone et de télécopie du bureau extérieur pertinent de l'OIM figureront sur les formulaires d'entretien, d'enregistrement et de demande, ou sur les dépliants distribués sur les sites de collecte.

Les procédures de plainte varieront, entre autres, en fonction des éléments suivants :

- le type de projet de l'OIM ;
- la nature de l'activité de l'OIM ;
- les facteurs environnementaux ;
- le contexte particulier ;
- la sensibilité des données à caractère personnel ;
- les capacités du personnel ; et
- les ressources disponibles.

Encadré 17 : Considérations en matière de plainte

- Autoriser à déposer les plaintes relatives à la protection des données en personne, par écrit ou par téléphone.
- Accuser réception de toutes les plaintes et les examiner.
- Protéger la confidentialité du plaignant.
- Au besoin, accorder une réparation appropriée.

Note : Toujours communiquer les coordonnées de l'OIM aux personnes concernées au moment de la collecte de données.

EXEMPLE :

Des boîtes en carton destinées à recueillir les plaintes peuvent être installées sur les sites de collecte de données, à des endroits réservés à cet effet dans les camps de réinstallation ou dans les bureaux de l'OIM. Si les données à caractère personnel sont très sensibles, et que les ressources et les capacités du personnel le permettent, une adresse électronique ou un numéro de permanence téléphonique peuvent servir à recueillir les plaintes relatives à la protection des données formulées par les personnes concernées.

32. Demande d'accès présentée par une personne concernée

Toute personne concernée a le droit de consulter et de rectifier à tout moment ses données à caractère personnel ; les responsables du traitement des données répondront aux demandes d'accès sans retard excessif. Les personnes concernées peuvent formuler leur demande d'accès par écrit[30] ou oralement.

La divulgation de données à caractère personnel ne saurait être automatique. Les responsables du traitement des données étudieront tout d'abord toutes les circonstances entourant la demande d'accès, parmi lesquelles l'intérêt supérieur de la personne concernée, l'absence de coercition, la falsification d'identité, les facteurs environnementaux, les incidences éventuelles sur les droits et les intérêts d'autres personnes concernées, ou encore la sécurité du personnel de l'OIM et des représentants de tiers autorisés.

[30] Voir le Modèle 4 pour un formulaire de demande d'accès type.

L'accès aux données à caractère personnel ne doit pas être refusé, à moins que cela ne soit clairement justifié. Les responsables du traitement des données ont toute latitude pour ne pas divulguer certaines catégories de données à caractère personnel, si leur accès immédiat fait obstacle à la finalité déterminée ou entrave l'aide apportée aux personnes concernées.

Les responsables du traitement des données ne révéleront des informations sur les personnes concernées qu'après avoir vérifié l'identité de celles-ci.

La personne concernée doit établir son identité de façon à ce que le responsable du traitement des données ait des motifs raisonnables de croire qu'elle est bien la personne qu'elle prétend être. Une carte d'enregistrement ou un document d'identité non officiel sont acceptés comme preuve d'identité dans les cas où les documents d'identité officiels font défaut.

Les données à caractère personnel seront communiquées aux personnes concernées de manière claire et intelligible, compte tenu du « besoin d'en connaître ». Les responsables du traitement des données ne communiqueront des résumés de dossiers individuels ou des copies de catégories de données à caractère personnel que pour répondre à la finalité de la demande d'accès.

Il y aura lieu d'accéder à toute demande visant à rectifier ou à effacer des données à caractère personnel erronées ou inexactes. Toute modification substantielle de données à caractère personnel sera communiquée au personnel de l'OIM et aux tiers autorisés qui ont accès aux données à caractère personnel relatives à la personne concernée. Toute information nouvelle sera versée au dossier électronique ou papier existant, et les responsables du traitement des données joindront une note indiquant toutes les corrections.

Encadré 18 : Considérations en matière d'accès

- Faire preuve de prudence en cas de demande d'accès à des données.
- Tenir compte de toutes les circonstances entourant la demande d'accès.
- Ne communiquer des renseignements personnels aux représentants autorisés que s'ils établissent leur identité.
- Ne communiquer de catégories de données à caractère personnel qu'en cas de « besoin d'en connaître » pour répondre à la finalité de la demande d'accès.
- Fournir des résumés de dossiers individuels et/ou des copies de dossiers électroniques ou papier.
- Accéder aux demandes de suppression ou de rectification de données à caractère personnel inexactes, et informer le personnel de l'OIM et les tiers autorisés chargés de traiter les données de toute modification substantielle.
- Tenir un registre des demandes d'accès et des catégories de données à caractère personnel divulguées.
- Motiver clairement le refus de donner accès aux données dans des circonstances exceptionnelles.

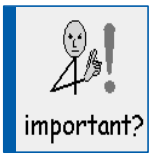
Note : L'intérêt supérieur des personnes concernées sera pris en considération à tout moment.

EXEMPLE :

De brefs résumés oraux peuvent être donnés en réponse à des demandes d'accès précises émanant de personnes concernées au lendemain d'un conflit. Les responsables du traitement des données feront toutefois preuve de toute la prudence requise pour empêcher la divulgation de données à caractère personnel sous un faux prétexte, en particulier si les informations demandées risquent de porter préjudice aux personnes concernées et de conduire à des actes de violence, tels que des attaques xénophobes.

33. Demande d'accès présentée par un tiers

Les divulgations aux tiers sont soumises aux trois conditions strictes qui régissent le transfert, à savoir le consentement exprès de la personne concernée, la finalité déterminée du transfert, et des garanties suffisantes (voir le Principe 5).



Les responsables du traitement des données feront preuve de bon sens et de toute la prudence requise lorsqu'ils répondent aux demandes d'accès présentées par un tiers.

Parents et tuteurs

Les demandes présentées par les parents et les tuteurs doivent être fondées sur l'intérêt supérieur de l'enfant. Les responsables du traitement des données pourront refuser de divulguer des données à caractère personnel concernant un enfant s'ils ont des raisons suffisantes de croire que cette communication serait contraire à son intérêt supérieur. Ces cas doivent être réglés en concertation avec LEG et l'unité/le département compétent de l'OIM.

Représentants

Les demandes présentées par des personnes ou des entités représentant les intérêts des personnes concernées doivent être soumises à des contrôles stricts.

Les responsables du traitement des données exerceront leur pouvoir discrétionnaire avec discernement et exigeront des documents d'identité valides ainsi qu'une preuve écrite ou orale de l'autorisation donnée par la personne concernée.

L'intérêt légitime des membres d'une famille à être regroupés et à savoir ce qu'il est advenu de personnes concernées et comment elles vont, doit être mis en balance avec la confidentialité des données à caractère personnel et les droits et intérêts des personnes concernées.

EXEMPLE :

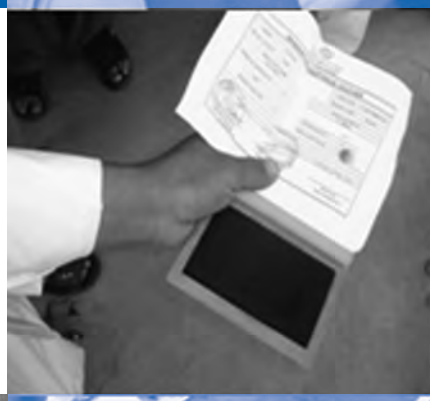
En l'absence de consentement, et dès lors qu'elle ne présente aucun risque en matière de sécurité, la divulgation aux proches et à l'entourage sera limitée au fait que la personne a été enregistrée auprès de l'OIM.

Seules des données à caractère non personnel seront communiquées aux proches et à l'entourage, sauf si la personne concernée autorise la divulgation de ses données à caractère personnel.

Il y a lieu de consulter LEG si des proches ou l'entourage demandent une divulgation complète sans le consentement de la personne concernée. Les responsables du traitement des données vérifieront l'authenticité des représentants au vu des informations fournies par la personne concernée et consignées dans des bases de données ou des formulaires d'entretien, d'enregistrement et de demande.

8

PRINCIPE 8 : SECURITE DES DONNEES



PRINCIPE 8 : SECURITE DES DONNEES

Les données à caractère personnel doivent être conservées en lieu sûr, tant sur le plan technique qu'organisationnel, et seront protégées par des mesures raisonnables et suffisantes contre toute modification non autorisée, falsification, destruction illégale, perte accidentelle, divulgation abusive ou transfert indu. Les mesures de protection énoncées dans les politiques et directives pertinentes de l'OIM s'appliqueront à la collecte et au traitement des données à caractère personnel.

Sécurité des données

La sécurité des données désigne un ensemble de mesures physiques et technologiques qui préservent la confidentialité et l'intégrité des données à caractère personnel et empêchent toute modification non autorisée, falsification, destruction illégale, perte accidentelle, divulgation abusive ou transfert indu.

Les responsables du traitement des données surveilleront l'échange interne et externe de données à caractère personnel pour s'assurer que des mesures de sécurité des données appropriées sont appliquées aux dossiers électroniques et papier.

Les mesures de sécurité des données varieront, entre autres, selon les éléments suivants :

- type de projet de l'OIM ;
- nature des données à caractère personnel ;
- format du support de stockage ;
- environnement du poste de travail ; et
- capacités technologiques à disposition du bureau extérieur pertinent de l'OIM.

Une « culture de la sécurité des données » sera adoptée pour garantir la sécurité de l'accès, du stockage, de la transmission et de la destruction des données à caractère personnel.

34. Risques liés à la sécurité des données

Les responsables du traitement des données préviendront les risques liés à la sécurité des données en procédant systématiquement à des évaluations[31] et en appliquant de bonnes pratiques de gestion des risques.

Des mesures physiques et technologiques appropriées seront appliquées en coordination avec l'informaticien compétent pour réduire les menaces et les vulnérabilités éventuelles.

Les mesures de sécurité des données seront régulièrement examinées et améliorées, afin que le niveau de protection des données soit adapté au degré de sensibilité attribué aux données à caractère personnel.

[31] Voir la Liste de vérification 2 pour une liste de vérification type en matière d'évaluation des risques liés à la sécurité, à utiliser conjointement aux normes et politiques informatiques pertinentes.

35. Classification des dossiers

Une classification type des dossiers sera établie après évaluation de la sensibilité des données à caractère personnel[32].

Il sera clairement indiqué dans tout dossier électronique ou papier que sa transmission est limitée aux membres du personnel autorisés de l'OIM et aux représentants de tiers autorisés.

Classification des dossiers électroniques ou papier :

../ ***Diffusion illimitée*** *:* Données globales anonymes[33], généralement diffusées au sein de l'Organisation, qui peuvent être publiées et divulguées à des tiers.

../ ***Diffusion restreinte*** *:* Données à caractère non personnel dont la divulgation est limitée aux flux internes comme suit :

- › Données à caractère non personnel divulguées au sein de l'Organisation à des fins internes, par exemple, rapports statistiques ou notes interservices ;
- › Données à caractère non personnel réservées à l'usage interne d'une unité ou d'un département de l'OIM et ne pouvant être diffusées dans l'ensemble de l'Organisation ; par exemple, l'analyse d'un projet ou les études de cas.

../ ***Confidentiel*** *:* Toute donnée à caractère personnel que la personne concernée a communiquée à l'OIM dans une relation de confiance.

../ ***Secret*** *:* Données à caractère personnel hautement sensibles[34] relatives à certaines personnes concernées, dont la diffusion pourrait avoir des répercussions graves et constituer une violation des droits de l'homme.

[32] La sensibilité sera évaluée avant la collecte des données. Pour plus de détails, voir le chapitre d'introduction.

[33] Les données anonymes restent soumises aux principes de l'OIM jusqu'à la destruction effective des données à caractère personnel auxquelles elles se rapportent.

[34] Les données hautement sensibles s'entendent de données à caractère personnel et de faits importants qui pourraient être utilisés pour nuire aux personnes concernées, aux membres du personnel ou aux agents de l'OIM, pour mettre leur vie en danger ou pour porter gravement atteinte aux droits et aux intérêts des personnes concernées. Le degré de sensibilité attribué aux données à caractère personnel sera déterminé par l'évaluation de la sensibilité effectuée avant la collecte des données.

Encadré 19 : Indicateurs d'une « culture de la sécurité des données »

- Evaluer les risques liés à la sécurité des données.
- Examiner et évaluer régulièrement les mesures de sécurité des données.
- Sensibiliser aux risques liés à la sécurité des données.
- Renforcer la confiance dans l'application des mesures de sécurité des données.
- Promouvoir la coopération entre les membres du personnel de l'OIM et avec les agents (fournisseurs de services/consultants), les partenaires d'exécution, les partenaires de l'OIM, les donateurs et autres tiers.
- Procéder à des contrôles d'accès stricts, utiliser des indicateurs de confidentialité et des outils de cryptage performants, et tenir un registre des accès des membres du personnel de l'OIM et des tiers autorisés à traiter des données à caractère personnel.
- Signaler toute activité suspecte à l'informaticien compétent.
- Intervenir dans les meilleurs délais en cas d'incident lié à la sécurité.
- Tenir compte de la sécurité des données dans les stratégies d'élaboration de projets, et prévoir les dépenses nécessaires dans les propositions de projet.
- Tenir à jour un inventaire de l'équipement et des espaces de stockage de données, et le communiquer à l'informaticien compétent.
- Coopérer avec la Division ITC au Siège pour que, d'un bout à l'autre du cycle de traitement, des mesures de sécurité soient appliquées aux données à caractère personnel.

Note : La consultation, le stockage et la transmission de données à caractère personnel hautement sensibles peuvent nécessiter des mesures de sécurité des données plus strictes.

36. Mesures de sécurité physiques

Tous les membres du personnel de l'OIM qui traitent des données à caractère personnel appliqueront les mesures de protection énoncées dans les principes et directives informatiques de l'OIM.

Dossiers papier

Les dossiers papier seront envoyés par les moyens les plus sûrs dont dispose le bureau extérieur pertinent de l'OIM, pour éviter les accès non autorisés, les pertes accidentelles ou les vols.

Moyens d'expédition sûrs :

- Service de messagerie exprès ou, au minimum, courrier recommandé ;
- Conversion des dossiers papier au format électronique :
  - en scannant les dossiers papier et en envoyant le support électronique crypté par messagerie ou par courrier recommandé ; ou

› en scannant les dossiers papier et en envoyant les données cryptées sur un serveur FTP sécurisé[35], c'est-à-dire en transférant les données à caractère personnel d'un ordinateur à un autre au moyen d'un protocole d'échange sécurisé sur Internet.

EXEMPLE :

L'envoi de dossiers papier sensibles concernant des migrants irréguliers peut nécessiter leur conversion au format électronique pour éviter que des données à caractère personnel ne « tombent entre de mauvaises mains » dans les aéroports. Les responsables du traitement des données pourront soit : 1) scanner les dossiers papier sur des CD et crypter ceux-ci avant de les envoyer par messagerie ou courrier recommandé ; ou 2) convertir les dossiers papier au format électronique et utiliser un site FTP comme système d'archivage pour échanger les données à caractère personnel. Même si le site FTP est protégé par un mot de passe, les dossiers n'y sont pas automatiquement cryptés. Les responsables du traitement des données veilleront à ce que les dossiers électroniques soient cryptés avant de communiquer une adresse FTP à des tiers autorisés.

Dossiers électroniques

Les dossiers électroniques et les supports tels que les CD, DVD, mémoires flash, microfiches, bandes vidéo, copies de bandes sonores et autres supports de stockage électronique contenant des données à caractère personnel seront conservés en un lieu sûr pour éviter qu'ils ne soient physiquement endommagés, consultés sans autorisation ou modifiés.

Mesures de protection physiques efficaces :

../ Classifier les dossiers selon le degré de sensibilité approprié ;

../ Limiter l'accès des bâtiments, bureaux et abris au personnel autorisé se prévalant des besoins légitimes du service ;

../ Sécuriser l'accès aux locaux de stockage en exigeant la présentation d'une carte d'identité ;

../ Séparer les données à caractère personnel de celles à caractère non personnel ;

../ Conserver les dossiers papier sous clé dans des coffres, des bibliothèques, des tiroirs, des armoires à classeurs ou des salles d'archives, et les replacer dans un lieu sûr après utilisation ;

../ Surveiller les imprimantes utilisées pour le tirage de données à caractère personnel, et veiller à ce que des méthodes d'élimination appropriées telles que le déchiquetage ou l'incinération soient utilisées pour détruire les documents imprimés ;

../ Conserver un nombre minimum de copies de sauvegarde dans des coffres ignifuges, et les stocker dans un lieu distinct de manière à pouvoir les transporter facilement en cas d'évacuation ou de déménagement ;

[35] L'application FTP (protocole de transfert de fichiers) est un protocole informatique permettant l'échange de fichiers entre des comptes informatiques, le transfert de fichiers entre un compte et un ordinateur de bureau, ou l'accès à des archives sur Internet via une adresse FTP (comparable à une adresse Web ou http://, mais avec le préfixe ftp://). L'ordinateur hôte fait fonction de système d'archivage protégé par un mot de passe et permettant d'envoyer et de télécharger des fichiers.

../ Veiller à ce que les dossiers électroniques soient stockés dans un lieu sûr dont l'accès est réservé au personnel autorisé de l'OIM ;

../ Archiver les fichiers dans un endroit secret auquel seul le personnel autorisé de l'OIM a accès ;

../ Protéger le code des coffres en en limitant l'accès et en le modifiant régulièrement.

EXEMPLE :

L'accès à des répertoires centraux de base de données, tels que MiMOSA ou des systèmes d'archivage, sera protégé par un mot de passe et limité au personnel autorisé de l'OIM.

Ingénierie sociale

Dans le domaine de la sécurité des données, l'ingénierie sociale désigne des pratiques trompeuses mises en œuvre pour amener des personnes par la ruse à révéler des données à caractère personnel ou des codes d'accès.

Les auteurs d'attaques par ingénierie sociale (dits « attaquants ») visent à obtenir un accès non autorisé à des données à caractère personnel.

De manière générale, les attaquants évitent de recourir à l'informatique et misent sur :

- les vulnérabilités de l'être humain ;
- l'incapacité de s'adapter à une culture profondément ancrée dans les technologies de l'information ; et
- une protection négligente des mots de passe.

EXEMPLE :

L'attaquant peut se lier d'amitié avec une personne autorisée à accéder à des espaces de stockage contenant des données à caractère personnel et abuser de sa confiance pour avoir accès à ces données. Il mettra à profit la tendance naturelle de cette personne à choisir des mots de passe qui ont pour elle une signification et qu'un ami peut facilement deviner.

L'être humain est souvent considéré comme le « maillon faible » de tout système de sécurité. Quel que soit le niveau de performance des mesures de sécurité des données, l'attaquant usera de moyens alternatifs pour duper autrui.

Le plus souvent, les pratiques d'ingénierie sociale consistent à :

- faire preuve de persuasion ou se livrer à des manipulations ;
- flatter l'orgueil ;
- imiter une personne occupant un poste de responsabilité ;
- espionner les conversations ;
- épier, c.-à-d. regarder par-dessus l'épaule de quelqu'un pour mémoriser des mots de passe ;

- « fouiller les poubelles », c.-à-d. examiner le contenu des corbeilles à papier pour y trouver des indices permettant de déverrouiller un dispositif de protection par mot de passe ;
- « hameçonner », c.-à-d. prétendre être une source électronique digne de confiance pour tenter d'obtenir frauduleusement des données à caractère personnel.

La divulgation non intentionnelle d'informations à des attaquants peut mettre en danger la vie de personnes concernées, ainsi que celle de membres du personnel de l'OIM et de représentants de tiers autorisés.

Les responsables du traitement des données tiendront compte des pratiques d'ingénierie sociale dans l'évaluation des risques liés à la sécurité des données et mettront en œuvre des stratégies de prévention appropriées.

Les stratégies de prévention sont notamment les suivantes :

../ Expliquer que l'ingénierie sociale est une pratique qui vise à mettre en péril les systèmes garantissant la sécurité des données ;

../ Actualiser les mesures garantissant la sécurité des données afin de lutter contre l'ingénierie sociale ;

../ Bien choisir et protéger le mot de passe ;

../ Préserver le caractère strictement confidentiel des données à caractère personnel ;

../ Eviter de divulguer des données à caractère confidentiel au moyen de lignes téléphoniques non sécurisées ;

../ Soumettre l'accès des locaux à autorisation ;

../ Surveiller l'élimination des données à caractère personnel ;

../ Déchiqueter ou incinérer les données à caractère personnel hautement sensibles.

37. Mesures de sécurité technologiques

Les responsables du traitement des données veilleront à ce que les dossiers électroniques soient protégés par un contrôle strict des accès. L'utilisation de systèmes informatiques, de bases de données et d'autres logiciels pour stocker des dossiers électroniques sera limitée au personnel autorisé de l'OIM. Tous les membres du personnel de l'OIM, y compris les informaticiens, signeront des formulaires de confidentialité visant à protéger les données à caractère personnel[36].

EXEMPLE :

Les fonctionnaires de la Division ITC signeront un accord de confidentialité, et la protection des données figurera dans les orientations concernant le code de conduite établi par la Division ITC et les politiques de l'OIM relatives aux technologies de l'information.

[36] Voir le Modèle 3 pour un formulaire de confidentialité type à l'intention des membres du personnel de l'OIM qui traitent des données à caractère personnel. Les informaticiens se conformeront aux politiques et directives informatiques et s'engageront à préserver la confidentialité des données à caractère personnel lorsqu'ils y auront accès.

Cryptage

Le cryptage consiste à convertir un texte en un code incompréhensible et à protéger le format original du texte au moyen d'une clé.

Les responsables du traitement des données doivent, dans la mesure du possible, encourager l'utilisation d'outils de chiffrement. Voir le Principe 10 pour d'autres méthodes d'élimination d'éléments identifiables avant la transmission/divulgation.

Le personnel de l'OIM qui traite des données à caractère personnel veillera avec l'informaticien compétent à ce que les mesures nécessaires soient prises pour protéger tous les dossiers électroniques avant leur transmission, y compris par le biais du cryptage.

EXEMPLE :

Des outils de cryptage intégrés dans les applications MS Office ou WinZip seront utilisés pour le transfert interne entre membres du personnel de l'OIM. Un système de cryptage plus performant, par exemple PGP (Pretty Good Privacy), sera utilisé pour les données à caractère personnel hautement sensibles.

Des clés de cryptage seront attribuées aux responsables du traitement des données ou aux dépositaires désignés, ainsi qu'aux informaticiens, afin de prévenir tout risque opérationnel au cas où les clés seraient perdues ou égarées et les dépositaires absents. Les clés de cryptage seront conservées en tout temps en un lieu sûr.

Le cryptage est une mesure de protection indispensable qui sera systématiquement utilisée pour protéger les données à caractère personnel contre les accès non autorisés, les modifications, les falsifications et les pertes accidentelles.

L'échange de courriers électroniques sera limité au personnel autorisé de l'OIM, et uniquement en cas de « besoin d'en connaître ». Les destinataires des courriers électroniques seront sélectionnés avec soin pour éviter que des données à caractère personnel confidentielles et secrètes ne soient diffusées dans l'ensemble de l'OIM.

Cryptage partiel

Aux fins des principes de l'OIM, le cryptage partiel s'entend du cryptage d'un nombre limité de zones mémoire électroniques, telles que les dossiers, les fichiers et les applications de bases de données contenant des données à caractère personnel.

EXEMPLE :

Des indicateurs propres à un cas particulier ne seront transférés en interne qu'au personnel autorisé de l'OIM. Les destinataires des courriers électroniques seront sélectionnés avec soin et, si l'identité des personnes concernées apparaît dans le texte d'un courrier électronique, elle sera remplacée par le numéro d'identité attribué par l'OIM. Les modèles MS Excel contenant des indicateurs clés seront cryptés au moyen d'outils appropriés.

Le cryptage partiel est une protection utile qui doit être utilisée pour protéger les zones mémoire électroniques contre les accès non autorisés, les modifications ou les falsifications. Il peut toutefois créer la fausse impression que les données sont sécurisées. C'est pourquoi, les responsables du traitement des données veilleront à ce que des dossiers ou des fichiers cryptés ne soient pas stockés par erreur hors de zones cryptées après leur extraction.

L'accès, le stockage et la transmission de dossiers électroniques feront l'objet d'une protection renforcée par un mot de passe.

En l'absence d'outils de cryptage, des pseudonymes, des mots de passe et des codes seront utilisés pour protéger la confidentialité des données à caractère personnel et l'anonymat des personnes concernées (voir le Principe 10).

Risques liés à la sécurité

Les responsables du traitement des données collaboreront avec l'informaticien compétent pour que les systèmes informatiques, les applications et les logiciels utilisés pour saisir et stocker des données à caractère personnel soient protégés par un antivirus, par des outils de suppression des logiciels espions et des logiciels publicitaires et par un pare-feu[37]. Si ces outils ne sont pas disponibles ou s'ils ne fonctionnent pas, les responsables du traitement des données se mettront immédiatement en relation avec l'informaticien compétent.

Perte et vol

Les informaticiens prendront toutes les mesures raisonnables pour récupérer les dossiers ou fichiers électroniques contenant des données à caractère personnel qui ont été perdus.

Tous les cas de perte ou de vol seront signalés sans retard excessif à l'informaticien compétent.

Les procédures de sécurité élaborées par la Division ITC au Siège, telles que les retouches et les derniers Service Packs, seront suivies pour éviter l'exposition aux risques.

Accès au serveur de l'OIM

L'accès à distance au serveur de l'OIM et l'utilisation d'ordinateurs portables ou de bureau à domicile seront conformes aux règles de sécurité énoncées dans les politiques relatives aux technologies de l'information de l'OIM, les questions informatiques concernant le travail à domicile, et la politique relative au domicile de l'OIM.

[37] En conformité avec les applications relatives aux risques liés à la sécurité autorisées par l'OIM.

Les dossiers électroniques contenant des données à caractère personnel ne seront ni traités ni transmis sans une protection suffisante contre les logiciels malveillants.

L'utilisation de prises Internet et de connexions sans fil non sécurisées pour extraire, échanger, transmettre ou transférer des données à caractère personnel est à éviter.

Le personnel de l'OIM qui traite des données à caractère personnel fera preuve de la prudence requise en se connectant au serveur de l'OIM depuis l'extérieur. Ils vérifieront qu'ils ont correctement fermé leur session ainsi que les fenêtres des navigateurs qu'ils ont ouvertes, et les mots de passe seront toujours protégés.

Ordinateurs portables, téléphones Blackberry, assistants numériques personnels et autres équipements multimédias portables

Les ordinateurs portables, les téléphones Blackberry, les assistants numériques personnels et autres équipements multimédias portables requièrent des mesures de sécurité spéciales, en particulier lorsqu'ils sont utilisés dans un environnement difficile. Les responsables du traitement des données veilleront toujours à ce que les fichiers électroniques contenant des données à caractère personnel soient protégés par un mot de passe, et à ce que les fonctionnalités protégées par un mot de passe[38] soient activées. Les équipements multimédias portables seront entreposés en permanence dans des lieux sûrs et sécurisés.

[38] Pour de plus amples précisions, consulter la Division ITC au Siège de l'OIM, en particulier à propos de l'application des principes et directives informatiques et des mesures de sécurité à prendre pour l'utilisation des appareils portables.

Encadré 20 : Considérations relatives aux dossiers électroniques

- Transmettre et stocker des données à caractère personnel uniquement sur des ordinateurs et des applications de bases de données protégés contre les risques liés à la sécurité.
- Se conformer aux procédures de connexion et aux prescriptions minimales de protection des mots de passe énoncées dans les principes relatifs aux technologies de l'information de l'OIM.
- Utiliser les fonctions de verrouillage automatique de l'ordinateur ou de clôture de session, et veiller à ce que tous les navigateurs soient fermés en cas d'absence du poste de travail, surtout lorsque les ordinateurs sont utilisés en réseau.
- Signaler le caractère confidentiel de tous les courriels contenant des données à caractère personnel en utilisant l'option proposée à cet effet par Microsoft Outlook ou d'autres applications de courrier électronique pour identifier le degré de sensibilité des courriels.
- Adresser les courriels uniquement au personnel autorisé de l'OIM et aux représentants de tiers autorisés.
- Remplacer les identifiants par des codes lors du stockage et de la transmission de données à caractère personnel, surtout lorsqu'il s'agit de catégories de données à caractère personnel hautement sensibles.
- Toujours crypter la transmission des courriels et pièces jointes contenant des données à caractère personnel :
  - *A l'intérieur de l'OIM* : utiliser les fonctions de cryptage des applications MS Office et WinZip et du système PGP ou d'autres applications de cryptage ;
  - *Hors de l'OIM* : utiliser les outils de cryptage les plus performants et veiller à ce que les tiers soient équipés des outils de décryptage appropriés.
- Recourir au cryptage partiel pour protéger les espaces de stockage électroniques et veiller à ce que les données à caractère personnel soient stockées de manière sécurisée dans des dossiers cryptés ou protégés par un mot de passe.
- Sécuriser les équipements multimédias portables et signaler sans retard excessif les pertes ou les vols d'équipement électronique.
- Veiller à ce que les procédures de sauvegarde soient appliquées à tous les dossiers électroniques.
- Eviter d'accéder au serveur de l'OIM au moyen de prises Internet ou de connexions sans fil non sécurisées pour extraire, échanger, transmettre ou transférer des données à caractère personnel.

Note : Les responsables du traitement des données collaboreront avec l'informaticien compétent pour veiller à ce que les outils de cryptage les plus performants soient utilisés pour transférer des données à des tiers hors de l'OIM, car seul un équipement préconfiguré de l'OIM garantit un échange d'informations sécurisé.

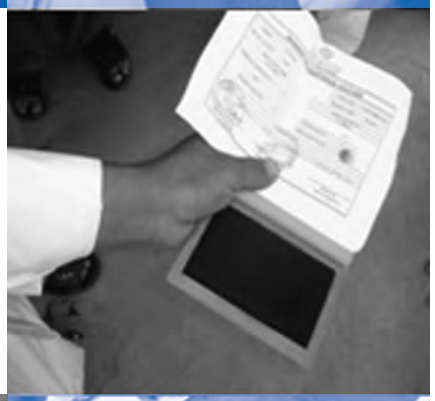
Les données à caractère personnel hautement sensibles ne seront pas stockées sur des appareils portables ou amovibles. Au cas où ce serait inévitable, elles seront transférées dès que possible sur des systèmes informatiques et des applications de bases de données appropriés. Si une mémoire flash, telle qu'une clé USB ou une carte mémoire, est utilisée pour stocker temporairement des données à caractère personnel, elle sera conservée en un lieu sûr, et le dossier électronique sera crypté. Au besoin, il faudra demander conseil à l'informaticien compétent.

Récupération et sauvegarde

Des mécanismes de récupération et des procédures de sauvegarde efficaces seront utilisés pour les dossiers électroniques, et l'informaticien compétent veillera à ce que les sauvegardes soient effectuées régulièrement. La fréquence des sauvegardes dépendra de la sensibilité des données à caractère personnel. La gestion des dossiers électroniques sera automatisée pour faciliter leur récupération dans les cas où les sauvegardes sont difficiles, notamment en raison de coupures de courant régulières, d'une défaillance du système ou d'une catastrophe naturelle. Lorsque les dossiers électroniques et les applications de bases de données ne sont plus nécessaires, le personnel de l'OIM veillera avec l'informaticien compétent à ce qu'ils soient définitivement éliminés.

9

PRINCIPE 9 : CONSERVATION DES DONNEES A CARACTERE PERSONNEL



PRINCIPE 9 : CONSERVATION DES DONNEES A CARACTERE PERSONNEL

Les données à caractère personnel seront conservées aussi longtemps que nécessaire ; elles seront détruites ou rendues anonymes dès que la ou les finalités déterminées pour lesquelles elles ont été recueillies et traitées auront été atteintes. Elles pourront toutefois être conservées pendant une période déterminée additionnelle si l'intérêt de la personne concernée l'exige.

Les responsables du traitement des données surveilleront la conservation et la destruction des données à caractère personnel car un excès de zèle dans l'application du principe de conservation peut conduire à une destruction prématurée de données à caractère personnel. Ils pourront déléguer la surveillance de la conservation des données au personnel autorisé de l'OIM chargé de gérer les contrôles d'accès, de protéger les supports de stockage et de vérifier si les dossiers sont lisibles et compréhensibles.

38. Période de conservation

La conservation des données à caractère personnel est rigoureusement liée à la réalisation des finalités déterminées. Le délai de conservation sera scrupuleusement respecté et sera calculé à partir de la date d'achèvement du projet de l'OIM.

Encadré 21 : Période de conservation

- **10 ans** : dossiers électroniques contenant des données à caractère personnel.
- **8 ans** : dossiers papier contenant des données à caractère personnel.

Note : **Les périodes de conservation peuvent toutefois varier selon les exigences des donateurs.**

Les données à caractère personnel ne doivent pas être conservées pendant une période indéterminée. Les dossiers électroniques et papier et les sauvegardes correspondantes seront détruits ou rendus anonymes dès l'expiration des périodes de conservation.

Le format dans lequel sont conservées les données à caractère personnel est laissé à la discrétion des responsables du traitement des données, qui tiendront compte, entre autres :

- des capacités technologiques du bureau extérieur de l'OIM concerné ;
- des mesures de sécurité des données ;
- des mesures de contrôle des accès ; et
- de l'espace de stockage disponible.

Les responsables du traitement des données veilleront à l'intégrité et à la qualité des dossiers électroniques et papier d'un bout à l'autre du cycle de traitement des données. L'informaticien compétent sera consulté pour que tous les dossiers électroniques soient compatibles avec les technologies informatiques les plus récentes.

Les données à caractère personnel seront conservées dans des lieux sûrs et sécurisés, dans le respect d'indicateurs de confidentialité appropriés et de mesures de contrôle d'accès suffisantes.

Les normes de sécurité électrique et de sécurité incendie énoncées dans les principes et directives informatiques de l'OIM et les lignes directrices de l'Unité de sécurité du personnel (SSU) s'appliqueront aux lieux de stockage. Les volumes de stockage seront limités au minimum nécessaire, et seules les informations essentielles seront conservées.

Les responsables du traitement des données vérifieront si des dossiers électroniques ou papier ont été collectés ou enregistrés en double. Si un scanner est à disposition et que le processus de numérisation n'est pas trop long, les dossiers papier seront convertis au format électronique et conservés sous cette forme pour réduire les volumes de stockage.

La nature des données à caractère personnel, les conditions climatiques et la facilité d'accès du personnel autorisé de l'OIM seront prises en considération lors de la surveillance du stockage des données à caractère personnel.

39. Conservation pendant une période déterminée additionnelle

La conservation de données à caractère personnel pour des finalités déterminées additionnelles sans rapport avec la finalité déterminée initiale ou avec des finalités compatibles requiert le consentement ultérieur des personnes concernées.

Le principe de conservation comporte toutefois une exception dans les cas où l'intérêt supérieur de la personne concernée exige que les données à caractère personnel soient conservées après la réalisation des finalités déterminées du traitement des données.

Encadré 22 : Autres considérations en matière de conservation

- Effectuer une évaluation du rapport risques/avantages.
- Définir la finalité déterminée additionnelle présentant un avantage pour la personne concernée.
- Dûment justifier une conservation plus longue.
- Fixer la durée de la nouvelle période de conservation.

Dans ces conditions, les responsables du traitement :

› Définiront la finalité déterminée additionnelle présentant un avantage pour les personnes concernées.
› Détermineront la période de conservation additionnelle compte tenu de la nature du projet de l'OIM et des avantages tirés d'une conservation plus longue.
› Evalueront le rapport risques/avantages.
› Consulteront l'unité ou le département compétent de l'OIM pour savoir si les personnes concernées peuvent raisonnablement s'attendre à ce que l'OIM utilise leurs données à caractère personnel pendant la période déterminée additionnelle.

Un dépassement de la période de conservation est possible dans les cas où il est nécessaire de conserver des données à caractère personnel pour un usage organisationnel au sein de l'OIM, par exemple aux fins :

- de surveillance et d'évaluation ;
- d'analyse des antécédents ;
- de cartographie des tendances ou schémas migratoires ; et
- d'analyse statistique.

EXEMPLE :

La personne concernée pourrait bénéficier d'un projet ultérieur de l'OIM, si bien que la destruction de ses données à caractère personnel serait non seulement disproportionnée par rapport à ses intérêts, mais aussi coûteuse et pénalisante pour l'OIM.

Les responsables du traitement des données soumettront à l'unité ou au département compétent de l'OIM des rapports d'évaluation sur la conservation des données pour justifier une conservation plus longue.

Tout prolongement de la période de conservation sera approuvé par l'unité ou le département compétent de l'OIM.

40. Méthodes de destruction

Les responsables du traitement des données se demanderont si les données à caractère personnel peuvent être utilisées à des fins d'analyse ou de recherche avant d'autoriser leur destruction.

Lorsqu'ils ne sont plus nécessaires, tous les dossiers et sauvegardes seront détruits ou rendus anonymes.

La destruction de dossiers électroniques et papier est soumise à l'autorisation du responsable du traitement des données après concertation avec l'unité ou le département compétent de l'OIM.

La méthode de destruction dépendra, entre autres :

- de la nature et de la sensibilité des données à caractère personnel ;
- du format et du support de stockage ; et
- du volume des dossiers électroniques et papier.

Les responsables du traitement des données évalueront la sensibilité des données à caractère personnel avant leur destruction, pour veiller à ce que des méthodes appropriées soient utilisées pour les éliminer.

Encadré 23 : Considérations en matière de destruction

- Avant toute destruction, examiner la possibilité d'une utilisation future conformément aux principes de l'OIM.
- Etre certain que les données à caractère personnel ne seront pas requises à des fins organisationnelles (utilisation statistique, surveillance ou évaluation).
- Veiller à ce que les décisions de destruction soient approuvées par l'unité ou le département compétent de l'OIM.
- Evaluer la sensibilité des données et communiquer à l'informaticien compétent une liste des emplacements de stockage électronique subdivisée en catégories.
- Consulter le service informatique pour veiller à ce que des méthodes de destruction appropriées soient suivies pour éliminer les dossiers électroniques.
- Surveiller les méthodes physiques de destruction.
- Veiller à ce que l'externalisation des fonctions de destruction soit régie par des contrats écrits préservant la confidentialité des données à caractère personnel et prévoyant la remise d'un certificat de destruction.
- Surveiller la destruction des fichiers électroniques jusqu'à leur élimination définitive.
- Joindre les documents d'élimination aux rapports finals de projet ou d'évaluation.
- Faire figurer la destruction des données à caractère personnel dans les contrats conclus avec les tiers, et exiger un certificat mentionnant que toutes les copies ont été détruites après la résiliation ou l'expiration du contrat.

Note : Veiller à ce que les tiers remettent des rapports d'élimination et des certificats de destruction, en particulier lorsque la destruction des données à caractère personnel est externalisée.

Destruction des dossiers papier

La destruction des dossiers papier s'effectuera au moyen de méthodes telles que le déchiquetage ou l'incinération, qui ne permettent aucune utilisation ou reconstitution ultérieure. L'évacuation et l'enfouissement des déchets sont à éviter.

Une fois les dossiers papier soigneusement numérisés, toute trace en sera détruite.

Destruction des dossiers électroniques

La destruction des dossiers électroniques sera signalée à l'informaticien compétent, car les fonctionnalités de suppression des systèmes informatiques ne garantissent pas nécessairement une élimination complète.

Les dons d'ordinateurs ou d'équipement électronique autorisés par le donateur du projet de l'OIM donneront lieu à un acte de donation.

EXEMPLE :

Si des données à caractère personnel ont été encodées et téléchargées dans une base de données par un opérateur de saisie des données, les responsables du traitement des données autoriseront leur destruction s'ils le jugent approprié et après avoir vérifié si les données à caractère personnel avaient correctement été enregistrées.

Préalablement au don, le responsable du traitement des données consultera l'informaticien compétent pour que toute trace de données à caractère personnel soit complètement éliminée.

Sur instruction, l'informaticien compétent s'assurera que toute trace de données à caractère personnel a été complètement supprimée des systèmes informatiques et autres logiciels. Les lecteurs de disques et les applications de bases de données seront vidés, et tous les supports réinscriptibles, tels que les CD, les DVD, les microfiches et les cassettes vidéo ou audio utilisés pour stocker des données à caractère personnel, seront vidés de leur contenu avant leur réutilisation[39]. Les mesures physiques de destruction de dossiers électroniques, telles que le recyclage, la pulvérisation ou l'incinération, feront l'objet d'un contrôle strict.

EXEMPLE :

La Division ITC veillera à ce que les dossiers électroniques contenant des données à caractère personnel soient complètement détruits avant que des ordinateurs ne soient donnés ou vendus. En l'absence de méthodes propres à garantir la destruction complète de dossiers électroniques, le disque dur sera retiré de l'ordinateur de façon à éliminer toute trace de données à caractère personnel.

Registres d'élimination

Les responsables du traitement des données s'assureront que tous les contrats de service, mémorandums d'accord, accords et contrats écrits de transfert indiquent une période de conservation aux fins de destruction des données à caractère personnel après que la finalité déterminée[40] a été atteinte. Le tiers restituera les données à caractère personnel à l'OIM et certifiera que toutes les copies desdites données, y compris celles divulguées à ses agents et sous-traitants autorisés, ont été détruites.

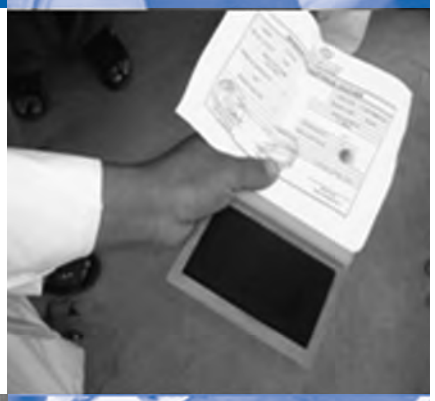
Des registres d'élimination indiquant la date et la méthode de destruction ainsi que la nature des documents détruits seront établis et joints aux rapports de projet ou d'évaluation.

La destruction de grandes quantités de dossiers papier pourra être confiée à des sociétés spécialisées. Dans ces cas, les responsables du traitement des données veilleront à ce que la confidentialité des données à caractère personnel soit garantie par écrit, et à ce que les tiers aient l'obligation contractuelle de remettre les registres d'élimination et les certificats de destruction.

[39] Les procédures et pratiques applicables seront suivies en coordination avec la Division ITC au Siège de l'OIM.
[40] Voir le Modèle 2.1 pour une clause type relative à la destruction des données.

10

PRINCIPE 10 : APPLICATION DES PRINCIPES



PRINCIPE 10 : APPLICATION DES PRINCIPES

Ces principes s'appliqueront aux dossiers électroniques et papier de données à caractère personnel, et pourront être complétés par des mesures de protection additionnelles selon, entre autres, la sensibilité des données à caractère personnel. Ils ne s'appliqueront pas aux données à caractère non personnel.

Les données à caractère personnel doivent être clairement distinguées des données à caractère non personnel, qui ne sont pas régies par les principes de l'OIM.

Les données à caractère personnel qui ont été rendues anonymes de telle sorte que les personnes concernées ne soient plus identifiables, restent soumises aux principes de l'OIM jusqu'à leur élimination effective.

Le codage, la pseudonymisation et l'anonymisation des données sont trois méthodes courantes d'élimination des caractéristiques identifiables qui sont utilisées pour préserver la confidentialité des données à caractère personnel et l'anonymat des personnes concernées.

Encadré 24 : Dépersonnaliser les données à caractère personnel

- Choisir la méthode appropriée pour dépersonnaliser les données :
  - codage des données ;
  - pseudonymisation ;
  - anonymisation.
- Désigner un dépositaire, afin de protéger les mots de passe et les principaux codes.
- Dans la mesure du possible, ne communiquer à des tiers que des données globales anonymes.
- Etre certain que l'anonymat est garanti, avant toute divulgation à des tiers.
- Utiliser des pseudonymes lors de la présentation d'études de cas et de la transmission de données à caractère personnel, surtout en cas d'absence de cryptage.
- Ne divulguer l'identité des personnes concernées qu'avec leur consentement exprès.

41. Codage des données

Le codage des données consiste à remplacer l'identité des personnes concernées ainsi que d'autres caractéristiques identifiables par des labels ou des chiffres et des lettres sans lien, afin d'empêcher ou de compliquer considérablement toute identification.

Le codage des données comporte deux étapes :

- La division des données à caractère personnel en ensembles de données gérables ; et
- La création et l'attribution de codes aux ensembles de données.

Les responsables du traitement des données ou les dépositaires désignés stockeront de manière sécurisée les mots de passe ou les clés permettant de décoder les ensembles de données. Les responsables du traitement des données veilleront à ce que les dépositaires surveillent tout à la fois les données codées et les données à caractère personnel enregistrées dans les systèmes informatiques ou les applications de bases de données.

Le codage des données est une mesure de sécurité et un outil de gestion utilisé pour stocker et transmettre des données à caractère personnel. Cette méthode est utile pour stocker des données à caractère personnel dans des applications de bases de données, parce qu'elle permet de bien gérer de grandes quantités de données à caractère personnel tout en offrant la possibilité de séparer les données à caractère personnel des données à caractère non personnel.

EXEMPLE :

Lors de l'attribution des codes, les données à caractère personnel pourront être séparées des données à caractère non personnel et stockées séparément dans un module de base de données crypté.

42. Pseudonymisation

La pseudonymisation consiste à remplacer les vrais noms par des noms fictifs, afin de dissimuler des caractéristiques d'identification et des faits réels ayant trait à des personnes concernées.

Afin d'éviter que l'identification des personnes concernées n'ait des conséquences néfastes, les responsables du traitement des données prendront l'habitude d'utiliser des pseudonymes pour présenter des études de cas et des rapports aux donateurs.

EXEMPLE :

En l'absence de cryptage, des pseudonymes seront utilisés dans les courriels adressés au personnel autorisé de l'OIM.

43. Anonymisation

L'anonymisation consiste à supprimer tous les identifiants et codes personnels de telle sorte qu'il n'existe aucune probabilité raisonnable que les personnes concernées soient identifiées ou retrouvées.

Les données à caractère personnel doivent être rendues anonymes de telle sorte que l'on ne puisse plus les relier à une personne concernée, sauf en mobilisant des compétences, un temps et des efforts démesurés.

Avant de communiquer des données anonymes à des tiers ou de les mettre à disposition en vue de leur publication, les responsables du traitement des données tiendront toujours compte des méthodes complexes susceptibles d'être mises en œuvre pour retrouver des personnes concernées (voir le point 2 pour une explication des méthodes complexes).

Finalité statistique et opérationnelle

Des données globales anonymes pourront être utilisées aux fins d'analyse statistique, d'évaluation, de rapport, de gestion de projets et de mise en œuvre de services connexes au profit

de personnes concernées. Les rapports statistiques écrits ou les rapports statistiques globaux établis par des applications de bases de données pourront être diffusés à l'intérieur de l'OIM.

En l'absence de consentement, seules des données globales anonymes qui ne permettent pas d'identifier ou de retrouver des personnes concernées pourront être publiées et diffusées.

Lorsqu'ils diffusent des données globales anonymes à des tiers, les responsables du traitement des données prendront toutes les précautions voulues, feront preuve de discernement, et prendront toutes les dispositions raisonnables pour que les ensembles de données ne contiennent aucune trace de données à caractère personnel.

EXEMPLE :

L'ensemble de données statistiques anonymes d'une étude de cas médicale concernant 15 femmes de 30 à 40 ans habitant une communauté rurale isolée où vivent 60 femmes, pourrait être déchiffré pour connaître l'identité des 15 femmes.

La question primordiale est de savoir s'il existe une probabilité raisonnable que la personne concernée puisse être retrouvée après une analyse minutieuse de l'ensemble de données globales anonymes.

Les responsables du traitement des données veilleront à ce que la divulgation de données globales anonymes à des tiers soit régie par une obligation contractuelle écrite car, avec suffisamment de détermination, il est possible de déchiffrer des données anonymes pour identifier et retrouver des personnes concernées.

44. Données migratoires

Les données migratoires s'entendent d'une compilation de divers ensembles de données globales conservées à l'intérieur de l'OIM à des fins historiques ou statistiques.

Les données migratoires sont de nature statistique ; elles sont recueillies dans le cadre des différents projets de l'OIM pour développer une expertise dans le domaine de la migration. Les données migratoires utilisées pour établir des tendances de la migration ne sont pas soumises aux principes de l'OIM dès lors qu'elles ne sont pas fondées sur des données à caractère personnel se rapportant à des personnes concernées et qu'elles n'en supposent pas l'usage.

Les données migratoires qui peuvent servir à identifier l'itinéraire suivi par une personne concernée, ou à établir un lien entre des mouvements migratoires et une personne concernée, sont soumises aux principes de l'OIM.

45. Publication

L'identité des personnes concernées et toutes les caractéristiques identifiables seront supprimées avant toute publication, surtout s'il s'agit de cas hautement sensibles ou de personnes vulnérables, telles que des victimes de la traite.

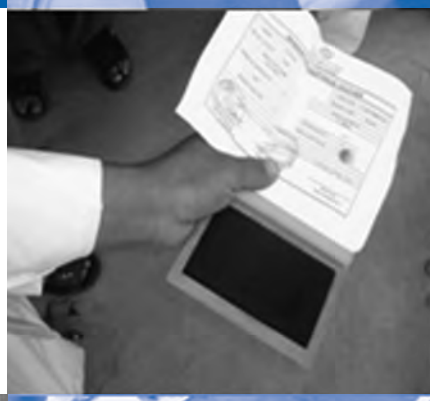
A moins que les personnes concernées ne consentent expressément à leur publication, leurs données à caractère personnel et leur image n'apparaîtront pas dans des documents accessibles à tous ni dans des documents d'information tels que les états actualisés des projets, les rapports de projet, les bulletins d'information, les résumés de dossier ou les communiqués de presse.

En l'absence de consentement, les personnes concernées seront à tout le moins informées de la diffusion de leur image avant toute publication (voir aussi le Principe 4).

EXEMPLE :

Dans la mesure du possible, seuls des ensembles de données cumulées, et non pas des renseignements précis et des données à caractère personnel, pourront figurer dans les rapports aux donateurs. Il se peut toutefois que la nature de l'activité menée par l'OIM et les exigences du donateur nécessitent une divulgation complète des données à caractère personnel. Dans ce cas, les personnes concernées seront informées de cette divulgation au moment de la collecte des données, et leur consentement exprès devra être obtenu.

11



PRINCIPE 11 :
PROPRIETE DES DONNEES A CARACTERE PERSONNEL

PRINCIPE 11 : PROPRIETE DES DONNEES A CARACTERE PERSONNEL
L'OIM est propriétaire des données à caractère personnel recueillies directement auprès des personnes concernées ou recueillies pour le compte de l'OIM, sauf accord contraire conclu par écrit avec un tiers.

La présomption de propriété en tant que norme institutionnelle permettra à l'OIM de conserver la propriété des données à caractère personnel en cas d'ambiguïté ou de silence dans les contrats conclus avec des tiers. La mémoire institutionnelle de l'Organisation et son mandat spécifique dans le domaine de la migration s'en trouveront également renforcés.

46. Clauses de propriété

En l'absence d'exigences du donateur ou d'obligation contractuelle écrite concernant la cession de données à caractère personnel, les responsables du traitement des données feront valoir le droit de propriété et incorporeront une clause de réserve de propriété[41] dans les contrats conclus avec les donateurs, les contrats de service, les mémorandums d'accord et les accords subsidiaires.

Les contrats écrits conclus avec les agents (fournisseurs de services/consultants), les partenaires d'exécution et autres tiers comprendront une clause de réserve de propriété et une clause de destruction. Ils indiqueront clairement que les données à caractère personnel recueillies au nom de l'OIM devront être restituées à l'Organisation après l'expiration ou la résiliation du contrat.

Les relations avec les partenaires de l'OIM et les partenaires d'exécution pourront avoir pour objet la collecte de différentes catégories de données à caractère personnel auprès des mêmes personnes concernées. Dans ces cas, le tiers pourra être propriétaire des données à caractère personnel divulguées à l'OIM. Les responsables du traitement des données veilleront néanmoins à ce que l'OIM se réserve le droit de propriété sur les catégories de données à caractère personnel qui seront recueillies ultérieurement par elle-même ou en son nom.

Tout contrat écrit en vigueur qui est silencieux sur les questions de propriété sera, dans la mesure du possible, complété par un accord subsidiaire qui prévoit un droit de propriété sur les données à caractère personnel et en précise le contenu.

L'OIM a intérêt à conserver la propriété des données à caractère personnel recueillies auprès des personnes concernées dans le cadre de ses activités.

[41] Voir le Modèle 2.1 pour une clause type de réserve de propriété qui sera incorporée dans tous les accords et mémorandums d'accord, y compris les contrats conclus avec les partenaires d'exécution, les partenaires de l'OIM, les donateurs, les fournisseurs de services, les consultants et autres tiers.

Encadré 25 : Considérations en matière de propriété

- Clarifier la question du droit de propriété en cas d'ambiguïté.
- Faire valoir le droit de propriété par écrit.
- Compléter les contrats en vigueur par des contrats subsidiaires si les contrats initiaux ne contiennent aucune clause de propriété.
- S'il y a lieu, s'assurer que tous les contrats écrits conclus avec des tiers contiennent une clause de réserve de propriété et une clause de destruction, et que les données à caractère personnel sont restituées à l'OIM ou détruites après la réalisation des finalités déterminées.

EXEMPLE :

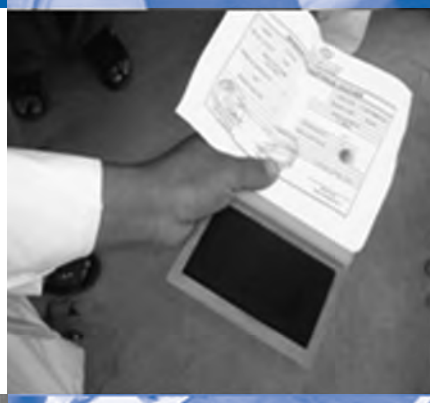
Les contrats conclus avec des consultants chargés de recherche stipuleront que l'OIM se réserve tous les droits de propriété ; que les données à caractère personnel seront restituées à l'OIM après la réalisation des termes du contrat ; et que des certificats seront remis attestant la destruction de toutes les copies de données à caractère personnel.

EXEMPLE :

En sa qualité de partenaire de l'OIM, le Haut-Commissariat des Nations Unies pour les réfugiés (HCR) peut être amené à divulguer à l'Organisation des données à caractère personnel pour faciliter le transport de réfugiés. Si, par la suite, l'OIM recueille des données médicales auprès de ces réfugiés, la propriété de ces données lui reviendra. Les responsables du traitement des données veilleront à ce que ce droit de propriété soit réservé et garanti par écrit.

12

PRINCIPE 12 :
SURVEILLANCE, RESPECT ET RECOURS INTERNES



PRINCIPE 12 : SURVEILLANCE, RESPECT ET RECOURS INTERNES

Un organe indépendant sera nommé pour surveiller l'application de ces principes et examiner les plaintes. Des correspondants pour la protection des données seront désignés pour apporter leur concours à la surveillance et à la formation. Des mesures seront prises pour remédier à toute collecte ou tout traitement illicite de données, ainsi qu'à toute atteinte aux droits et intérêts de la personne concernée.

Les responsables du traitement des données encourageront la formation et l'établissement de rapports réguliers afin de surveiller l'application des principes de l'OIM.

47. Formation à la protection des données

Une formation à la protection des données sera organisée à toutes les étapes du cycle de traitement des données, dès l'élaboration et la mise en œuvre des projets et jusqu'à l'évaluation et l'établissement des rapports.

> **La formation est un outil essentiel qui servira à insuffler une « culture de la protection des données » au sein de l'OIM.**

La protection des données sera intégrée dans les séances de formation existantes, et les propositions de projet prévoiront un montant suffisant pour couvrir les coûts de séances de formation indépendantes, si nécessaire. Pendant les séances de formation, les formateurs distribueront des questionnaires détaillés pour savoir quelles pratiques de protection des données sont suivies dans les différents bureaux extérieurs de l'OIM. Les enquêteurs et les autres personnes associées à la collecte de données, ainsi que les nouveaux membres du personnel de l'OIM et tous ceux qui sont autorisés à traiter des données à caractère personnel bénéficieront d'une orientation sur les procédures à suivre pour adopter les meilleures pratiques et respecter les principes de l'OIM.

Il sera peut-être utile d'organiser des séances de formation conjointes avec les agents (fournisseurs de services/consultants), les partenaires d'exécution, les partenaires de l'OIM, les donateurs et les autorités gouvernementales des pays d'opération et des pays hôtes. Elles permettront de faire connaître les principes de l'OIM et de promouvoir la coopération en vue de leur application effective.

Les formations qui relèvent des secteurs de services de l'OIM traiteront également des mesures de protection des données afin de protéger les données à caractère personnel des participants. Si des listes des participants sont nécessaires à l'établissement de rapports aux donateurs, ou si les noms et les coordonnées des participants doivent être mentionnés dans les rapports de formation et les publications, les personnes concernées en seront informées, et la ou les finalités visées ou prévues leur seront communiquées ; leur consentement devra être obtenu lors de la collecte et de la signature des états de présence.

48. Respect

Les chefs de mission/bureau et les approbateurs de projet ou le personnel désigné de l'unité, du département ou du bureau régional de l'OIM examineront toutes les propositions de projet pour s'assurer que la protection des données est dûment prise en compte dans les stratégies d'élaboration de projets, les activités de projet et les budgets.

Les dépenses indispensables liées à la protection des données concernent, entre autres :

- les mesures de sécurité des données ;
- le matériel et/ou les logiciels informatiques ;
- les capacités du personnel ; et
- les formations.

Les indicateurs de respect sont notamment les suivants :

../ Diffuser l'information et mettre en œuvre une formation continue ;
../ Distribuer des questionnaires détaillés pour connaître les pratiques de traitement des données suivies dans les différents bureaux extérieurs de l'OIM[42] ;
../ Effectuer systématiquement des audits internes en distribuant des listes de vérification à intervalles réguliers ;
../ Soumettre des rapports d'évaluation en vue des audits annuels relatifs à la protection des données ;
../ Veiller à ce que la protection des données soit prise en compte dans les stratégies d'élaboration de projets et les propositions de projet formulées conformément aux considérations politiques de l'OIM ;
../ Budgétiser les dépenses absolument nécessaires pour appliquer les principes de l'OIM ;
../ Mentionner les pratiques de protection des données dans les évaluations de projet internes/externes, ainsi que dans les rapports réguliers sur l'avancement des projets qui doivent être établis selon la procédure mise en place à cette fin à l'OIM.

[42] Il sera ainsi possible d'approuver et de surveiller la destruction de dossiers électroniques ou papier obsolètes.

Encadré 26 : Considérations en matière de respect et de surveillance

- Encourager la coopération entre tous les membres du personnel de l'OIM et les tiers autorisés.
- Entretenir des relations avec les donateurs et les partenaires de l'OIM, les informer et leur expliquer que les principes de l'OIM s'appliquent à tous les projets et s'imposent à tous les bureaux de l'OIM.
- Nommer des correspondants pour la protection des données.
- Effectuer des évaluations régulières en distribuant des listes de vérification.
- Etablir des rapports réguliers selon la procédure mise en place à cette fin à l'OIM.
- Mentionner la protection des données dans les rapports et les évaluations de projet.
- Encourager les audits annuels et signaler les plaintes et les pratiques douteuses en matière de protection des données.

Note : Toujours demander conseil à l'unité ou au département compétent de l'OIM, à LEG et à la Division ITC, au Siège, pour garantir le respect des principes de l'OIM.

La fréquence des rapports et des évaluations de projet variera selon la durée du projet de l'OIM et les exigences des donateurs. Les rapports d'évaluation établis aux fins d'audit interne de projets ne divulgueront que des données globales non personnelles et comprendront, entre autres, une étude des mesures de sécurité prises et une évaluation des pratiques de protection des données.

49. Surveillance

Correspondants pour la protection des données

Les représentants régionaux veilleront à ce que des correspondants pour la protection des données (« correspondants ») soient nommés pour faciliter la surveillance de l'application des principes de l'OIM.

Un correspondant par région devrait suffire, sauf si la taille de la région ou le nombre de projets régionaux traitant des données à caractère personnel nécessitent plusieurs correspondants. Selon le nombre de projets de l'OIM traitant des données à caractère personnel, le correspondant désigné pourra déléguer certaines de ses tâches à des sous-correspondants autorisés.

Les tâches des correspondants seront notamment les suivantes :

../ Bien connaître les règles de protection des données ;
../ Surveiller les pratiques de protection des données suivies dans la région de l'OIM concernée ;
../ Promouvoir les principes de l'OIM et analyser les besoins de formation ;
../ Recueillir les rapports d'évaluation auprès des responsables du traitement des données aux fins d'audit de protection des données ;
../ Faire des recommandations sur la base de la situation du pays et de l'expérience dans la région ;
../ Contribuer à l'examen des propositions de projet sous l'angle de la protection des données.
../ Consulter LEG sur l'application des principes de l'OIM, en particulier dans les cas complexes.

Les correspondants exerceront des fonctions consultatives pour accélérer le processus de décision sur les questions liées à la protection des données et assurer le relais entre le Siège et les bureaux extérieurs de l'OIM, en particulier dans les situations appelant une réponse immédiate. LEG et l'unité ou le département compétent de l'OIM apporteront aux correspondants tout le soutien dont ils ont besoin.

Audits de protection des données

Afin de garantir le respect des principes de l'OIM dans toute l'Organisation, la protection des données figurera parmi les domaines régulièrement visés par les audits annuels. L'organisme de vérification chargé des audits annuels sera indépendant et impartial.

L'organisme de vérification devra notamment :

../ Contrôler systématiquement le respect des principes de l'OIM ;
../ Enquêter sur toute violation grave ;
../ Evaluer l'efficacité des pratiques de traitement des données.

Tous les rapports d'évaluation des données et les plaintes justifiant une enquête seront soumis à l'organisme de vérification avant la date de l'audit. L'intensité de l'audit de protection des données dépendra de la nature des données à caractère personnel traitées, de la technologie utilisée pour garantir la sécurité des données, des conséquences de pratiques de traitement des données inappropriées, et des coûts engendrés par les audits annuels.

50. Recours internes

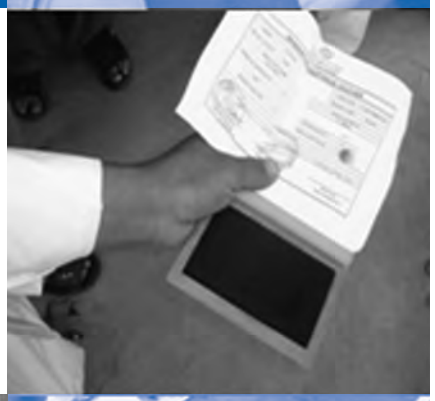
Le non-respect des principes de l'OIM et le traitement illicite de données seront immédiatement signalés au responsable du traitement des données, qui enquêtera sur les plaintes sans retard excessif.

S'il s'avère qu'une plainte est justifiée, des mesures appropriées seront prises, ainsi que des suggestions et recommandations visant à modifier les politiques et les pratiques.

Toute atteinte importante ou grave aux droits et intérêts d'une personne concernée ayant pour effet de porter préjudice à celle-ci, à un membre du personnel de l'OIM ou à un tiers autorisé sera signalée à LEG et au Bureau de l'Inspecteur général, au Siège. Les membres du personnel de l'OIM impliqués dans une violation grave des droits et intérêts d'une personne concernée pourront faire l'objet d'une mesure disciplinaire.

13

PRINCIPE 13 : EXCEPTIONS



PRINCIPE 13 : EXCEPTIONS

Toute intention de déroger à ces principes doit être soumise au préalable, pour approbation, au Bureau des affaires juridiques de l'OIM ainsi qu'à l'unité ou au département compétent au Siège de l'OIM.

Les cas exceptionnels dans lesquels il est nécessaire de déroger aux principes de l'OIM seront systématiquement soumis, pour approbation, à LEG et à l'unité ou au département compétent de l'OIM. Si la dérogation requiert le consentement de la personne concernée, les responsables du traitement des données veilleront à l'obtenir, dans la mesure du possible, avant la dérogation.

51. Intention de déroger

Une dérogation aux principes de l'OIM ne sera envisagée que si le risque d'atteinte à la vie privée des personnes concernées et à la confidentialité des données à caractère personnel est relativement faible, et qu'il existe des intérêts concurrents qui priment les droits et intérêts des personnes concernées. Au nombre des intérêts concurrents figurent, entre autres, des considérations d'intérêt général ou des menaces imminentes pour la vie, la santé et la sécurité des personnes concernées, des membres du personnel de l'OIM et des tiers autorisés.

Les responsables du traitement des données procéderont à une évaluation du rapport risques/avantages en coordination avec l'unité ou le département compétent de l'OIM, afin de déterminer si la dérogation est raisonnable et justifiable.

L'évaluation du rapport risques/avantages sera fondée sur les principes du caractère raisonnable et de la proportionnalité. L'avantage apporté à la personne concernée sera le critère déterminant, et toutes les circonstances du moment seront prises en considération.

Encadré 27 : Considérations en matière de dérogation

- L'avantage apporté aux personnes concernées et au groupe de population cible est primordial.
- Les menaces pour la vie, la santé et la sécurité des personnes concernées, du personnel de l'OIM et des représentants de tiers autorisés.
- L'inexistence de moyens de rechange pour atteindre la finalité déterminée et les objectifs du projet de l'OIM.
- La dérogation est raisonnable au vu des circonstances du moment.
- Les incidences de la dérogation sur la protection des données.
- La proportionnalité entre les limitations des droits et intérêts des personnes concernées et les avantages apportés par la dérogation.
- Les avantages apportés par la dérogation doivent toujours l'emporter sur les incidences que cette dérogation aura sur les droits et intérêts des personnes concernées.

Note : Toute dérogation, surtout si elle est liée à l'intérêt général et à la santé et la sécurité publiques, doit être soumise à LEG pour approbation.

Les limitations des droits et intérêts de la personne concernée seront toujours proportionnelles aux avantages tirés de la dérogation.

Les facteurs à prendre en considération pour justifier le caractère raisonnable d'une dérogation sont notamment :

../ La nature des données à caractère personnel ;
../ Les circonstances du moment ;
../ La nécessité pressante de déroger aux principes de l'OIM ;
../ La finalité atteinte par la dérogation ;
../ La nature et l'étendue de la dérogation ;
../ Le lien entre la dérogation et les finalités déterminées de la collecte et du traitement des données ;
../ La proportionnalité entre l'étendue de la dérogation et sa finalité ;
../ Une atteinte minime à la protection des données et aux droits et intérêts des personnes concernées.

Des solutions de rechange seront envisagées avant l'approbation de la dérogation.

La décision de déroger doit être équitable et suffisamment justifiée car toute décision arbitraire sera incompatible avec la finalité des principes de l'OIM.

52. Conclusion

Pour s'assurer que les pratiques de traitement des données sont conformes aux mesures de protection des données énoncées dans le présent Manuel, les responsables du traitement des données pourraient s'aider d'une liste de vérification concernant la protection des données[43]. Celle-ci sera signée par l'administrateur de projet puis stockée en un lieu sûr avec les dossiers électroniques ou papier aux fins de surveillance, d'évaluation et d'établissement de rapports.

[43] Voir la Liste de vérification 3 pour un liste de vérification type concernant la protection des données.

ANNEXE A

INSTRUMENTS INTERNATIONAUX

DROITS LIES A LA PROTECTION DE LA VIE PRIVEE		
1948	Déclaration universelle des droits de l'homme	Articles 7, 12, 13
1950	Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales	Article 8
1969	Convention américaine relative aux droits de l'homme	Article 11
1966	Pacte international relatif aux droits économiques, sociaux et culturels	
1966	Pacte international relatif aux droits civils et politiques	Articles 12, 17, 26
1988	Comité des droits de l'homme des Nations Unies, Observation générale n° 16 du PIDCP, article 17 (droit à la vie privée)	Article 17
1989	Convention relative aux droits de l'enfant	Articles 2, 12, 16
1990	Convention internationale sur la protection des droits de tous les travailleurs migrants et des membres de leur famille	Articles 1, 8, 14
PROTECTION DES DONNEES		
1980	Lignes directrices de l'Organisation de coopération et de développement économiques (OCDE) régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel	
1981	Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, telle que modifiée par le Protocole additionnel	
1990	Principes directeurs des Nations Unies pour la réglementation des fichiers informatisés contenant des données à caractère personnel	
1995	Directive 95/46/CE du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données	
2000	Charte des droits fondamentaux de l'Union européenne (article 8 : Protection des données à caractère personnel)	
2000	Règlement (EC) n° 45/2001 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données	
2001	Décision de la Commission relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers en vertu de la directive 95/46/CE	
2002	Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information	
2005	Comité des droits de l'enfant, Observation générale n° 6 (2005), Traitement des enfants non accompagnés et des enfants séparés en dehors de leur pays d'origine	
2006	Directive 2006/24/CE du Parlement européen et du Conseil sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE	
2007	Principes de Paris – Principes directeurs relatifs aux enfants associés aux forces armées ou aux groupes armés	
2010	Décision de la Commission du 5 février 2010 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers en vertu de la directive 95/46/CE du Parlement européen et du Conseil	

* ***Note :*** La Directive 95/46/CE du Parlement européen et du Conseil est l'instrument relatif à la protection des données le plus complet. Elle fait actuellement l'objet d'une révision afin de : renforcer les droits de la personne ; renforcer la dimension « marché intérieur » de la protection des données ; réviser les règles de protection des données dans les domaines de la coopération policière et judiciaire en matière pénale ; tenir compte de la dimension mondiale de la protection des données ; et renforcer le cadre institutionnel en vue de l'application effective des règles de protection des données. Pour plus d'informations, prière de consulter la Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social et au Comité des régions : « Une approche globale de la protection des données à caractère personnel dans l'Union européenne », COM (2010) 609 final, disponible à l'adresse http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_fr.pdf.

LOIS NATIONALES RELATIVES A LA PROTECTION DES DONNEES

Albanie : Loi sur la protection des données à caractère personnel nº 9887 de 2008

Allemagne : Loi fédérale sur la protection des données de 2001

Argentine : Loi sur la protection des données à caractère personnel nº 25.326 de 2000

Arménie : Loi de la République d'Arménie sur la protection des données à caractère personnel de 2002

Australie : Loi sur la protection de la vie privée de 1988, modifiée par la Loi de 2000 modifiant la législation sur la protection de la vie privée (secteur privé)

Autriche : Loi sur la protection des données de 2000

Bahamas : Protection des données (Loi sur la protection des données à caractère personnel de 2003)

Belgique : Loi du 8 décembre 1992 relative à la protection des données à l'égard du traitement de données à caractère personnel, modifiée par la Loi du 11 décembre 1998 transposant la Directive 95/46/CE

Bosnie-Herzégovine : Loi sur la protection des données à caractère personnel de 2001

Brésil : Loi de 1997 d'Habeas Data

Bulgarie : Loi de 2001 sur la protection des données à caractère personnel (avec modifications jusqu'en 2006)

Canada : Loi sur la protection des renseignements personnels et les documents électroniques (LPRDE) de 2000

Chili : Loi sur la protection de la vie privée (Ley sobre protección de la vida privada) n° 19.628 de 1999

Chypre : Loi sur le traitement des données à caractère personnel (protection des personnes) nº 138(1) de 2001 (telle que modifiée en 2003)

Colombie : Loi 1266 de 2008 (Loi d'Habeas Data)

Costa Rica : Loi sur la protection des personnes contre le traitement des données à caractère personnel de 2009

Corée (République de) : Loi sur la promotion de l'utilisation des réseaux d'information et de communications et la protection des données de 2000 (telle que modifiée en 2005)

Croatie : Loi sur la protection des données à caractère personnel de 2003 (telle que modifiée en 2006)

Danemark : Loi sur le traitement des données à caractère personnel de 2000 (Loi nº 429 du 31 mai 2000) (telle que modifiée jusqu'en 2007)

Emirats arabes unis : Loi sur la protection des données de 2007

Espagne : Loi organique 15/99 du 13 décembre 1999 sur la protection des données à caractère personnel

Estonie : Loi sur la protection des données à caractère personnel de 2003

Etats-Unis d'Amérique : Loi de 1974 sur la protection de la vie privée ; Loi de 1996 relative à la transférabilité de l'assurance maladie et à la responsabilité des assureurs

(HIPAA) ; règles de 2000 concernant la confidentialité des informations sanitaires identifiables de façon individuelle (Normes de l'HIPAA) et les Normes 2002 de l'HIPAA (CFR 45, section 160 et sous-sections A et E de la section 164)

Ex-République yougoslave de Macédoine : Loi sur la protection des données à caractère personnel de 2005

Fédération de Russie : Loi fédérale de la Fédération de Russie n° 152-FZ du 27 juillet 2006 sur les données à caractère personnel

Finlande : Loi sur la protection des données à caractère personnel (523/1999) (telle que modifiée en 2000)

France : Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

Grèce : Loi nº 2472/1997 sur la protection des personnes à l'égard du traitement des données à caractère personnel, telle que modifiée par les lois 2819/2000 et 2915/2000

Hongrie : Loi nº LXIII de 1992 sur la protection des données à caractère personnel et l'accès du public aux données d'intérêt public modifiée par la Loi nº XLVIII de 2003

Islande : Loi sur la protection des personnes à l'égard du traitement des données à caractère personnel de 2000 (Loi n° 77/2000)

Irlande : Loi sur la protection des données de 1988 (telle que modifiée en 2003)

Israël : Loi sur la protection de la vie privée de 1981 (telle que modifiée en 1985 et en 1996)

Italie : Code italien de protection des données à caractère personnel (Décret législatif n° 196 du 30 juin 2003)

Japon : Loi sur la protection des données à caractère personnel de 2003 (en vigueur depuis le 1er avril 2005)

Lettonie : Loi sur la protection des données à caractère personnel de 2000 (telle que modifiée en 2002)

Lituanie : Loi sur la protection des données à caractère personnel de 1996 (telle que modifiée en 2008)

Luxembourg : Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel

Malte : Loi sur la protection de données de 2001 (entrée en vigueur en 2003)

Maurice : Loi sur la protection des données de 2004

Mexique : Loi fédérale sur la protection des données à caractère personnel de 2010

Moldova (République de) : Loi nº 17-XVI du 15 février 2007 sur la protection des données à caractère personnel (telle que modifiée par la Loi n° 141-XVI de 2008)

Maroc : Loi nº 09-08 de 2009 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel

Nouvelle-Zélande : Loi sur la protection de la vie privée de 1993

Norvège : Loi sur la protection des données à caractère personnel de 2000

Pakistan : Loi sur la protection et la sécurité des données électroniques de 2005

Panama : Loi sur la protection des données à caractère personnel de 2002

Paraguay : Règlement sur les données à caractère personnel de 2000

Pays-Bas : Loi sur la protection des données à caractère personnel de 2000 (entrée en vigueur en 2001)

Pérou : Loi sur la protection des données de juillet 2001 (n° 27.489[4])

Pologne : Loi sur la protection des données à caractère personnel (telle que modifiée en 2004)

Portugal : Loi relative à la protection des données à caractère personnel de 1998 (Loi 67/98 du 26 octobre)

République tchèque : Loi sur la protection des données à caractère personnel n° 101 de 2000 (Loi n° 101 du 4 avril 2000 sur la protection des données à caractère personnel et sur la modification d'autres lois y afférentes)

Roumanie : Loi nº 677/2001 de 2001 sur la protection des personnes à l'égard du traitement des données à caractère personnel et la libre circulation de telles données

Royaume-Uni de Grande-Bretagne et d'Irlande du Nord : Loi sur la protection des données de 1998

Sénégal : Loi n° 2008-12 du 25 janvier 2008 portant sur la protection des données à caractère personnel

Serbie : Loi sur la protection des données à caractère personnel de 2008

Slovaquie : Loi nº 428 de 2002 relative à la protection des données à caractère personnel (nº 428/2002 Coll.) (telle que modifiée en 2005)

Slovénie : Loi sur la protection des données à caractère personnel de 1999 (telle que modifiée jusqu'en 2004)

Suède : Loi sur la protection des données de 1998

Suisse : Loi fédérale sur la protection des données de 1992

Tunisie : Loi portant sur la protection des données à caractère personnel (Loi n° 2004-63 du 27 juillet 2004)

Ukraine : Loi sur la protection des données dans les systèmes automatisés de 1994 (telle que modifiée en 2004)

Uruguay : Loi 17838 de 2004 sur la protection des données à caractère personnel utilisées dans les communiqués commerciaux et dans les procédures en habeas corpus (telle que modifiée par la Loi n°18.331 de 2008 sur la protection des données).

***Note :** Cette liste de lois nationales relatives à la protection des données n'est pas exhaustive. Un certain nombre de pays ont inscrit des dispositions sur la vie privée dans leur constitution, dans leur législation sur les télécommunications ou dans des lois traitant de questions se rapportant à la protection des données. D'autres pays, comme la Chine, la Malaisie, l'Afrique du Sud ou la Thaïlande, ont entrepris d'élaborer des lois sur la protection des données. Prière de consulter également le site : http://heatmap.forrestertools.com/.

GLOSSAIRE

Accord subsidiaire : Accord amiable juridiquement contraignant qui complète un mémorandum d'accord ou un contrat.

Agent : Personne physique ou morale, gouvernement ou autre entité ayant directement reçu l'autorisation d'agir au nom du responsable du traitement des données dans le but d'atteindre la ou les finalités déterminées initiales pour lesquelles des données à caractère personnel sont recueillies et traitées.

Anonymat : L'identité personnelle ou les données identifiables relatives à une personne concernée sont inconnues.

Attaquant : voir Auteur d'attaques par ingénierie sociale

Auteur d'attaques par ingénierie sociale : Personne pratiquant l'ingénierie sociale dans le but d'obtenir un accès non autorisé à des données à caractère personnel.

Bénéficiaire : Toute personne qui reçoit une aide ou des avantages au titre d'un projet de l'OIM.

Besoin d'en connaître : Octroi ou refus au cas par cas, après mûre réflexion, de l'accès à des catégories de données à caractère personnel.

Biométrie : Etude des caractéristiques biologiques des personnes selon des méthodes quantitatives. Les identifiants biométriques sont des éléments d'encodage des caractéristiques physiques qui permettent de distinguer une personne d'une autre (par exemple, empreintes digitales, images de la rétine ou identification de la voix). Certains gouvernements établissent des passeports, visas et permis de résidence contenant des identifiants biométriques afin de réduire les risques de falsification.

BlackBerry : Terminal de poche offrant des fonctions telles que la messagerie électronique en temps réel (« push e-mail »), la téléphonie mobile, la messagerie textuelle, la télécopie par Internet, la navigation sur le Web et d'autres services d'information sans fil.

Bureau extérieur de l'OIM : Bureau de l'OIM situé dans une zone d'intervention.

Cellule familiale : Droit de toute famille de vivre réunie et, en tant que cellule sociale de base, d'être respectée, protégée, aidée et soutenue. Ce droit n'est pas limité aux personnes qui vivent dans le pays dont elles sont ressortissantes, et il est protégé par le droit international.

Clause contractuelle : Clause spéciale d'un contrat écrit destinée à lever toute ambiguïté.

Conflit armé : « Cas de guerre déclarée ou tout autre conflit armé surgissant entre deux ou plusieurs [Etats], même si l'état de guerre n'est pas reconnu par l'[un d'eux] » (art. 2, Conventions de Genève I-IV, 1949). « Un conflit armé existe chaque fois qu'il y a un recours à la force armée entre Etats, ou un conflit armé prolongé entre les autorités gouvernementales et des groupes armés organisés ou entre de tels groupes au sein d'un

Etat » (Le Procureur c/ Dusko Tadic, affaire n° IT-94-1-AR72, Chambre d'appel du Tribunal pénal international pour l'ex-Yougoslavie).

Connaissances : Capacité de comprendre et de saisir pleinement la ou les finalités déterminées pour lesquelles des données à caractère personnel sont recueillies et traitées.

Consentement : Décision libre, volontaire et éclairée donnée explicitement ou implicitement pour une finalité déterminée.

Contrat de transfert écrit : Accord juridiquement contraignant qui énonce les conditions dans lesquelles les données à caractère personnel sont transférées aux tiers.

Correspondant pour la protection des données : Tout membre du personnel de l'OIM nommé par des représentants régionaux de l'OIM pour faire fonction d'interlocuteur ou de personne de référence en ce qui concerne la protection des données, qui est chargé de surveiller les pratiques de protection des données suivies dans la région à laquelle il est affecté.

Cryptage : Progiciel garantissant le transfert électronique sécurisé de données à caractère personnel confidentielles. Le texte est converti en un code incompréhensible qui ne peut être décodé qu'au moyen d'une clé qui protège le format original du texte.

Cryptage partiel : Cryptage d'espaces d'un nombre limité de zones mémoire électroniques, telles que les dossiers, les fichiers et les applications de bases de données contenant des données à caractère personnel.

Demandeur d'asile : Personne sollicitant son admission dans un pays autre que le sien pour échapper à des persécutions ou à des atteintes graves, et qui attend à cet effet une décision d'octroi du statut de réfugié en application des instruments nationaux et internationaux pertinents. En cas de décision de rejet, le demandeur débouté doit quitter le territoire de l'Etat considéré. Il est susceptible de faire l'objet d'une mesure d'expulsion au même titre que tout étranger en situation irrégulière ou illégale, à moins qu'une autorisation de séjour lui soit accordée pour des raisons humanitaires ou sur un autre fondement.

Détention : Restriction, par les autorités d'un pays, de la liberté de mouvement d'une personne, habituellement par une mesure d'internement forcé.

Diligence raisonnable : Précautions prises par un responsable du traitement des données au moment du transfert des données à des tiers, pour défendre les droits et intérêts des personnes concernées.

Division ITC : Division Technologie de l'information et communications au Siège de l'OIM

Donateur : Toute personne ou entité, souvent un Etat, qui contribue au financement d'un projet de l'OIM.

Données à caractère non personnel : Toute information qui ne se rapporte pas à une personne concernée identifiée ou identifiable.

Données à caractère personnel : Toute information qui pourrait permettre d'identifier des personnes concernées ou de leur porter préjudice ; toute information se rapportant à une

personne concernée identifiée ou identifiable, consignée dans un dossier électronique ou papier.

Données anonymes : Données dont tous les éléments identifiables à caractère personnel ont été éliminés des ensembles de données de façon qu'il soit impossible, selon toute probabilité raisonnable, d'identifier la personne concernée ou d'en retrouver la trace.

Données globales : Informations, généralement des statistiques récapitulatives, qui peuvent être recueillies à partir de données à caractère personnel mais qui sont regroupées de manière à empêcher l'identification de cas individuels.

Dossier électronique : Tout système électronique d'archivage de données qui contient des données à caractère personnel.

Dossier papier : Tout document imprimé ou écrit qui contient des données à caractère personnel.

Droits de l'homme : Libertés et avantages basés sur la dignité de la personne dont, selon des valeurs contemporaines reconnues, tous les êtres humains devraient pouvoir se prévaloir « de droit » dans la société où ils vivent. Ces droits sont énoncés dans la Charte internationale des droits de l'homme, qui comprend la Déclaration universelle des droits de l'homme (1948), le Pacte international relatif aux droits économiques, sociaux et culturels et le Pacte international relatif aux droits civils et politiques (1966). Ils ont été développés à partir de ces textes fondamentaux dans d'autres traités (p. ex., la Convention sur la protection de tous les travailleurs migrants et des membres de leur famille, 1990).

Enfant : Tout être humain âgé de moins de 18 ans, sauf si la majorité est atteinte plus tôt en vertu de la législation qui lui est applicable (Convention des Nations Unies relative aux droits de l'enfant, 1989, art. 1).

Enfants séparés de leur famille : Enfants qui sont séparés de leurs deux parents ou de la personne qui était précédemment chargée, selon la loi ou la coutume, de subvenir à leurs besoins, mais pas nécessairement d'autres proches. Il peut donc s'agir aussi d'enfants accompagnés par d'autres membres de leur famille. Selon la *Déclaration de bonne pratique* de 2004, du Programme en faveur des enfants séparés en Europe (PESE), ce terme désigne les enfants de moins de 18 ans qui se trouvent hors de leur pays d'origine et qui sont séparés de leurs deux parents ou de la personne qui était précédemment chargée, selon la loi ou la coutume, de subvenir à leurs besoins. Le PESE utilise le mot « séparé » plutôt que « non accompagné » parce que, si certains enfants semblent être « accompagnés » lorsqu'ils arrivent en Europe, les adultes qui les accompagnent ne sont pas forcément capables ou en mesure d'assumer la responsabilité de leur prise en charge.

Entourage : Personnes entretenant des relations étroites avec la personne concernée et agissant au mieux de ses intérêts.

EUROPOL : Agence de renseignement criminel de l'Union européenne, qui appuie la coopération transfrontalière entre les services répressifs nationaux des Etats membres de l'UE.

Evaluation du rapport risques/avantages : Evaluation des risques et des avantages liés au traitement des données.

Fournisseur de services : Toute entité qui fournit des prestations en vue de contribuer à la réalisation de la finalité déterminée pour laquelle les données à caractère personnel sont recueillies et traitées.

Groupe de population cible : Groupe particulier de personnes qui sont les bénéficiaires visés d'un projet de l'OIM.

Groupe vulnérable : Groupe social ou secteur de la société plus exposé que d'autres, sur le territoire d'un pays donné, au risque de discrimination, d'actes de violence, de catastrophes naturelles ou environnementales ou de difficultés économiques ; tout groupe social ou secteur de la société (femmes, enfants, personnes âgées ou présentant un handicap, peuples autochtones ou migrants) exposé à des risques accrus en cas de conflit ou de crise.

HCR : Haut-Commissariat des Nations Unies pour les réfugiés

Informaticien : Fonctionnaire chargé de la technologie de l'information et des communications au sens des politiques relatives aux technologies de l'information de l'OIM.

Ingénierie sociale : Pratiques trompeuses mises en œuvre pour amener des personnes par la ruse à révéler des données à caractère personnel ou des codes d'accès.

Instruments internationaux : Conventions, déclarations et autres règles et principes juridiques internationaux et régionaux qui protègent les libertés et les intérêts individuels.

Intérêt général : Bien commun, santé ou bien-être de la société dans son ensemble ou de populations spécifiques.

INTERPOL : Organisation internationale de police criminelle

LEG : Bureau des affaires juridiques au Siège de l'OIM

Législation nationale : Droit interne d'un Etat

Mémorandum d'accord : Accord à l'amiable juridiquement contraignant, conclu entre l'OIM et un tiers.

Ménage dirigé par une femme : Ménage dirigé par une veuve ou une femme divorcée.

Ménage dirigé par un enfant : Ménage dans lequel un enfant tient le rôle d'un adulte et a acquis le statut de chef de ménage.

Migration : Déplacement d'une personne ou d'un groupe de personnes d'un pays à un autre, ou d'une région à une autre à l'intérieur d'un même pays. La notion de migration englobe tous les types de mouvements de population, quelles que soient leur cause, leur composition, leur durée, incluant ainsi les réfugiés, les personnes déplacées, les migrants économiques et les personnes se déplaçant pour d'autres motifs, y compris le regroupement familial.

MiMOSA (Application relative aux systèmes opérationnels et de gestion des migrants) : logiciel utilisé par certains bureaux de l'OIM pour stocker des données sur les migrants, suivre et gérer des activités opérationnelles, établir des rapports statistiques et améliorer l'aide aux migrants.

Mineur/enfant non accompagné : Personne n'ayant pas atteint l'âge de la majorité se trouvant dans un pays autre que celui dont elle possède la nationalité et sans être accompagnée d'un parent, d'un tuteur ou de tout autre adulte qui, en vertu de la loi ou de la coutume, est responsable d'elle. Les mineurs non accompagnés présentent des difficultés particulières aux autorités frontalières car la détention et les autres mesures appliquées aux étrangers majeurs dépourvus de documents peuvent être inadaptées aux enfants.

Obsolescence : Pour le matériel ou le logiciel de systèmes informatiques ou leurs composants, fait de ne plus bénéficier du soutien technique du fabricant.

OIM : Organisation internationale pour les migrations

Organisme d'audit : Organisme indépendant et impartial qui n'intervient pas dans la collecte et la protection des données mais qui vérifie systématiquement le respect des principes de protection des données, enquête sur toute violation, et évalue le respect et la mise en œuvre des principes de l'OIM.

Partenaire de l'OIM : Toute partie prenante ayant conclu un accord de coopération et de coordination avec l'OIM, y compris les gouvernements, les organismes des Nations Unies, les organisations internationales, les organisations non gouvernementales, les instituts de recherche, les entreprises et les sociétés privées.

Partenaire d'exécution : Entité qui œuvre aux côtés de l'OIM à la réalisation d'une activité de projet de l'OIM.

Pays d'accueil/pays hôte : Pays de destination ou pays tiers. Dans le cas d'un retour ou d'un rapatriement, il peut également s'agir du pays d'origine.

Pays d'opération : Pays dans lequel le projet de l'OIM est mis en œuvre.

Personne concernée : Bénéficiaire de l'OIM pouvant être identifié directement ou indirectement en fonction d'un ou plusieurs éléments précis, à savoir, entre autres : un nom, un numéro d'identification, une situation matérielle ou des caractéristiques physiques, mentales, culturelles, économiques ou sociales.

Personnel de l'OIM : Toute personne employée à titre temporaire ou permanent par l'OIM, y compris les interprètes officiels et officieux, les commis à la saisie des données, les stagiaires, les chercheurs, les conseillers désignés et les médecins.

Personnes déplacées à l'intérieur de leur propre pays : Personnes ou groupes de personnes qui ont été forcés ou contraints à fuir ou à quitter leur foyer ou leur lieu de résidence habituelle, notamment en raison d'un conflit armé, de situations de violence généralisée, de violations des droits de l'homme ou de catastrophes naturelles ou provoquées par l'homme ou pour en éviter les effets, et qui n'ont pas franchi les frontières internationalement reconnues d'un Etat *(par. 2 des Principes directeurs relatifs au déplacement de personnes à l'intérieur de leur propre pays, document ONU*

E/CN.4/1998/53/Add.2).

Population touchée par un conflit : Groupe de personnes touchées par un conflit armé.

Prise en considération des sexospécificités : Reconnaissance des différences et des inégalités et, parallèlement, défense des intérêts, besoins et priorités des hommes et des femmes, comme des filles et des garçons.

Proches : Personnes appartenant au même arbre généalogique que la personne concernée et qui lui sont apparentées par la naissance, le mariage ou l'adoption, ou qui partagent ses croyances culturelles ou convictions religieuses.

Protection des données : Application systématique d'un ensemble de mesures de protection institutionnelles, techniques et physiques qui protègent le droit au respect de la vie privée en ce qui concerne la collecte, le stockage, l'utilisation et la divulgation de données à caractère personnel.

Rapatriement : Droit personnel d'un réfugié, d'un prisonnier de guerre ou d'un détenu civil de retourner dans son pays de nationalité selon des conditions précises énoncées dans divers instruments internationaux (*Conventions de Genève de 1949 et Protocoles de 1977, Règlement concernant les lois et coutumes de la guerre sur terre, annexé à la quatrième Convention de La Haye de 1907*, des instruments relatifs aux droits de l'homme, et le droit international coutumier).

Réfugié : Personne qui, « craignant avec raison d'être persécutée du fait de sa race, de sa religion, de sa nationalité, de son appartenance à un certain groupe social ou de ses opinions politiques, se trouve hors du pays dont elle a la nationalité et qui ne peut ou, du fait de cette crainte, ne veut se réclamer de la protection de ce pays » (Convention relative au statut des réfugiés, 1951, art. 1er a, § 2, modifiée par le Protocole de 1967).

Regroupement familial : Processus par lequel des membres d'une même famille séparés par la migration volontaire ou forcée se regroupent dans un pays autre que leur pays d'origine.

Réinstallation : Transfert et intégration de personnes (réfugiés, personnes déplacées à l'intérieur de leur propre pays, etc.) dans une autre région géographique et un autre environnement, habituellement dans un pays tiers. S'agissant des réfugiés, ce terme s'entend du transfert du pays où ils ont cherché refuge vers un autre Etat qui a accepté de les accueillir. Les réfugiés obtiennent généralement l'asile ou une autre forme de droit de résidence de longue durée et, très souvent, ont la possibilité d'obtenir la naturalisation.

Responsable du traitement des données : Membre du personnel de l'OIM ou personne représentant un tiers qui est habilité à décider du contenu et de l'utilisation des données à caractère personnel.

Sécurité des données : Ensemble de mesures physiques et technologiques qui préservent la confidentialité et l'intégrité des données à caractère personnel et empêchent toute modification non autorisée, falsification, destruction illégale, perte accidentelle, divulgation abusive ou transfert indu.

Services répressifs : Autorité nationale ou internationale investie du pouvoir d'assurer ou de faciliter l'application de la loi, y compris la police, la police des frontières, la police de

l'immigration, les douanes, ou tout fonctionnaire chargé d'appliquer la loi.

Siège de l'OIM : Locaux de l'OIM à Genève (Suisse)

Tiers : Personne physique ou morale, gouvernement ou autre entité sans rapport avec la ou les finalités initiales déterminées pour lesquelles les données à caractère personnel sont recueillies et traitées. Le tiers qui souscrit par écrit aux conditions de transfert énoncées au Principe 5 sera autorisé à accéder aux données à caractère personnel et à les traiter.

Traitement des données : Techniques et méthodes utilisées pour recueillir, enregistrer, stocker, archiver, récupérer, utiliser, diffuser, communiquer, transférer et détruire des données à caractère personnel.

Travaux de recherche d'intérêt général : Tous travaux de recherche servant l'intérêt général, nécessaires pour le bien commun, la santé ou le bien-être de la société dans son ensemble ou de populations spécifiques.

UE : Union européenne

UNICEF : Fonds des Nations Unies pour l'enfance

Unité ou département de l'OIM : Au Siège de l'OIM, structure responsable de domaines d'activité de l'OIM

Victime de la traite d'êtres humains : Personne physique soumise à la traite des personnes au sens de l'article 3 a) du Protocole additionnel à la Convention des Nations Unies contre la criminalité transnationale organisée visant à prévenir, réprimer et punir la traite des personnes, en particulier des femmes et des enfants, 2000.

BIBLIOGRAPHIE

Publications

Anderson, H.
2006 The privacy gambit: Toward a game theoretic approach to international data protection, *Vanderbilt Journal of Entertainment and Technology Law*, vol. 9, p. 1. Voir : http://law.bepress.com/expresso/eps/1056

Association de coopération économique Asie-Pacifique (APEC)
2005 *APEC Privacy Framework*. Secrétariat de l'APEC, Singapour. Voir : http://publications.apec.org/publication-detail.php?pub_id=390

Baker, R.
2005 Offshore IT outsourcing and the 8th data protection principle – legal and regulatory requirements – with reference to financial services, *International Journal of Law and Information Technology*, vol. 14, nº 1, pp. 1-27.

Bargiotas, T. et E. Maganaris
2006 Privacy under attack? The surveillance phenomenon in Europe, the implementation of the respective European Directives in Greece and the legitimacy of workplace monitoring, *Revue européenne de droit public*. Esperia Publications, Londres, vol. 18, nº 3, pp. 1037-1082.

Barquin, R. et C. Northouse
2003 *Data Collection and Analysis: Balancing Individual Rights and Societal Benefits*, Computer Ethics Institute, Washington, D.C. Voir : http://www7.nationalacademies.org/cnstat/Barquin_Paper.pdf

Bergkamp et al.
2002 EU data protection policy: The privacy fallacy: Adverse effects of Europe's data protection policy in an information-driven economy, *Computer Law and Security Report*, vol. 18, nº 1.

Bianchini, G. et al.
2005 *Tomorrow is the tomorrow we should have worried about yesterday: a proposal for an Italian law, regulation usage, retention and deletion of geo-referenced and chrono-reference, automatically collected data containing unique user identifiers*, 20e conférence BILETA : Over-commoditized; Over-observed: The New Digital Legal World?

Booth, S. et al.
2004 *What are 'Personal Data'? A study conducted for the UK Information Commissioner*, Université de Sheffield, Royaume-Uni

Bygrame, L.
1998 Data protection pursuant to the right to privacy in human rights treaties, *International Journal of Law and Information Technology*, vol. 6, pp. 247-284.

2001 The place of privacy in data protection law, *University of New South Wales Law Journal*.

2002a *Data Protection Law: Approaching its Rationale, Logic and Limits*, Kluwer Law International, La Haye, Londres, New York.

2002b The 1995 EC Directive on data protection under official review - feedback so far, *Privacy Law & Policy Reporter*.

2004 Privacy protection in a global context – a comparative overview, *Scandinavian Studies in Law*, vol. 47, pp. 319-348.

Campbell, D. et C. Bàn
2005 *Legal Issues in the Global Information Society*, Ocean Publications, New York.

Cavoukian, A.
2005 The new breed of practical privacy: An evolution, *Jusletter 3*, octobre 2005.

Chambre de commerce internationale
2003 *Privacy Toolkit: An international business guide for policy makers*, Chambre de commerce internationale, France. Voir : http://www.iccwbo.org/advocacy-codes-and-rules/basis/igf/

Clarke, R.
2000 *Beyond the OECD Guidelines: Privacy Protection for the 21st Century*. Voir : http://www.anu.edu.au/people/Roger.Clarke/DV/PP21C.html

Cogan, J. K.
2007 Cooperation with international tribunals — binding orders directed at States and International Organizations, *American Journal of International Law*, vol. 101, p. 163.

Comité international de la Croix-Rouge (CICR)
2002 *Personnes portées disparues : La protection juridique des données personnelles et des dépouilles mortelles*, CICR, Genève.
Voir : http://www.icrc.org/fre/resources/documents/misc/5gyfh7.htm

Comité permanent interorganisations (IASC)
2006 *Femmes, filles, garçons et hommes : des besoins différents, des chances égales, Guide pour l'intégration de l'égalité des sexes dans l'action humanitaire*. Voir : https://ochanet.unocha.org/p/Documents/IASC%20Gender%20Handbook%20(French).pdf

Commissariat à l'information de l'Australie
2006 *Privacy Impact Assessment Guide*, Gouvernement de l'Australie, Commissariat à l'information, révisé en mai 2010. Voir : www.privacy.gov.au

Conseil de l'Europe

2002 *Guide relatif à l'élaboration de clauses contractuelles régissant la protection des données lors de communications de données à caractère personnel à des tiers non soumis à un niveau de protection des données adéquat*. Conseil de l'Europe, Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel.

2010 *La protection des données : Recueil des textes du Conseil de l'Europe*. Direction générale des droits de l'homme et des affaires juridiques, Conseil de l'Europe, Strasbourg.

Cope, H. et al.

2002 The right to privacy in personal data: The EU prods the US and the controversy continues, *Tulsa Journal of Comparative and International Law*, vol. 9, p. 391.

Correa, C.

2002 Public health and international law: Unfair competition under the TRIPS Agreement: Protection of Data submitted for the Registration of Pharmaceuticals, *Chicago Journal of International Law*, vol. 3, p. 69.

Danna, A. et O.H. Gandy

2002 *All that glitters is not gold: Digging beneath the surface of data mining, Journal of Business Ethics*, vol. 40, pp. 373-386.

De Borchgrave, A.

2001 *Cyber Threats and Information Security: Meeting the 21st Century Challenge*, CSIS Press, Washington, D.C.

Del Villar, R.

2001 *Regulation of Personal Data Protection and of Reporting Agencies: A Comparison of Selected Countries of Latin America, the United States and European Union Countries*.

Dmytrenko, O. et A. Nardali

2005 .NET Passport under the scrutiny of US and EU privacy law: Implications for the future of online authentication, *Journal of Law and Policy for the Information Society*, vol. 1, p. 619.

Eisenhauer, M. et J. Jordan

2005 *Internal Privacy Governance Frameworks*, 2nd Technical Assistance Seminar on Implementation of APEC Privacy Framework: International Implementation Issues, 2005/SOM3/ECSG/SEM/010, point VI de l'ordre du jour.

Fonds des Nations Unies pour l'enfance (UNICEF)

2006a *UNICEF Guidelines on the Protection of Child Victims of Trafficking*, UNICEF, New York.
Voir : http://www.unicef.org/ceecis/0610-Unicef_Victims_Guidelines_en.pdf

2006b *Reference Guide on Protecting the Rights of Child Victims of Trafficking in Europe*, UNICEF, Genève.
Voir : http://www.unicef.org/ceecis/UNICEF_Child_Trafficking_low.pdf

Gandy, O.H.
2003 *Public Opinion Surveys and the Formation of Privacy Policy*, The Society for the Psychological Study of Social Issues.

Garcia, F.
2005 Bodil Lindqvist: A Swedish churchgoer's violation of the European Union's data protection directive should be a warning to US legislators, *Fordham Intellectual Property Media and Entertainment Law Journal*, vol. 15, p. 1205.

Gromovs, J.
2008 *A compendium of legal instruments of the European Union and the Council of Europe concerning the use of security features and biometric identifiers in passport and travel documents, residence permits and short-term visas.* Commission européenne/Organisation internationale pour les migrations, Minsk.

Guadamuz, A.
2000 Habeas data: The Latin-American response to data protection, *Journal of Information, Law and Technology*, vol. 2.

Gutwirth, G. et al.
2009 *Reinventing Data Protection?* Springer, Science and Business Media B.V., Pays-Bas.

Harper, J. et A. Spies
2006 *A Reasonable Expectation of Privacy? Data Protection in the United States and Germany*, American Institute for Contemporary German Studies – Université Johns-Hopkins, Policy Report nº 22.

Haut-Commissaire des Nations Unies pour les réfugiés (HCR)
1994 *Refugee Children: Guidelines on Protection and Care*, HCR, Genève.
Voir : http://www.unhcr.org/refworld/docid/3ae6b3470.html

2001 *Guidelines on the Sharing of Information on Individual Cases: "Confidentiality Guidelines"*, Département de la protection internationale, HCR, Genève. Voir : http://www.humanitarianreform.org/humanitarianreform/Portals/1/cluster%20approach%20page/clusters%20pages/CCm/IDP%20Key%20Resources/UNHCR%20Confidentiality%20Guidelines.pdf

2005 *Advisory Opinion on the Rules of Confidentiality Regarding Asylum Information*, HCR, Genève. Voir : http://www.unhcr.org/refworld/docid/42b9190e4.html

2008a *Principes directeurs du HCR relatifs à la détermination de l'intérêt supérieur de l'enfant*, HCR, Genève.
Voir : http://www.unhcr.fr/mwg-internal/de5fs23hu73ds/progress?id=sHJJ1+Cboz

2008b *Access Policy, Archives UNHCR*, http://www.unhcr.org/3b03896a4.html

2008c Model agreement on the sharing of personal data with governments in the context of hand-over of the refugee status determination process, http://www.unhcr.org/refworld/pdfid/4a54bbf9d.pdf

Holvast, J. et al.
1999 *The Global Encyclopaedia of Data Protection Regulation*, Kluwer, La Haye.

Hondius, F.
1983 A decade of international data protection, *Netherlands International Law Review*, vol. 30, nº 2, pp. 103-128.

InterAction Protection Working Group
2004 Data Collection in Humanitarian Response: A guide for incorporating protection, Interaction Protection Working Group, Washington, D.C. Voir : http://www.globalprotectioncluster.org/_assets/files/tools_and_guidance/InterAction_Guide_Incorporating_Protection_2003_EN.pdf

James, M.
1994 *Privacy and Human Rights: An International and Comparative Study, with special reference to developments in information technology*, Organisation des Nations Unies pour l'éducation, la science et la culture, Dartmouth Publishing Company Limited, Angleterre.

Korff, D.
2002 *EC Study on Implementation of the Data Protection Directive: Comparative Summary of National Laws*, Human Rights Centre, Université de l'Essex, Royaume-Uni.

Kranenborg, H.
2008 Access to documents and data protection in the European Union: on the public nature of personal data, *Common Market Law Review*, vol. 45, nº 4, pp. 1079-1114.

McCullagh, K.
2007 Data sensitivity: Proposals for resolving the conundrum, *Journal of International Commercial Law and Technology*, vol. 2, nº 4.

Michael, J.
1994 *Privacy and Human Rights: An International and Comparative Study, with special reference to developments in information technology*, Organisation des Nations Unies pour l'éducation, la science et la culture (UNESCO), Dartmouth Publishing Company Ltd., France et Angleterre.

Moshell, R.
2005 And then there was one: the outlook for a self-regulatory United States amidst a global trend toward comprehensive data protection, *Texas Tech Law Review*, vol. 37, p. 357.

Organisation de coopération et de développement économiques (OCDE)
1996 *Lignes directrices de l'OCDE régissant la sécurité des systèmes d'information,* OCDE, Paris.

2002 *Lignes directrices de l'OCDE régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel, contenant la Déclaration sur les flux transfrontières de données et la Déclaration relative à la protection de la vie privée sur les réseaux*, OCDE, Paris.

2003 *Protection de la vie privée en ligne : orientations politiques et pratiques de l'OCDE*, OCDE, Paris.

Organisation des Nations Unies pour l'éducation, la science et la culture (UNESCO)

2005 *The United Nations and Personal Data Protection*, Jusletter 3. Voir : http://jusletter.weblaw.ch/login.php?ref_url_succ=http%3A%2F%2Fjusletter.weblaw.ch%3A80%2Farticle%2Fde%2F_4236&ref_url_fail=http://jusletter.weblaw.ch/fail.php#

Organisation internationale de police criminelle (Interpol)

2004 *Règlement sur le traitement d'informations pour la coopération policière internationale*, amendé par la résolution AG-2005-RES-15 du 1er janvier 2006. Voir : https://secure.interpol.int/Public/ICPO/LegalMaterials/constitution/info/defaultFr.asp

2010 *Règlement relatif au contrôle des informations et à l'accès aux fichiers d'Interpol.* Voir : http://www.interpol.int/fr/contentinterpol/search?SearchText=R%C3%A8glement+relatif+au+contr%C3%B4le+des+informations+et+%C3%A0+l%E2%80%99acc%C3%A8s+aux+fichiers+d%E2%80%99INTERPOL

Organisation internationale du Travail (OIT)

1996 Le recueil de directives pratiques du BIT sur la protection des données personnelles du travailleur, *Revue internationale du Travail*, vol. 135, nº 5.

1997 *Protection des données personnelles des travailleurs*, OIT, Genève. Voir : http://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---safework/documents/normativeinstrument/wcms_112624.pdf

Organisation internationale pour les migrations (OIM)

2002 *Emergency Operations Manual*, OIM, Genève.

2004 *Research Manual*, OIM, Genève.

2005a *Biometrics and International Migration Law*, série Droit international de la migration n° 5, OIM, Genève.

2005b *Guide to Selected EU Legal and Policy Instruments on Migration*, OIM, Vienne.

2006 *Guide on Gender Indicators for Project Development*, OIM, Genève.

2007a *The IOM Handbook on Direct Assistance for victims of Trafficking*, OIM, Genève.

2007b *Registration Survey Analysis*, Technology Application in Migration Management, Working Group Presentation, OIM, Genève.

2009 *Principes relatifs à la protection des données de l'OIM,* Instruction IN/138, OIM, Genève.

2010a *Migration Initiatives*, OIM, Genève.

2010b *Assisted Voluntary Return and Reintegration Handbook*, OIM, Genève.

2011 *Glossary on Migration, 2nd Edition*, série Droit international de la migration nº 25, OIM, Genève.

Organisation pour la sécurité et la coopération en Europe (OSCE)
2004 *Les mécanismes nationaux d'orientation : Renforcer la coopération pour protéger les droits des victimes de la traite, un manuel pratique,* Bureau des institutions démocratiques et des droits de l'homme, Pologne.
Voir : http://www.osce.org/fr/odihr/13972

Papakonstantinou, V.
2001 A Data Protection Approach to Data Matching Operations Among Public Bodies, *International Journal of Law and Information Technology*, vol. 9, nº 1, p. 39.

Perruchoud, R. et K. Tömölovà
2007 *Droit international de la migration, recueil d'instruments*, OIM, Genève.

Programme commun des Nations Unies sur le VIH/sida (ONUSIDA)
2007 *Interim Guidelines on Protecting the Confidentiality and Security of HIV Information*, ONUSIDA, Genève.
https://www.unaids.org/en/media/unaids/contentassets/dataimport/pub/manual/2007/confidentiality_security_interim_guidelines_15may2007_en.pdf

Rempell, S.
2006 Personal data and subject access rights in the European data directive and implementing UK statute: Durant V. Financial Services Authority as a paradigm of data protection nuances and emerging dilemmas, *Florida Journal of International Law*, vol. 18, p. 807.

Shaffer, G.
2000 Globalization and social protection: The impact of EU and international rules in the ratcheting up of U.S. privacy standards, Yale Journal of International Law, vol. 25, nº 1, pp. 1-88.

Simitis, S.
1998 From the general rules on data protection to a specific regulation of the use of employee data: Policies and constraints of the European Union, *Comparative Labor Law and Policy Journal*, vol. 19, p. 351.

Stanley, P.
2008 *The Law of Confidentiality: A Restatement*, Hart Publishing, Oxford, Angleterre.

Swire, P. et R. Litan
1998 *None of Your Business: World Data Flows, Electronic Commerce and the European Privacy Directive*, The Brookings Institute, Washington D.C..

Tan, D.R.
1999 Personal Privacy in the Information Age: Comparison of Internet Data Protection Regulations in the United States and European Union, *Loyola of Angeles International and Comparative Law Journal*, vol. 21, nº 4, pp. 661-684.

Van Wasshnova, M.
2008 Data protection conflicts between the United States and the European Union in the war on terror: lessons learned from the existing system of financial information exchange, *Case Western Reserve Journal of International Law*, vol. 39, nº 3, pp. 827-886.

Wakan, J.
2003 The Future of Online Privacy: a Proposal for International Legislation, *Loyola of Los Angeles International and Comparative Law Series*, vol. 26, nº 1, p. 151-179.

Walden, I.
2002 Anonymising personal data, *International Journal of Law and Information Technology*, été 2002, vol. 10, nº 2, p. 224.

Walden, I et R. Savage
1988 Data protection and privacy laws: should organizations be protected? *International and Comparative Law Quarterly*, vol. 37, nº 2, p. 337-347.

Warren, A. et al.
2001 Sources of literature on data protection and human rights, *Journal of Information, Law and Technology*, vol. 2.

Webb, P.
2003 A comparative analysis of data protection laws in Australia and Germany, *Journal of Information, Law and Technology*, vol. 2.

Sources documentaires

Charte des droits fondamentaux de l'Union européenne, 2000 [Journal officiel C 364, 18/12/2000, pp. 0001 – 0022]. Voir : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000X1218(01):FR:HTML

Comité des droits de l'enfant, Observation générale nº 6 (2005) : Traitement des enfants non accompagnés et des enfants séparés en dehors de leur pays d'origine, 1er septembre 2005 [CRC/GC/2005/6].
Voir : http://www.unhchr.ch/tbs/doc.nsf/(symbol)/CRC.GC.2005.6.Fr?OpenDocument

Comité des droits de l'homme, Observation générale n° 16 : Le droit au respect de la vie privée, de la famille, du domicile et de la correspondance, et le droit d'être protégé contre les atteintes à l'honneur et à la réputation (art. 17), 8 avril 1988.
Voir : http://www.unhchr.ch/tbs/doc.nsf/0/7dc7e7821c5da97680256523004a423d?Opendocument

Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions : Une approche globale de la protection des données à caractère personnel dans l'Union européenne COM(2010) 609 final.
Voir : http://register.consilium.europa.eu/pdf/fr/10/st15/st15949.fr10.pdf

Conférence internationale des commissaires à la protection des données et à la vie privée

2005a Dans un monde globalisé, un droit universel à la protection des données personnelles et à la vie privée dans le respect des diversités (Déclaration de Montreux), 16 septembre 2005. Voir : http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Cooperation/Conference_int/05-09-16_Montreux_declaration_FR.pdf

2005b Résolution sur l'utilisation de la biométrie dans les passeports, cartes d'identité et documents de voyage, 27e Conférence internationale des commissaires à la protection des données et à la vie privée, Montreux, 2005. Voir : http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Cooperation/Conference_int/05-09-16_resolution_biometrics_FR.pdf

2005c Résolution sur l'utilisation de données personnelles pour la communication politique, Montreux, 2005. Voir : http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Cooperation/Conference_int/05-09-16_resolution_political_communication_FR.pdf

2009 Résolution de Madrid sur des normes internationales sur la vie privée et la protection des données personnelles, Conférence internationale des commissaires à la protection des données et à la vie privée, 5 novembre 2009. Voir : http://www.privacyconference2009.org/media/Publicaciones/common/estandares_resolucion_madrid_en.pdf

Convention américaine relative aux droits de l'homme, 1969 (entrée en vigueur le 18 juillet 1978) [1114 U.N.T.S.123]. Voir : http://www.cidh.oas.org/Basicos/French/c.convention.htm

Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales, 1950 (entrée en vigueur le 3 septembre 1953) [78 U.N.T.S. 222].
Voir : http://conventions.coe.int/treaty/fr/treaties/html/005.htm

Convention internationale sur la protection des droits de tous les travailleurs migrants et des membres de leur famille, 1990 (entrée en vigueur le 1er juillet 2003) [A/RES/45/158].
Voir : http://www2.ohchr.org/french/law/cmw.htm

Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, 1981, Conseil de l'Europe (adoptée le 28 janvier 1981) [STE nº 108, Strasbourg, 28.1.1981]. Voir : http://conventions.coe.int/Treaty/fr/Treaties/Html/108.htm

Amendements à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE nº 108) permettant l'adhésion des Communautés européennes, 1999, Conseil de l'Europe (adoptés le 15 juin 1999). Voir : http://conventions.coe.int/Treaty/fr/Treaties/Html/108-1.htm

Protocole additionnel à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, concernant les autorités de contrôle et les flux transfrontières de données [STE nº 108, Strasbourg, 08.11.01].
Voir : http://conventions.coe.int/Treaty/FR/treaties/html/181.htm

Convention relative aux droits de l'enfant, 1989 (entrée en vigueur le 2 septembre 1990) [A/RES/44/25]. Voir : http://www2.ohchr.org/french/law/crc.htm

Convention sur l'élimination de toutes les formes de discrimination à l'égard des femmes, 1979 (entrée en vigueur le 3 septembre 1981) [1249 U.N.T.S. 13].
Voir : http://www2.ohchr.org/french/law/cedaw.htm

Décision de la Commission relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers en vertu de la directive 95/46/CE du Parlement européen et du Conseil (2010/87/EU).
Voir : http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32010D0087:FR:HTML

Déclaration universelle des droits de l'homme, 1948 [G.A. res. 217A (III)].
Voir : http://www.un.org/fr/documents/udhr/

Directive 95/46/CE du Parlement européen et du Conseil relative à la protection des personnes physiques et à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (adoptée par le Parlement européent et le Conseil le 24 octobre 1995) [Journal officiel L 281, 23.11.1995, pp. 0031 – 0050]. Voir : http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_fr.pdf

Directive 2006/24/CE du Parlement européen et du Conseil sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE (adoptée par le Parlement européen et le Conseil le 15 mars 2006) [Journal officiel L 105, 13/04/2006, pp. 0054 – 0063].
Voir : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:FR:HTML

Fonds des Nations Unies pour l'enfance (UNICEF), Les principes de Paris : Principes directeurs relatifs aux enfants associés aux forces armées ou aux groupes armés, février 2007. Voir : http://www.unicef.org/french/protection/files/ParisPrincipesFrench310107.pdf

Lignes directrices de l'OCDE régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel (adoptées le 23 septembre 1980). Voir : http://www.oecd.org/fr/internet/ieconomie/lignesdirectricesregissantlaprotectiondelaviepriveeetlesfluxtransfrontieresdedonneesdecaracterepersonnel.htm

Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information : vers une culture de la sécurité (adoptées le 25 juillet 2002).
Voir : http://www.oecd.org/dataoecd/16/22/15582260.pdf

Pacte international relatif aux droits civils et politiques, 1966 (entré en vigueur le 23 mars 1976) [99 U.N.T.S 171]. Voir : http://www2.ohchr.org/french/law/ccpr.htm

Principes directeurs pour la réglementation des fichiers personnels informatisés, adoptés le 14 décembre 1990 par l'Assemblée générale des Nations Unies, Nations Unies [A/RES/45/95]. Voir :
http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/45/95&referer=http://www.un.org/Depts/dhl/resguide/r45.htm&Lang=F

Protocole visant à prévenir, réprimer et punir la traite des personnes, en particulier des femmes et des enfants, additionnel à la Convention des Nations Unies contre la criminalité transnationale organisée, annexe II, 2000 [G.A. res. A/RES/55/25] (entré en vigueur le 25 décembre 2003). Voir : http://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-f.pdf

Règlement (CE) nº 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données, Parlement européen et Conseil [Journal Officiel L 008, 12/01/2001, pp. 0001-0022]. Voir : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:008:0001:0022:fr:PDF

Modèles et listes de vérification relatifs à la protection des données de l'OIM

Ces modèles et listes de vérification ont un caractère général. Ils ont pour but de garantir la mise en application des principes et lignes directrices de l'OIM en matière de protection des données. Tous les contrats écrits doivent être soumis au Bureau des affaires juridiques (LEG@iom.int) pour examen et approbation.

TABLE DES MATIERES

MODELE 1.1

1.1 Autorisation type concernant la collecte de données à caractère personnel auprès de bénéficiaires

FORMULAIRE DE CONSENTEMENT GENERAL

Je soussigné(e) *[Nom de la personne concernée]* autorise par la présente l'Organisation internationale pour les migrations (ci-après « l'OIM ») et toute autre personne ou entité habilitée agissant au nom de l'OIM à recueillir, utiliser, divulguer et détruire mes données à caractère personnel et, le cas échéant, celles des personnes à ma charge *[Noms du ou des enfants/des membres de la famille]* pour les finalités suivantes :

FINALITES Déterminées et définies avant la collecte de données	DESCRIPTION	CONSENTEMENT	
	A remplir par le responsable du traitement des données ou l'enquêteur	OUI	NON
a) Finalité déterminée initiale	…… ……		
b) Continuum de l'aide	…… ……		
c) Finalité de recherche additionnelle	…… ……		
d) Finalités additionnelles prévisibles	…… ……		

J'accepte que mes données à caractère personnel soient divulguées, pour la ou les finalités précitées, aux tiers suivants :

	NOM DU TIERS	CONSENTEMENT	
	A remplir par le responsable du traitement des données ou l'enquêteur	OUI	NON
e) Membres du personnel de l'OIM habilités	*indiquer le nom des membres du personnel habilités de différents projets de l'OIM ……si un flux interne au sein de l'OIM est prévu ……..*		
f) Tiers habilités	*……indiquer tous les tiers prévisibles ……..... ……par ex., donateur, partenaires de projet, etc……..*		

Déclaration de consentement éclairé de la personne concernée :

1. J'ai été informé(e) de la (des)finalité(s) déterminée(s) et additionnelle(s) pour lesquelles mes données à caractère personnel seront recueillies, utilisées et divulguées, comme indiqué plus haut.
2. J'ai bien compris que mes données à caractère personnel pourront être utilisées et divulguées pour des finalités secondaires, nécessaires pour atteindre la ou les finalités déterminées précitées.
3. J'ai bien compris que je peux accéder à mes données à caractère personnel et les rectifier sur demande en contactant l'OIM.
4. J'ai bien compris que le retrait de mon consentement peut mettre l'OIM dans l'incapacité de fournir un service en ma faveur.
5. Je déclare que les renseignements fournis sont, à ma connaissance, véridiques et exacts.

MODELE 1.1

6. Par la présente, je décharge et libère l'OIM, ses fonctionnaires, employés et agents de toute obligation et accepte de les mettre hors de cause en cas de dommages causés, directement ou indirectement, à moi-même, à ma famille ou à mes proches en raison de la présente autorisation, à la suite de l'utilisation ou de la divulgation de mes données à caractère personnel pour la ou les finalités déterminées, énoncées plus haut.

7. J'ai pris connaissance de la teneur du présent formulaire de consentement éclairé :

   a) Après lecture des dispositions précitées : OUI/NON
   b) Après qu'il m'a été donné lecture des dispositions précitées ou que celles-ci ont été traduites : OUI/NON

8. Je fais cette déclaration de mon plein gré et consens librement à ce que l'OIM recueille et traite mes données à caractère personnel.

Signature à (lieu) ……le (date)…….

…… Signature de l'interprète

……..... Signature ou marque de la personne concernée (ou d'un parent/tuteur/mandataire)

**** NOTE : Ce formulaire de consentement type est proposé à titre indicatif lorsque des données à caractère personnel sont recueillies auprès de personnes concernées. Il contient les éléments requis pour s'assurer que le consentement est obtenu pour la ou les finalités déterminées, les finalités prévisibles et la divulgation à des tiers. Il peut être adapté selon que de besoin pour atteindre les objectifs du projet. Si le formulaire de consentement est téléchargé sous forme électronique dans une base de données aux fins de stockage, l'encadré de consentement ci-après peut être utilisé pour consigner avec exactitude la forme du consentement obtenu.***

ENCADRE DE CONSENTEMENT			
Forme du consentement donné par la personne concernée :			
Exprès		Implicite	Procuration
écrit	*oral*		
Liste des catégories de finalités déterminées pour lesquelles le consentement a été donné :			
1. Finalité déterminée initiale : …… *2. Continuum de l'aide : ……* *3. Recherche additionnelle/autres finalités déterminées ……* *4. Divulgation au personnel de différents projets de l'OIM ……* *5. Transfert à des tiers prévisibles ……*			

MODELE 1.2

1.2 Autorisation type du bénéficiaire concernant sa participation à des projets de l'OIM

AUTORISATION DU BENEFICIAIRE

Je soussigné(e) _____ décide en toute connaissance de cause de coopérer avec l'Organisation internationale pour les migrations (ci-après « l'OIM ») et de participer au projet de l'OIM intitulé *[nom du projet]*, qui vise à *[préciser l'objectif du projet]*.

J'ai bien compris que mes données à caractère personnel et celles des personnes à ma charge *[Noms du ou des enfants/des membres de la famille]* sont nécessaires pour *[décrire l'aide fournie par l'OIM]*. J'ai été informé(e) de la ou des finalités déterminées et additionnelles, et autorise par la présente l'OIM et toute personne ou entité habilitée agissant au nom de l'OIM à recueillir, utiliser, divulguer et détruire les données à caractère personnel communiquées dans le présent formulaire. Je sais que, pour atteindre la ou les finalités déterminées, ces données à caractère personnel seront communiquées et traitées par *[nom du tiers, p. ex., donateurs, institutions/entités gouvernementales]*, et j'y consens.

Par la présente, je décharge et libère l'OIM de toute obligation et accepte de la mettre hors de cause en cas de dommages causés, directement ou indirectement, à moi-même, à l'un de mes enfants ou à ma famille en lien avec la présente autorisation. J'accepte qu'en cas de dommage corporel ou de décès pendant et/ou après ma participation au projet de l'OIM, ni l'OIM ni aucune autre organisation ou entité gouvernementale associée au projet ne puisse d'aucune façon être tenue pour responsable.

Je déclare que les renseignements communiqués sont, à ma connaissance, véridiques et exacts. Je suis conscient(e) du fait que, si je fais une fausse déclaration en signant le présent formulaire, l'OIM sera en droit de mettre fin à tout moment à l'assistance qu'elle m'apporte.

Signé le *[date]*, à *[lieu]* :

Signature du demandeur : _____

⁎ *NOTE : Cette autorisation type du bénéficiaire est un exemple de déclaration de consentement destinée à être utilisée dans le cadre de projets de l'OIM tels que les projets d'aide au retour volontaire et à la réintégration (AVRR). Elle pourra être adaptée pour être incluse dans les formulaires d'entretien, d'enregistrement et de demande. L'autorisation exigée de la part du bénéficiaire dépendra de la nature du projet et du type d'activité menée par l'OIM. Par exemple, des victimes, ou des victimes présumées, de la traite devront signer des modèles précis, tels que le formulaire d'entretien de sélection et le formulaire d'entretien en vue d'une assistance.*

MODELE 1.3

1.3 Autorisation type concernant la prise de photographies

FORMULAIRE DE CONSENTEMENT A LA PRISE DE PHOTOGRAPHIES

Je soussigné(e) *[nom de la personne ou du parent/tuteur]* [selon le cas] autorise par la présente *[nom du photographe]* à prendre, au nom de l'Organisation internationale pour les migrations (ci-après « l'OIM »), des photographies de mon enfant *[nom de l'enfant]*/de moi-même [selon le cas] (ci-après « les photographies ») :

1. Je consens [au nom de mon enfant et en mon nom propre] [selon le cas] à être photographié(e) par *[nom du photographe]*.

2. J'ai bien compris que les photographies sont prises dans le cadre du projet intitulé *[nom du projet]* (ci-après le « projet »), et y consens. Ce projet vise à *[préciser l'objectif du projet]*.

3. J'autorise l'OIM à utiliser et à reproduire les photographies hors du cadre du projet en vue d'une utilisation future dans ses activités, notamment dans le but de :

   - Améliorer la connaissance et la compréhension des questions de migration.
   - Mener des actions de sensibilisation dans le cadre de campagnes, d'activités promotionnelles, de stratégies de communication et de communications publiques.
   - Faire connaître et promouvoir l'action de l'OIM.
   - Informer les donateurs et les partenaires de l'OIM, les médias, le grand public et d'autres, des programmes et activités de l'OIM.

4. J'ai bien compris que l'utilisation future des photographies englobe, sans y être limitée, la reproduction dans des publications, des supports de sensibilisation, des brochures, des rapports, des articles, des exposés, des expositions futures, et l'affichage sur les sites Internet de l'OIM et d'autres médias électroniques de tiers, et j'y consens.

5. J'ai bien compris la nature de la séance photo et l'utilisation prévue des photographies, et j'autorise par la présente cette utilisation pour les finalités susmentionnées. Je sais en outre que les photographies peuvent être montrées dans un espace public.

6. Je suis conscient(e) que l'OIM n'est pas tenue d'utiliser les photographies.

7. Par la présente, je décharge et libère l'OIM, ses fonctionnaires, employés et agents de toute obligation et accepte de les mettre hors de cause en cas de dommages causés, directement ou indirectement, à moi-même ou à ma famille en raison de la présente autorisation, à la suite de l'utilisation de l'une quelconque des photographies pour la finalité du projet ou aux fins d'utilisation future par l'OIM.

8. J'ai bien compris que l'OIM détiendra les droits d'auteur et tous les autres droits de propriété intellectuelle relatifs aux photographies et qu'elle peut utiliser et publier celles-ci, et autorise des tiers à les utiliser et les publier sans mon accord, et j'y consens.

9. Je suis conscient(e) du fait que [ni mon enfant ni moi-même] ne serons rétribués pour la séance photo ou pour l'utilisation des photographies, qu'aucun paiement ne sera effectué et qu'aucune possibilité de rémunération ne sera envisagée.

10. J'ai bien compris la teneur du présent formulaire de consentement :

    a) Pour avoir lu les dispositions précitées : OUI/NON
    b) Après qu'il m'a été donné lecture des dispositions précitées : OUI/NON

11. Je fais cette déclaration de mon plein gré et consens librement à ce que mon enfant/moi-même soyons photographiés par le photographe pour le compte de l'OIM.

Signé le [date] à [lieu] :

Signé par :

_____	_____
[Nom]	***[Nom]***
(Signature ou marque de la personne ou d'un parent/tuteur)	(Signature ou marque de l'enfant) [le cas échéant]

_____

Signature de l'interprète [le cas échéant]

** NOTE : Le consentement de l'enfant est requis dès lors qu'en raison de son âge et de sa maturité, il est raisonnablement nécessaire d'en tenir compte. Le consentement du parent ou du tuteur doit toujours être obtenu. Si l'enfant refuse de donner son consentement, aucune photographie ne sera prise, malgré le consentement donné par le parent ou le tuteur.*

MODELE 1.4

1.4 Autorisation type concernant les médias

AUTORISATION CONCERNANT LES MEDIAS

Je soussigné(e) *[nom de la personne ou d'un parent/du tuteur]* [selon le cas] autorise par la présente l'Organisation internationale pour les migrations (OIM) et toute autre personne ou entité autorisée agissant au nom de l'OIM à divulguer les informations personnelles me concernant et, le cas échéant, les données à caractère personnel des personnes à ma charge, *[Nom du ou des enfants/des membres de la famille]* à *[nom du tiers]*, et à lui permettre d'entrer en contact avec moi.

1. J'ai bien compris que *[nom du tiers]* a demandé à pouvoir m'interviewer et à me filmer [ainsi que la ou les personnes à ma charge, le cas échéant] afin de produire et de diffuser un témoignage audio et vidéo dans le but suivant :

.....

.....

.....

2. Les risques et les conséquences de ma participation à l'interview et au film m'ont été expliqués ; par la présente, je donne mon autorisation à la réalisation du but précité. J'ai bien compris que l'enregistrement audio et vidéo de mon témoignage pourra être diffusé dans un cadre public.

3. Sauf accord contraire par écrit, j'ai bien compris que *[nom du tiers]* veillera à ce que les conditions suivantes soient réunies :

a) Mon nom et mon adresse ne seront pas mentionnés pendant l'entretien, et les informations géographiques me concernant seront protégées.
b) Mon visage et ma voix seront rendus méconnaissables.
c) Une copie de la bande magnétique de l'interview me sera remise après la production du film vidéo.
d) L'OIM et *[nom du tiers]* n'utiliseront la bande magnétique de l'interview que dans le but de produire le film vidéo demandé.

4. J'ai été informé(e) qu'un accord écrit serait conclu entre moi-même et *[nom du tiers]*. Par la présente, je décharge et libère l'OIM, ses fonctionnaires, employés et agents de toute obligation, et accepte de les mettre hors de cause en cas de dommages causés, directement ou indirectement, à moi-même, à ma famille ou à mes proches en raison de la présente autorisation.

5. J’ai bien compris la teneur de la présente autorisation :

a) Après avoir lu les dispositions précitées : OUI/NON
b) Après que les dispositions précitées m’ont été traduites ou qu’il m’en a été donné lecture : OUI/NON

Je fais cette déclaration de mon plein gré et consens librement à ce que l’OIM divulgue mes données à caractère personnel.

Signé à (lieu) ……, le (date) ……..

[Nom] (Signature ou marque de la personne concernée ou d’un parent/du tuteur)	[Nom] (Signature ou marque de l’enfant) [le cas échéant]

Signature de l’interprète
[le cas échéant]

** NOTE : Cette autorisation type concernant les médias peut être utilisée pour faciliter l’accès aux bénéficiaires de l’OIM et/ou la divulgation de données à caractère personnel consécutivement à une demande adressée par les médias. Sauf accord exprès et écrit de la personne concernée, les visages seront floutés et les identités cachées. Ces précautions sont indispensables dans les cas extrêmement sensibles et pour les personnes vulnérables qui peuvent être en danger. Toute demande adressée par les médias pour rencontrer des personnes concernées ou accéder à leurs données à caractère personnel devra être analysée au cas par cas, après avoir déterminé le niveau de risque et s’être assuré que les questions de protection ont été prises en considération.*

MODELE 2.1

2.1 Clauses types à l'intention des tiers traitant des données à caractère personnel

CLAUSES CONTRACTUELLES GENERALES A L'INTENTION DES TIERS TRAITANT DES DONNEES A CARACTERE PERSONNEL

Confidentialité des données à caractère personnel

….. *(Nom du tiers)*…..… se conformera aux principes de protection des données de l'OIM lorsqu'il(elle) recueille, reçoit, utilise, transfère ou stocke toute donnée à caractère personnel lors de l'exécution du présent accord. ……..*(Nom du tiers)*…..… conservera les données à caractère personnel qu'il(elle) reçoit de l'OIM dans des conditions strictes de confidentialité et de sécurité, et ne les communiquera à aucun tiers sans l'autorisation écrite préalable de l'OIM. L'accès aux données à caractère personnel sera donné uniquement pour répondre « au besoin d'en connaître » aux employés et aux agents autorisés de ……. *(nom du tiers)*…..… qui acceptent d'être tenus par les obligations de confidentialité au titre du présent accord. L'obligation de confidentialité découlant de la présente clause subsistera après l'expiration ou la résiliation de l'accord.

[OU]

Clause standard de confidentialité

Toute information, y compris les informations à caractère personnel des bénéficiaires, dont ……..*(Nom du tiers)*…..… entre en possession ou a connaissance du fait du présent accord ou du projet, doit être traitée de manière strictement confidentielle. ……..*(Nom du tiers)*…..… ne communiquera d'informations de ce genre à aucun tiers sans l'autorisation écrite préalable de l'OIM. ……..*(Nom du tiers)*…..… se conformera aux principes de protection des données de l'OIM lorsqu'il(elle) recueille, reçoit, utilise, transfère ou stocke toute donnée à caractère personnel lors de l'exécution du présent accord. L'obligation de confidentialité découlant de la présente clause subsistera après l'expiration ou la résiliation de l'accord.

Confidentialité de la source d'information

…….. (Nom de l'organisme juridique)…..… veillera à ce que l'identité de la personne concernée (si elle est divulguée) et le rôle joué par l'OIM dans la communication de données à caractère personnel demeurent strictement confidentiels et ne soient en aucun cas communiqués à des tiers sans le consentement écrit préalable de la personne concernée et de l'OIM.

Destruction des données à caractère personnel

En cas de résiliation du présent accord ou de réalisation de la ou des finalités déterminées qui y sont prévues, *……..(nom du tiers)…..…* cessera d'accéder aux données à caractère personnel reçues de l'OIM, de les utiliser, ou de les traiter. *……..(Nom du tiers)…..…* restituera les données à caractère personnel à l'OIM et en détruira toutes les copies dans un délai de *……..(période de conservation)……..… /(à l'expiration ou à la résiliation du présent accord)* et certifiera que lui-même, ses agents et sous-traitants ont détruit toute trace de ces données.

Propriété des données à caractère personnel

L'OIM se réserve tous les droits de propriété se rapportant aux données à caractère personnel qu'elle reçoit des personnes concernées ou qui sont recueillies en son nom. Elle détient tous les droits d'auteur et autres droits de propriété intellectuelle découlant du présent accord. *……..(Nom du tiers)…..…* ne peut, pour quelque raison que ce soit, utiliser, publier, mentionner ou citer les données à caractère personnel sans l'autorisation écrite préalable de l'OIM, sauf dans les cas prévus par le présent accord.

[OU]

Clause standard de propriété intellectuelle

L'OIM détient tous les droits de propriété intellectuelle et autres droits de propriété, notamment mais pas exclusivement les droits de brevet, les droits d'auteur, les droits sur la marque et les droits de propriété des données découlant de l'exécution du projet, et a le droit d'en utiliser, reproduire, adapter, publier et diffuser sans restriction tout élément ou partie.

Résiliation de l'accord

L'OIM se réserve le droit de résilier le présent accord à tout moment, sans préjudice d'une demande de dommages-intérêts au cas où ……..*(nom du tiers)*……. manquerait aux obligations énoncées dans le présent accord.

[OU]

Clause standard de résiliation

L'une ou l'autre partie peut résilier le présent accord moyennant un préavis de [X mois] adressé par écrit à la partie cocontractante. Cependant, en cas de violation, par…….. *(nom du tiers)*……, de l'un quelconque des termes et conditions du présent accord, l'OIM peut mettre fin à l'accord avec effet immédiat.

**** NOTE : Ces clauses contractuelles types seront adaptées selon la nature de chaque accord conclu avec le tiers. Elles peuvent être utilisées pour tout contrat établi avec des fournisseurs de services, des partenaires d'exécution, des donateurs ou autres qui nécessite de recueillir, recevoir, utiliser, transférer ou stocker des données à caractère personnel concernant des bénéficiaires de l'OIM.***

MODELE 2.2

2.2 Clauses types relatives aux contrats de transfert et au traitement de données à caractère personnel

TRANSFERT AUX TIERS

Clause générale de protection des données

…….. *(Nom du tiers)* …..… se conformera aux principes de protection des données de l'OIM lorsqu'il(elle) recueille, reçoit, utilise, transfère ou stocke toute donnée à caractère personnel lors de l'exécution du présent accord. Cette obligation subsistera après l'expiration ou la résiliation de l'accord.

…….. *(Nom du tiers)* …..… a bien compris que l'OIM est liée par le devoir de confidentialité à l'égard des données à caractère personnel qu'elle reçoit des personnes concernées ou qui sont recueillies en son nom. Les données à caractère personnel demeureront en tout temps strictement confidentielles, et ne seront divulguées à des tiers sans le consentement écrit préalable de la personne concernée et de l'OIM.

Non-divulgation

…….. *(Nom du tiers)* …..… se conformera aux principes de protection des données de l'OIM lorsqu'il(elle) recueille, reçoit, utilise, transfère ou stocke des données à caractère personnel lors de l'exécution du présent accord.

…….. *(Nom du tiers)* …..… n'utilisera les données à caractère personnel confidentielles qu'il(elle) reçoit de l'OIM qu'en vue de la ou des finalités déterminées prévues par le présent accord, et il(elle) ne divulguera, ne publiera et ne transmettra à un tiers, indirectement ou directement, aucune de ces données sans l'autorisation écrite préalable de l'OIM.

Obligations générales incombant aux tiers

…….. *(Nom du tiers)* …..… prendra toutes les précautions raisonnables et nécessaires pour protéger la confidentialité des données à caractère personnel et l'anonymat des personnes concernées. Toutes les données à caractère personnel seront recueillies, utilisées, transférées, stockées en toute sécurité et détruites conformément aux principes de protection des données de l'OIM.

…….. *(Nom du tiers)* …..… atteste qu'il(elle) observera les mesures de protection des données

énoncées dans le présent accord et qu'il(elle) s'acquittera des obligations qui lui incombent au titre du présent accord de façon à éviter que ses obligations en matière de protection des données envers les personnes concernées ne soient violées. ……. *(Nom du tiers)* …..… s'engage en particulier à :

1. Utiliser les données à caractère personnel qu'il(elle) reçoit de l'OIM exclusivement pour atteindre la ou les finalités déterminées du transfert prévue(s) dans le présent accord.
2. Prendre des mesures de sécurité des données appropriées afin de préserver l'intégrité des données à caractère personnel et d'empêcher leur altération, perte, dommage, accès non autorisé ou divulgation abusive.
3. Observer des règles de confidentialité strictes, appliquer des mesures de contrôle d'accès appropriées, et veiller à ce que toute transmission de données à caractère personnel soit cryptée.
4. Prendre toutes les dispositions raisonnables pour que tous ses employés, agents et sous-traitants se conforment aux obligations de confidentialité au titre du présent accord.
5. Interdire tout traitement des données à caractère personnel qui n'est pas conforme aux conditions énoncées dans le présent accord.
6. Immédiatement mettre à jour, rectifier et/ou supprimer les données à caractère personnel sur instruction de l'OIM.
7. Informer l'OIM de toute réglementation interne ou de toute disposition législative ou réglementaire nationale, actuelle ou future, qui pourrait influer sur les principes de protection des données de l'OIM.
8. Ne pas traiter plus avant, divulguer, publier ou transmettre les données à caractère personnel à un tiers sans l'autorisation écrite préalable de l'OIM.
9. Ne conserver les données à caractère personnel que dans la mesure et selon les modalités nécessaires à la réalisation de la ou des finalités déterminées du transfert.
10. Détruire les données à caractère personnel dans un délai de ……. *(période de conservation) ……./ (à l'expiration ou à la résiliation du présent accord)* à compter de la date de réalisation de la ou des finalités déterminées du transfert, et remettre à l'OIM un certificat attestant que toute trace des données à caractère personnel a été détruite.

Obligations propres aux agents qui recueillent des données à caractère personnel pour le compte de l'OIM

Lorsque, conformément aux obligations qui lui incombent au titre du présent accord, ……. *(nom de l'agent)* ……. recueille et traite des données à caractère personnel pour le compte de l'OIM, il(elle) :

1. Se conformera aux principes de protection des données de l'OIM, qui font partie intégrante du présent accord [à joindre en annexe].
2. Recueillera et traitera les données à caractère personnel conformément aux instructions reçues de l'OIM. [Il peut s'agir d'instructions particulières ou générales énoncées dans le présent accord, ou notifiées par l'OIM pendant la période de traitement des données.]
3. Ne traitera les données à caractère personnel que dans la mesure et selon les modalités

nécessaires à la réalisation de la ou des finalités prévues dans le présent accord.

4. Ne transférera les données à caractère personnel aux agents ou aux sous-traitants qu'avec l'autorisation écrite préalable de l'OIM, en conformité avec les principes de protection des données de l'OIM.

[Ces obligations seront ajoutées aux obligations générales incombant aux tiers énoncés plus haut, si les données à caractère personnel sont recueillies et traitées pour le compte de l'OIM.]

**** NOTE : Ces clauses contractuelles types seront adaptées et complétées selon la nature du contrat de transfert et les relations entre l'OIM et le tiers. Les clauses relatives à la « confidentialité », à la « propriété », à la « destruction » et à la « résiliation » reproduites dans le modèle 2.1 seront également incorporées dans le contrat de transfert.***

MODELE 3

3.1 Formulaire général de confidentialité à l'intention du personnel, des stagiaires et des consultants

ACCORD DE CONFIDENTIALITE

Par la présente, je reconnais qu'en ma qualité de …… *(compléter)* …… j'aurai accès à des données à caractère personnel confidentielles concernant les bénéficiaires de l'OIM.

1. J'ai bien compris que l'OIM est liée par un devoir de confidentialité à l'égard des données à caractère personnel qu'elle reçoit des personnes concernées. Les données à caractère personnel resteront toujours confidentielles entre l'OIM et la personne concernée, et ne seront pas communiquées à des tiers sans le consentement écrit préalable de la personne concernée.

2. Je me conformerai aux principes de protection des données de l'OIM lorsque je recueille, reçois, utilise, transfère, stocke ou détruis toute donnée à caractère personnel lors de l'exécution du présent accord de confidentialité.

3. Par la présente, j'accepte de traiter toutes les données à caractère personnel auxquelles j'ai accès en toute prudence et confidentialité.

4. En vertu de la présente déclaration :

    1. J'accepte de préserver l'anonymat des bénéficiaires de l'OIM et la confidentialité des données à caractère personnel qui me sont communiquées.
    2. J'accepte de ne pas divulguer de données à caractère personnel confidentielles se rapportant au projet …… *(nom du projet de l'OIM et code de projet)* …… autres que celles requises par mes fonctions particulières, sans l'autorisation de l'administrateur de projet et/ou du responsable du traitement des données.
    3. J'accepte de ne divulguer à personne ni à aucune entité des données à caractère personnel confidentielles se rapportant au projet …… *(indiquer le projet de l'OIM)* ……, pendant ou après mon activité salariée à l'OIM.
    4. J'ai bien compris que je ne peux m'entretenir d'aucune question relative à un cas précis avec les médias sans avoir demandé et obtenu l'autorisation de l'administrateur de projet et/ou du responsable du traitement des données précisant la nature, l'objectif et les limites de toute communication aux médias, et j'y consens.
    5. J'accepte de signaler à l'administrateur de projet et/ou au responsable du traitement des données tout manquement à mes obligations ou tout conflit d'intérêts au titre du présent accord de confidentialité.
    6. J'ai bien compris qu'en cas de violation délibérée du présent accord de confidentialité, l'OIM prendra des mesures appropriées à mon encontre.

7. J’ai bien compris que l’obligation de respecter le présent accord de confidentialité subsistera après ma cessation de service à l’OIM, et j’y consens.

5. En signant et en renvoyant un exemplaire du présent accord de confidentialité à l’administrateur de projet et/ou au responsable du traitement des données chargé du projet ……. *(indiquer le projet de l’OIM)* …… ou à la personne qu’il aura désignée, je confirme que j’ai bien compris et que j’accepte les clauses susmentionnées, et m’engage à respecter les termes du présent accord.

Signé à (lieu) ……, **le (date)** …….

……
Signature

MODELE 4

4. Formulaire de demande d'accès des personnes concernées à leurs données à caractère personnel

FORMULAIRE DE DEMANDE D'ACCES DES PERSONNES CONCERNEES

1. Nom du demandeur.....
2. Prénom du demandeur.....
3. Date de naissance (JJ/MM/AAAA).....
4. Numéro d'enregistrement/de la demande (s'il y a lieu/s'il est connu).....
5. Adresse :.....
   .....
   .....
   .....
   Code postal :.....
   Téléphone : .....
6. Etes-vous : a) La personne concernée ? OUI / NON

   b) Un représentant de la personne concernée dûment mandaté par écrit ? OUI/NON
7. Quelles catégories de données à caractère personnel demandez-vous ?

   .....
   .....
   .....
   .....
   .....
   .....

Signé à (lieu)..... **le (date)**.....

.....

Signature du demandeur

LISTE DE VERIFICATION 1

LISTE DE VERIFICATION – QUALITE DES DONNEES

QUALITE	OUI	NON
Les enquêteurs ont-ils reçu une formation qui les sensibilise à l'importance de préserver la qualité des données tout au long du processus de collecte des données ?		
Les sites de collecte ont-ils été vérifiés de façon à ce que les données à caractère personnel soient fournies dans des conditions sûres et sécurisées ?		
Les enquêteurs ont-ils souligné l'attachement de l'OIM à la confidentialité des données à caractère personnel ?		
La nécessité de disposer de données à caractère personnel véridiques a-t-elle été soulignée, et les conséquences d'une utilisation de données à caractère personnel inexactes ont-elles été mises en évidence ?		
Les personnes concernées ont-elles validé les catégories de données à caractère personnel fournies à l'enquêteur ?		
Le format et le support des dossiers électroniques ont-ils été vérifiés et transférés sur un support compatible ?		
Les dossiers électroniques sont-ils stockés sur des supports sûrs qui sont protégés contre les risques en matière de sécurité et un accès non autorisé, et des sauvegardes régulières sont-elles effectuées ?		
Les dossiers papier sont-ils stockés dans un lieu sûr pour prévenir leur détérioration et tout accès non autorisé ?		
Les dossiers papier et électroniques sont-ils lisibles et ont-ils été mis à jour ?		
PERTINENCE	**OUI**	**NON**
La qualité des données à caractère personnel est-elle altérée par des inexactitudes ?		
Des changements importants ont-ils rendu inutiles les données à caractère personnel initialement enregistrées ?		
La situation des personnes concernées a-t-elle changé, et de nouveaux éléments rendent-ils les données initialement enregistrées obsolètes et sans intérêt ?		
Les anciens supports électroniques ont-ils été remis à la Division ITC de l'OIM pour destruction ?		
Dans quelle mesure les données initialement enregistrées peuvent-elles encore apporter une valeur ajoutée aux objectifs du projet de l'OIM, et vaut-il la peine de continuer à les conserver ?		
Les données à caractère personnel sans intérêt et inutiles peuvent-elles être utilisées à des fins statistiques ou de recherche compatibles avec la finalité déterminée pour laquelle les données à caractère personnel ont été recueillies ?		

EXACTITUDE	OUI	NON
L'exactitude des données a-t-elle été vérifiée par les enquêteurs au moment de la collecte ?		
L'exactitude des données a-t-elle été vérifiée par des membres autorisés du personnel de l'OIM au moment de la conversion des dossiers papier en dossiers électroniques ?		
Les mises à jour ont-elles été correctement enregistrées dans les dossiers électroniques et papier ?		
L'exactitude des données a-t-elle été vérifiée par des membres autorisés du personnel de l'OIM au moment de l'extraction et avant l'utilisation ?		
Les catégories de données à caractère personnel ont-elles été vérifiées avant l'utilisation et la divulgation ?		

Date de la précédente évaluation de la qualité des données……..

Signé à (lieu)……., **le (date)**…….……..

……

Signature du responsable
du traitement des données

LISTE DE VERIFICATION 2

LISTE DE VERIFICATION – EVALUATION DES RISQUES EN MATIERE DE SECURITE DES DONNEES

CONTROLE DES SYSTEMES ACTUELS	OUI	NON
Les données à caractère personnel sensibles qui relèvent de votre domaine de responsabilité sont-elles toutes classées correctement, selon le niveau de sensibilité qui leur est appliqué ?		
Avez-vous analysé le niveau de sécurité aux postes de travail sous l'angle du degré de sensibilité, de la confidentialité, de l'intégrité, de la transmission et de l'accès aux données à caractère personnel ?		
Avez-vous constaté des facteurs environnementaux, techniques ou humains qui posent des problèmes de sécurité particuliers ?		
Toutes les mesures physiques et techniques importantes ou utiles qui relèvent de votre sphère de contrôle ont-elles été identifiées ?		
Avez-vous déterminé de quelle manière poursuivre les opérations et la fourniture de services en cas de perte de données à caractère personnel ?		
Vous êtes-vous concerté avec l'informaticien compétent pour que des sauvegardes soient effectuées régulièrement afin de préserver les dossiers électroniques en cas de perte accidentelle ?		
Avez-vous participé à des exercices de contrôle fiables réalisés avec des membres du personnel autorisés qui stockent des données à caractère personnel extrêmement sensibles dans des systèmes informatiques non protégés ?		
Avez-vous évalué les lieux de stockage et les mesures de sécurité nécessaires pour protéger les dossiers papier ?		
Avez-vous évalué les emplacements de stockage électronique et les mesures de sécurité nécessaires pour protéger les dossiers électroniques ?		
Vous êtes-vous renseigné sur la disponibilité de logiciels de cryptage ?		
IDENTIFICATION DES RISQUES EN MATIERE DE SECURITE	**OUI**	**NON**
Avez-vous étudié les menaces pesant sur la sécurité des lieux de stockage ou du système informatique utilisé pour stocker des données à caractère personnel ?		
Avez-vous étudié les faiblesses éventuelles des lieux de stockage et des systèmes informatiques ?		
Avez-vous évalué les effets des procédés utilisés par certaines personnes pour accéder sans autorisation aux systèmes de sécurité ?		
Avez-vous analysé les conséquences et incidences que les risques en matière de sécurité pourraient avoir sur la confidentialité, l'intégrité et la disponibilité des données à caractère personnel ?		
Avez-vous prévu la façon dont les risques peuvent être atténués compte tenu des mesures de sécurité opérationnelles, techniques et physiques actuellement disponibles ?		
Prévoyez-vous d'autres mesures d'atténuation des risques qui pourraient être		

appliquées au poste de travail en question ?		
GARANTIES IDENTIFIEES	**OUI**	**NON**
Avez-vous identifié de nouvelles mesures de sécurité pour faire face au niveau de risques en matière de sécurité et le réduire ?		
Avez-vous testé la faisabilité des nouvelles mesures de sécurité identifiées ?		
Avez-vous déterminé la probabilité résiduelle de la menace après la mise en œuvre des mesures identifiées ?		

Date de la précédente évaluation des risques en matière de sécurité des données……..…….

Signé à (lieu)……., **le (date)**…….

……

Signature du responsable
du traitement des données

LISTE DE VERIFICATION 3
LISTE DE VERIFICATION – PROTECTION DES DONNEES

DOCUMENTS REQUIS (Voir les modèles relatifs à la protection des données de l'OIM)
☐ Formulaire de demande d'accès : (si nécessaire) pour donner effet au droit des personnes concernées d'accéder à leurs données à caractère personnel.
☐ Formulaire de consentement : indiquer la finalité déterminée, les finalités déterminées additionnelles, le continuum de l'aide, les finalités de recherche additionnelles de l'OIM/ou autres finalités additionnelles et les transferts prévisibles à des tiers. Si le formulaire de consentement est converti sous forme électronique ou téléchargé dans une base de données aux fins de stockage, l'encadré de consentement doit être rempli avec exactitude. Les encadrés de consentement sous forme électronique indiqueront la forme du consentement et les catégories de finalités déterminées pour lesquelles le consentement a été obtenu.
☐ Autorisation concernant les médias : autoriser l'accès aux bénéficiaires et/ou la divulgation de leurs données à caractère personnel aux médias.
☐ Formulaire de confidentialité : autoriser le personnel, les stagiaires et les consultants de l'OIM à accéder aux données à caractère personnel et à les traiter.
☐ Liste de vérification relative à la qualité des données : évaluer la pertinence et l'exactitude des données tout au long du cycle de leur traitement.
☐ Liste de vérification relative à la sécurité des données : évaluer les mesures techniques et physiques de sécurité des données prises tout au long du cycle de traitement des données.
☐ Formulaires d'entretien, d'enregistrement et de demande : inclure dans les formulaires préexistants des clauses relatives à la protection des données, à la confidentialité, à la déclaration de consentement et d'autres clauses pertinentes.
☐ Contrats de transfert : inclure dans les contrats de services, les mémorandums d'accord et les accords de mise en œuvre des clauses relatives à la protection des données, aux finalités déterminées, à la confidentialité des données à caractère personnel (et de l'OIM en tant que source, si nécessaire), à la non-divulgation, à la sécurité des données, à la destruction des données, à la propriété, aux privilèges et immunités et d'autres clauses pertinentes.
INDICATEURS UTILES POUR LA PHASE ANTERIEURE À LA COLLECTE DE DONNEES
☐ Conciliation des intérêts : réaliser un juste équilibre entre les objectifs du projet de l'OIM et les droits et intérêts des personnes concernées.
☐ Proportionnalité : veiller à ce qu'il existe une proportionnalité, ou un équilibre judicieux, entre toute limitation de la protection des données et les avantages tirés du projet de l'OIM.
☐ Probabilité et ampleur du préjudice : Examiner la probabilité du préjudice et la façon dont il peut se répercuter sur les personnes concernées, le personnel de l'OIM ou les autres personnes habilitées intervenant dans le processus de collecte, et veiller à ce que des garanties suffisantes soient en place pour prévenir les menaces et les pratiques discriminatoires.
☐ Flexibilité : faire preuve d'une flexibilité suffisante pour tenir compte de la diversité des personnes touchées par le projet de l'OIM, et envisager des degrés de sensibilité accrue.

☐ Diffusion de l'information : communiquer aux personnes concernées des informations suffisantes pour qu'elles comprennent clairement tous les avantages liés à la fourniture de données à caractère personnel et les risques réels associés à la dissimulation de certaines catégories de données à caractère personnel. Toute relation préexistante avec des donateurs, des partenaires de l'OIM, des partenaires d'exécution et des fournisseurs de services devra être communiquée aux personnes concernées. Le consentement aux finalités de recherche additionnelles de l'OIM et aux transferts prévisibles à des tiers devra être obtenu au moment de la collecte des données.
☐ Règles minimales : garantir le respect de la vie privée et la confidentialité, et promouvoir l'adoption de mesures de protection suffisantes pour le traitement continu des données à caractère personnel.
☐ Transparence et obligation redditionnelle : veiller à une bonne information, à l'existence de procédures d'accès et de plainte, et à la surveillance du processus de collecte des données.
☐ Vérification après la mise en œuvre : évaluer le rapport risques/avantages, se demander si des risques imprévus sont apparus, et informer les personnes concernées de tout risque additionnel.
INDICATEURS UTILES CONCERNANT LE RAPPORT RISQUES/AVANTAGES
☐ Déterminer si les limites aux principes de la protection de la vie privée et de la confidentialité sont acceptables au regard des attentes raisonnables des personnes concernées.
☐ Décider si le projet de l'OIM est suffisamment important pour justifier des restrictions aux droits et intérêts des personnes concernées. L'importance du projet de l'OIM doit être déterminée sur la base du mandat de l'OIM et des circonstances entourant le projet de l'OIM, parmi lesquelles figurent la protection des personnes concernées, les mesures exigées par la communauté internationale, l'intérêt général, les atteintes aux droits de l'homme, les catastrophes naturelles, etc..
☐ Déterminer si les risques en matière de sécurité, de santé ou de discrimination sont raisonnables par rapport aux avantages, et dans quelle mesure ces risques peuvent être réduits au minimum.
☐ Tenir compte des circonstances particulières et des vulnérabilités des personnes concernées, et promouvoir la prise en considération du sexe, de l'âge, de la langue, et des comportements sociaux, culturels ou religieux du groupe de population cible ou de chacune des personnes concernées.
☐ Veiller à ce que des garanties appropriées soient incluses dans le processus de collecte des données, afin de protéger les droits et le bien-être des personnes concernées susceptibles d'être exposées à la coercition ou à l'intimidation comme, par exemple, les enfants, les détenus, les femmes enceintes victimes ou présumées victimes de la traite, les personnes physiquement ou mentalement handicapées, ou les personnes concernées qui sont défavorisées sur le plan économique ou éducatif.
☐ Donner aux personnes concernées une description juste et exacte des risques et des avantages au moment de la collecte de données.
☐ Réexaminer régulièrement l'équilibre entre les risques et les avantages, afin de tenir compte d'une éventuelle modification du rapport risques/avantages.
☐ Prévoir une formation adaptée pour les membres du personnel de l'OIM et ceux qui participent au processus de collecte de données.

☐ Analyser les effets des flux de données à caractère personnel sur les droits et les intérêts des personnes concernées tout au long du cycle de traitement des données, et veiller à ce que des mesures en matière de sécurité des données soient prises pour réduire les risques au minimum et maximiser les avantages.
INDICATEURS UTILES CONCERNANT LA FINALITE
☐ Examiner la mesure dans laquelle la finalité déterminée, les finalités connexes et les finalités additionnelles ont été expliquées aux personnes concernées au moment de la collecte des données.
☐ Déterminer si les personnes concernées peuvent raisonnablement s'attendre à ce que leurs données à caractère personnel soient utilisées et divulguées pour des finalités secondaires visant à atteindre la finalité déterminée initiale.
☐ Tenir un registre des divulgations qui sont nécessaires pour atteindre la finalité déterminée.
☐ Surveiller en permanence l'utilisation et la divulgation des données à caractère personnel pour s'assurer qu'elles se limitent à la finalité déterminée initiale.
☐ Déterminer si des catégories de données à caractère personnel sont utilisées ou divulguées en vue de finalités incompatibles.
☐ Arrêter les mesures qu'il est nécessaire de prendre pour remédier à une utilisation et à une divulgation de données à caractère personnel inappropriées et incompatibles.
INDICATEURS UTILES EN MATIERE DE COMPATIBILITE
☐ La finalité déterminée additionnelle (p. ex., une recherche ultérieure en vue de finalités de l'OIM) était prévue au moment de la collecte des données, et la personne concernée a expressément consenti à ce que, pour atteindre la finalité déterminée additionnelle, ses données à caractère personnel soient partagées entre des projets de l'OIM explicitement désignés.
☐ La finalité déterminée additionnelle est compatible avec la finalité déterminée initiale pour laquelle les données à caractère personnel ont été recueillies et traitées.
☐ Le consentement a été donné au moment de la collecte des données pour un « continuum d'aide », en sachant que les données à caractère personnel seraient utilisées par des unités/départements spécifiques de l'OIM dans l'intérêt des personnes concernées tout au long du cycle de traitement des données.
☐ La finalité déterminée additionnelle est nécessaire pour apporter une aide supplémentaire aux personnes concernées, et il n'y a aucune raison de penser que le consentement serait refusé dès lors que rien n'empêche qu'il soit obtenu.
INDICATEURS EN MATIERE DE QUALITE DES DONNEES
☐ Examiner les circonstances dans lesquelles les données sont recueillies, pour garantir un environnement sûr et favoriser la fourniture de données à caractère personnel véridiques.
☐ Prendre des dispositions raisonnables pour vérifier l'exactitude et la véracité des données à caractère personnel au moment de leur collecte.
☐ Veiller à ce que les enquêteurs soient correctement formés, afin de préserver la qualité des données tout au long du processus de collecte.
☐ Encourager la double vérification avant la saisie de données à caractère personnel, et la vérification préalable avant l'utilisation et la divulgation de données à caractère personnel.
☐ Vérifier les catégories de données à caractère personnel, le mode de stockage et les conséquences éventuelles de l'utilisation de données à caractère personnel inexactes.
☐ Tenir compte de l'importance des inexactitudes et se demander si elles sont susceptibles d'influer sur l'utilisation continue des données à caractère personnel.

☐ Veiller à ce que les dossiers électroniques soient compatibles avec la technologie utilisée par le bureau extérieur de l'OIM.
☐ Encourager l'utilisation des dossiers originaux contenant des données à caractère personnel exactes parce que le filtrage augmente le risque d'erreurs.
INDICATEURS EN MATIERE DE COMMUNICATION
☐ Souligner l'importance du consentement.
☐ Expliquer la nature et les catégories de données à caractère personnel requises.
☐ Enoncer les finalités spécifiques et connexes pour lesquelles les données à caractère personnel sont recueillies.
☐ Veiller à ce que les avantages de la collecte de données et le besoin de données à caractère personnel véridiques et exactes soient clairement expliqués.
☐ Appeler l'attention sur le flux interne de données à caractère personnel au sein d'un projet particulier de l'OIM, et sur le flux nécessaire de données à caractère personnel entre divers projets de l'OIM.
☐ Décrire les méthodes de saisie et de stockage utilisées pour garantir la sécurité et la confidentialité des données.
☐ Indiquer clairement l'utilisation et les divulgations, tous les transferts prévisibles et toutes les finalités déterminées additionnelles qui sont prévues au moment de la collecte des données.
☐ Indiquer en détail les relations préexistantes entre l'OIM et des tiers (agents, fournisseurs de services, partenaires d'exécution, donateurs, partenaires de l'OIM, pays dans lesquels intervient l'Organisation, pays hôtes, institutions gouvernementales, forces de police, etc.), et préciser les divulgations nécessaires et prévisibles.
☐ Veiller à ce que les avantages de la collecte de données, du traitement des données, et tous les transferts prévisibles soient précisés au moment de la collecte des données.
☐ Indiquer les conséquences d'un refus de donner son consentement, et préciser que celui-ci peut être retiré à chaque étape du cycle de traitement des données.
☐ Insister sur l'attachement de l'OIM à la protection des données, et expliquer les procédures d'accès et de plainte.
INDICATEURS UTILES EN MATIERE DE CONSENTEMENT
☐ Vérifier si les personnes concernées ont la capacité de donner leur consentement, et consulter l'unité/le département compétent de l'OIM et le Bureau des affaires juridiques au Siège de l'OIM au sujet de la collecte de données à caractère personnel concernant les enfants et les personnes mentalement handicapées.
☐ Songer à la forme du consentement (explicite, implicite ou par procuration) compte tenu du projet particulier de l'OIM. Toujours obtenir un consentement écrit, si possible. Si un consentement implicite a été obtenu, s'assurer que les personnes concernées ont été informées des finalités déterminées. Si un consentement par procuration a été obtenu, veiller à ce que tous les membres de la famille soient présents et, si ce n'est pas possible, veiller à ce que leurs données à caractère personnel soient vérifiées dès que possible.
☐ Donner tous les détails nécessaires pour que les personnes concernées puissent saisir et comprendre les conséquences du consentement.
☐ Encourager les enquêteurs à insister sur les finalités déterminées et connexes, ainsi que sur toutes les finalités déterminées additionnelles, telles que le continuum de l'aide, les recherches additionnelles au sein de l'OIM et d'autres finalités prévues. Le consentement doit être obtenu au moment de la collecte des données pour toutes les divulgations prévisibles à des tiers.

☐ Dans la mesure du possible, s'assurer que les formulaires ou les déclarations de consentement ont été signés et, lorsque les données à caractère personnel sont saisies sur le terrain sous forme électronique, faire signer une feuille de consentement collectif en veillant à ce que toutes les personnes concernées y apposent leur signature.
☐ Saisir la liste des catégories de finalités déterminées pour lesquelles un consentement a été obtenu, et s'assurer que les documents convertis sous forme électronique et les bases de données contiennent des cases de consentement.
INDICATEURS UTILES EN MATIERE DE TRANSFERT
☐ Consulter l'unité/le département de l'OIM et le Bureau des affaires juridiques, au Siège, avant toute divulgation.
☐ Analyser la finalité déterminée de la divulgation, et se demander comment elle permettra d'atteindre la finalité déterminée de la collecte et du traitement des données.
☐ Veiller au respect des principes de l'OIM relatifs à la protection des données, et tenir compte des lois et réglementations nationales relatives à la protection des données qui peuvent également s'appliquer à des tiers.
☐ Evaluer la situation dans le pays, le respect des droits de l'homme et la sécurité des personnes concernées.
☐ Assurer un niveau de protection des données comparable, et veiller à ce que des garanties soient données en vertu d'une obligation contractuelle écrite.
☐ Encourager le partage de données à caractère non personnel globales et anonymes.
☐ Limiter la quantité de données à caractère personnel à ce qui est nécessaire pour atteindre la finalité déterminée du transfert, et s'assurer que les dossiers originaux contenant des données à caractère personnel sont conservés.
☐ Donner aux personnes concernées une description appropriée des données à caractère personnel qui doivent être transférées, et des tiers associés au processus.
☐ S'assurer que la méthode de divulgation et de transmission des données à caractère personnel est sûre.
☐ Garantir une transmission sûre en veillant à assurer le niveau de confidentialité le plus élevé, en utilisant des outils de cryptage en cas de besoin, et en vérifiant si les tiers disposent d'outils de décryptage compatibles.
☐ Conserver un registre de toutes les divulgations qui indique une justification raisonnable de la divulgation et la catégorie de données à caractère personnel divulguées.
INDICATEURS UTILES EN MATIERE DE CONFIDENTIALITE
☐ Encourager un « climat de confidentialité » en veillant à ce que les membres du personnel de l'OIM, les consultants, les agents et les personnes représentant des tiers habilités soient suffisamment formés pour comprendre l'importance de la confidentialité des données à caractère personnel.
☐ Veiller à ce que les membres du personnel de l'OIM, les consultants, les agents et les migrants ou les autres bénéficiaires participant au processus de collecte des données soient suffisamment formés pour pouvoir communiquer l'engagement de confidentialité de l'OIM aux personnes concernées au moment de la collecte des données.
☐ Limiter l'accès à certaines catégories de membres du personnel de l'OIM, de consultants et de personnes représentant des tiers habilités.
☐ Imposer des contrôles d'accès stricts et tenir un registre d'accès aux données à caractère personnel divulguées.
☐ Gérer la sécurité des dossiers électroniques et papier afin de prévenir toute extraction non autorisée.

☐	Se demander si des personnes concernées pourraient faire l'objet d'attaques physiques ou d'un traitement discriminatoire à la suite de la divulgation.
☐	Encourager un respect strict de la confidentialité en imposant une obligation contractuelle écrite, et s'assurer que tous les tiers acceptent de respecter la confidentialité des données à caractère personnel avant leur divulgation.
☐	Sécuriser toutes les transmissions de données à caractère personnel en s'assurant que la mention « Confidentiel » est indiquée dans toute correspondance, et que les destinataires des courriels sont sélectionnés avec discernement.
☐	Remplacer les identifiants par des codes lors du stockage et de la transmission de données à caractère personnel, surtout lorsqu'il s'agit de catégories de données à caractère personnel hautement sensibles.
☐	Encourager le respect strict de la confidentialité, afin d'éviter toute divulgation non intentionnelle à des personnes cherchant à obtenir un accès non autorisé aux données à caractère personnel.
☐	Surveiller l'élimination des documents imprimés et autres documents papier contenant des données à caractère personnel, y compris leur déchiquetage.
REPONSE AUX DEMANDES D'ACCES	
☐	Exiger une preuve d'identité.
☐	Tenir compte de l'intérêt supérieur de la personne concernée.
☐	Ne révéler des catégories de données à caractère personnel qu'en cas de « besoin d'en connaître ».
☐	Divulguer des résumés de dossiers individuels et/ou des copies de dossiers électroniques ou papier, s'il y a lieu.
☐	S'assurer que les représentants sont dûment autorisés par les personnes concernées.
☐	Accepter les demandes d'accès des représentants par écrit.
☐	Consigner toute demande d'accès, la date de la demande et les catégories de données à caractère personnel communiquées.
☐	Se montrer prudent à l'égard des demandes d'information sur des personnes concernées.
INDICATEURS UTILES EN MATIERE DE DESTRUCTION	
☐	Déterminer si les données à caractère personnel ont été utilisées pour atteindre la ou les finalités déterminées.
☐	Examiner si les données à caractère personnel peuvent être utilisées pour atteindre des finalités additionnelles conformément aux principes de l'OIM.
☐	Se concerter avec l'unité/le département compétent de l'OIM, au Siège, pour s'assurer que les données à caractère personnel ne sont pas détruites prématurément.
☐	Autoriser la destruction des données, et utiliser la méthode d'élimination la plus efficace.
☐	Procéder à une évaluation de la sensibilité et présenter à la Division ITC une liste des dossiers électroniques par catégories.
☐	Surveiller l'externalisation des activités de destruction, en veillant à ce que les tiers signent les formulaires de confidentialité afin de protéger les données à caractère personnel jusqu'à leur élimination définitive, et exiger la remise de certificats de destruction.
☐	Contrôler la destruction des données jusqu'à leur élimination définitive et joindre les documents d'élimination aux rapports finals de projet ou aux rapports de supervision.

INDICATEURS UTILES EN MATIERE DE CONFORMITE
☐ Sensibiliser et former à la protection des données.
☐ Distribuer des questionnaires détaillés pour savoir quelles pratiques de traitement des données sont suivies par les différents bureaux extérieurs de l'OIM. Il sera ainsi possible d'approuver et de surveiller la destruction de dossiers électroniques ou papier obsolètes.
☐ Consulter les correspondants pour la protection des données, le Bureau des affaires juridiques, les unités/départements compétents de l'OIM, et la Division Technologie de l'information et communications au Siège.
☐ Effectuer systématiquement des audits internes en distribuant des listes de vérification à intervalles réguliers.
☐ Soumettre des rapports d'évaluation en vue des audits annuels relatifs à la protection des données effectués par un organisme de vérification indépendant.
☐ S'assurer que la conception du projet englobe la protection des données, et que les propositions de projet tiennent dûment compte des dépenses indispensables, requises aux fins de mise en œuvre des principes de l'OIM.
☐ Mentionner les pratiques de protection des données dans les évaluations de projet internes/externes, ainsi que dans les rapports réguliers sur l'avancement des projets, qui doivent être établies selon la procédure mise en place à cette fin à l'OIM.
☐ Vérifier les rapports aux donateurs et les publications pour s'assurer que toute identification des personnes concernées est impossible et que tous les éléments identifiables ont été éliminés, surtout si le projet concerne des personnes vulnérables et des cas sensibles.

Signé à (lieu)……, **le (date)**……

……
Signature du responsable du traitement des données

……
Signature de l'administrateur de projet