RESTORING FAMILY LINKS

Réseau des liens familiaux du Mouvement international de la Croix-Rouge et du Croissant-Rouge

Code de conduite relatif à la protection des données à caractère personnel

Version 1.0

Novembre 2015

Avant-propos

Le présent Code de conduite a été rédigé par un groupe de travail (le « Groupe de travail ») composé de représentants de la Croix-Rouge autrichienne (Claire Schocher-Döring), de la Croix-Rouge de Belgique (Flandres) (Axel Vande Veegaete et Nadia Terweduwe), de la Croix-Rouge britannique (Mark Baynham et Emily Knox), de la Croix-Rouge allemande (Jutta Hermanns), du Bureau Croix-Rouge/Union européenne (Olivier Jenard), du Comité international de la Croix-Rouge (Romain Bircher, Massimo Marelli et Katja Gysin) et de la Fédération internationale des Sociétés de la Croix-Rouge et du Croissant-Rouge (Christopher Rassi). Plusieurs autres représentants de ces institutions ont également participé à la rédaction, aux discussions et aux réunions, auxquelles ils ont apporté une contribution importante. Le Groupe de travail a engagé les discussions sur ce projet à la fin de l'année 2013 et a tenu plusieurs réunions, à Mechelen (avril 2014), Bruxelles (juillet 2014), Vienne (septembre 2014), Sofia (novembre 2014) et Londres (janvier 2015), ainsi que de multiples conférences téléphoniques et échanges de courriels. Le Groupe de travail a tenu compte des observations formulées par de nombreuses de Sociétés nationales et a adopté le Code de conduite par consensus.

Le Code de conduite a été jugé nécessaire en raison 1) du grand nombre d'acteurs du Mouvement international de la Croix-Rouge et du Croissant-Rouge (le « Mouvement ») qui opèrent dans le cadre du Réseau des liens familiaux, et de la nécessité d'échanger des donnés au sein du Mouvement ainsi qu'avec d'autres acteurs, et 2) de l'évolution de l'environnement réglementaire en Europe et dans le monde en ce qui concerne la législation et les standards en matière de protection des données à caractère personnel (ci-après « données »). Le Code de conduite énonce les principes, engagements et procédures minimums que les membres du Mouvement doivent respecter lorsqu'ils traitent des données dans le cadre du Réseau des liens familiaux. Il s'aligne sur les normes les plus strictes en matière de protection des données, notamment la législation de l'Union européenne dans ce domaine. Les utilisateurs du Code de conduite doivent également s'assurer qu'ils respectent leur propre législation nationale. Le Code de conduite est un document de référence qui s'ajoute à l'ensemble de documents d'orientation du Mouvement sur le rétablissement des liens familiaux (RLF). Les différents membres du Mouvement devront l'adopter et le transposer dans leurs propres procédures de travail.

Le Code de conduite constitue un outil unique que tous les membres du Mouvement peuvent et doivent utiliser pour garantir les libertés et droits fondamentaux des personnes concernées par les activités de RLF, en particulier le droit au respect de la vie privée et à la protection des données personnelles. Nous espérons qu'il contribuera à renforcer la confiance des individus et des autorités de réglementation à l'égard des activités menées par Mouvement, ainsi que des membres du Mouvement qui sont amenés à échanger des données dans le cadre des activités de RLF.

Table des matières

DÉFINITIONS

Activités de rétablissement des liens familiaux et activités liées au rétablissement des liens familiaux

« Rétablissement des liens familiaux » (RLF) est un terme générique qui désigne diverses activités visant à prévenir la dispersion des familles et à aider les membres d'une même famille à rétablir et maintenir le contact entre eux, ainsi que des activités visant à élucider le sort de personnes disparues et à savoir où elles se trouvent.

Ces activités peuvent être liées à d'autres services de soutien, comme la fourniture d'une aide psychologique et psychosociale, juridique, administrative et matérielle aux familles et autres personnes touchées ; elles peuvent également être liées à des programmes de réinstallation et de réinsertion et à des services de protection sociale (voir l'annexe 1 pour plus de détails).

Agence centrale de recherches

L'Agence centrale de recherches (ACR) est un service permanent institué au sein du CICR conformément aux dispositions des quatre Conventions de Genève et de leurs Protocoles additionnels et aux Statuts du Mouvement. L'ACR – en coopération avec d'autres composantes du Mouvement – mène des activités de rétablissement des liens familiaux pendant les conflits armés et autres situations de violence, les catastrophes et d'autres circonstances qui nécessitent une intervention humanitaire. Conformément à l'Accord de Séville de 1997, à ses mesures supplémentaires adoptées en 2005 et à la Stratégie pour le Mouvement international de la Croix-Rouge et du Croissant-Rouge relative au rétablissement des liens familiaux (2008 – 2018), l'ACR exerce un rôle de chef de file au sein du Mouvement pour toutes les questions relatives au RLF ; elle coordonne les activités et intervient en tant que conseiller technique des Sociétés nationales.

Autres personnes

En dehors du demandeur et de la personne recherchée, les activités de RLF peuvent concerner d'autres personnes, telles que d'autres membres de la famille, des témoins, des voisins, des chefs de communauté, d'autres personnes recherchées, etc.

Correspondant pour la protection des données dans le cadre du RLF

On entend ici par « correspondant pour la protection des données dans le cadre du RLF » la personne ou l'unité chargée de veiller au respect du Code de conduite.

Destinataire

On entend ici par « destinataire » une personne, une autorité publique, un service ou tout autre organisme autre que la personne concernée, le responsable du traitement ou le sous-traitant, qui reçoit

communication de données personnelles.

Données personnelles

On entend ici par « données personnelles » toute information relative à une personne physique identifiée ou identifiable. Est réputée être une personne physique identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant tel qu'un nom, un support audiovisuel, un numéro, des données de localisation ou un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

Les données personnelles ne contiennent pas d'informations anonymes, c'est-à-dire des informations qui : a) ne sont pas associées à une personne physique identifiée ou identifiable ; ou b) ont été rendues anonymes de telle sorte que la personne concernée n'est pas ou n'est plus identifiable.

Étapes du traitement

Les étapes du traitement sont les principales étapes de la procédure. Les responsables du traitement inscriront et conserveront les informations relatives à chacune de ces étapes, notamment :

- la date et la source de la collecte de données ;
- dans les cas où le fondement juridique du traitement est le consentement, toute limitation au consentement exprimée par la personne concernée ;
- la date et l'objet de la demande formulée par la personne concernée aux fins de l'exercice de ses droits, et le résultat de cette demande ;
- la date et le destinataire de tout transfert de données ;
- la date et le support de publication ;
- l'analyse d'impact relative à la protection des données, s'il en a été effectué une ;
- la clôture du dossier ;
- l'archivage, s'il y a lieu.

Membres de la famille

Les personnes considérées comme étant des membres de la famille sont au moins :

- les enfants nés du mariage ou hors mariage, les enfants adoptés et les enfants du conjoint ou de la conjointe ;
- les partenaires de vie, par mariage ou non ;
- les parents (y compris les belles-mères, les beaux-pères et les parents adoptifs) ;
- les frères, sœurs, demi-frères et demi-sœurs, ou frères et sœurs adoptés ;
- les autres proches[1].

La définition figurant dans la législation nationale devrait également être prise en considération.

[1] Dans de nombreux contextes socioculturels, la famille peut désigner toutes les personnes vivant sous le même toit que les membres d'une famille ou ayant des relations étroites avec eux. La notion de famille doit par conséquent être comprise sur la base de la pratique et de la reconnaissance sociétales.

Mineurs

Tout être humain de moins de dix-huit ans, à moins que, en vertu de la législation applicable à l'enfant considéré, la majorité soit atteinte plus tôt.

Mouvement international de la Croix-Rouge et du Croissant-Rouge

Le Mouvement est un réseau humanitaire mondial qui a pour mission « de prévenir et d'alléger en toutes circonstances les souffrances des hommes ; de protéger la vie et la santé et de faire respecter la personne humaine, en particulier en temps de conflit armé et dans d'autres situations d'urgence ; d'œuvrer à la prévention des maladies et au développement de la santé et du bien-être social ; d'encourager l'aide volontaire et la disponibilité des membres du Mouvement, ainsi qu'un sentiment universel de solidarité envers tous ceux qui ont besoin de sa protection et de son assistance ».

Le Mouvement comprend le Comité international de la Croix-Rouge (CICR), les Sociétés nationales de la Croix-Rouge et du Croissant-Rouge (Sociétés nationales) et la Fédération internationale des Sociétés de la Croix-Rouge et du Croissant-Rouge (Fédération internationale).

Personne concernée

On entend ici par « personne concernée » une personne physique (c'est-à-dire un individu) qui peut être identifiée, directement ou indirectement, notamment par référence à des données personnelles.

Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens raisonnablement susceptibles d'être utilisés, soit par le responsable du traitement, soit par une autre personne, pour identifier ladite personne, directement ou indirectement. Afin d'établir si certains moyens sont raisonnablement susceptibles d'être utilisés pour identifier la personne, il faut tenir compte de tous les éléments objectifs, tels que les frais et le temps nécessaires pour l'identification, en tenant compte de la technologie disponible au moment du traitement et des progrès techniques. Par conséquent, les données personnelles ne comprennent pas les informations anonymes, qui ne sont pas associées à une personne physique identifiée ou identifiable, ni les données rendues anonymes de telle sorte que la personne concernée n'est plus identifiable. Le présent Code de conduite ne s'applique donc pas au traitement des données qui ont été rendues anonymes, notamment à des fins statistiques ou à des fins de recherche.

Lorsqu'elles utilisent des services en ligne, les personnes peuvent se voir associer des identifiants en ligne par les appareils, applications, outils et protocoles utilisés, par exemple des adresses IP ou des témoins de connexion (« cookies »). Ces identifiants peuvent laisser des traces qui, combinées aux identifiants uniques et à d'autres informations reçues par les serveurs, peuvent servir à créer des profils et à identifier les personnes. Des numéros d'identification, des données de localisation, des identifiants en ligne (par ex. des adresses IP ou des cookies) ou d'autres éléments spécifiques ne doivent pas être considérés, en soi, comme des données personnelles dès lors que ces éléments n'identifient pas une

personne ou ne permettent pas de l'identifier.

Personne vulnérable

Dans le contexte du présent Code de conduite, le terme « personne vulnérable » désigne toute personne dont la capacité de manifester sa volonté de façon libre, spécifique et éclairée est diminuée, que ce soit en raison i) des conséquences émotionnelles et psychologiques de la séparation familiale et de l'impact de la situation humanitaire, ou ii) de la complexité du traitement de données nécessaire, qui ne lui permet pas d'évaluer pleinement les risques et les avantages qu'il comporte, ou d'une combinaison des deux.

Réseau des liens familiaux

Lorsque les familles sont dispersées et que des personnes sont portées disparues en raison d'un conflit armé ou d'autres situations de violence, d'une catastrophe, de la migration ou d'autres crises humanitaires, tout ce qu'il est possible de faire doit être fait pour établir ce qu'il est advenu d'elles et où elles se trouvent, rétablir le contact entre elles et, si les circonstances le permettent, les réunir.

Les services de RLF des Sociétés nationales et le CICR forment un réseau mondial unique appelé « **Réseau des liens familiaux** ». L'Agence centrale de recherches est le conseiller technique et le coordinateur de ce Réseau des liens familiaux. La force de ce réseau humanitaire est sa capacité mondiale de mobiliser des employé-e-s et des volontaires et de travailler, selon les mêmes principes et les mêmes méthodes et à travers les frontières, dans les régions du monde touchées par des conflits armés, d'autres situations de violence, des catastrophes, la migration et d'autres crises humanitaires.

Pour de plus amples informations sur le Réseau des liens familiaux, voir le site web dédié au RLF à l'adresse : http://familylinks.icrc.org.

Responsable du traitement

On entend ici par « responsable du traitement » toute composante du Mouvement qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données personnelles.

Services de RLF

Les Sociétés nationales et les délégations du CICR à travers le monde disposent, dans leur structure, de personnel chargé de mettre au point et de réaliser des activités de RLF ainsi que des activités liées au RLF.

Sous-traitant

On entend ici par « sous-traitant » une personne, une autorité publique, un service ou tout autre

organisme qui traite des données personnelles pour le compte d'un responsable du traitement.

Traitement

On entend ici par « traitement » toute opération ou tout ensemble d'opérations effectuée-s ou non à l'aide de procédés automatisés, et appliquée-s à des données personnelles ou des ensembles de données personnelles, telle-s que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, ou l'effacement. Un transfert de données, au sein ou hors du Mouvement, constitue une opération de traitement.

Violation de données personnelles

On entend ici par « violation de données personnelles » une violation de la sécurité entraînant de manière accidentelle ou illicite la destruction, la perte, l'altération, la divulgation ou la consultation non autorisées de données personnelles transmises, conservées ou traitées d'une autre manière, ou le risque que ces situations se produisent.

1. Introduction

1.1 Objet du Code de conduite

Le présent Code de conduite énonce les principes, les engagements et les procédures minimums que le personnel du CICR, des Sociétés nationales et de la Fédération internationale chargé du RLF doit respecter lorsqu'il traite des données dans le cadre d'activités de RLF, afin de : 1) se conformer aux standards et à la législation applicables en matière de protection des données ; 2) permettre l'échange fluide de données personnelles nécessaire pour les activités de RLF et 3) protéger, dans le cadre des activités de RLF, les libertés et droits fondamentaux des demandeurs, des personnes recherchées et d'autres personnes telles que les témoins ou d'autres membres de la famille, conformément au droit international humanitaire (DIH), au droit international des droits de l'homme et à d'autres normes internationales, notamment le droit au respect de la vie privée et à la protection des données personnelles.

1.2 Portée du Code de conduite

1.2.1 Rétablissement des liens familiaux

Le présent Code de conduite s'applique aux activités de RLF et aux activités liées au RLF menées par le responsable du traitement (voir l'annexe 1).

1.2.2 Données personnelles

Le présent Code de conduite s'applique au traitement, par les responsables du traitement et dans le cadre des activités de RLF, des données personnelles (y compris des données relatives à des personnes décédées) concernant le/les demandeur-s, la/les personnes recherchée-s et d'autres personnes concernées.

1.3 Le Réseau des liens familiaux

Les Conventions de Genève de 1949, leurs Protocoles additionnels de 1977, les Statuts du Mouvement international de la Croix-Rouge et du Croissant-Rouge (les « Statuts du Mouvement ») ainsi que des résolutions du Conseil des Délégués et de la Conférence internationale de la Croix-Rouge et du Croissant-Rouge donnent aux responsables du traitement mandat de mener des activités de RLF.

Les Sociétés nationales exécutent ce mandat en tant qu'auxiliaires des pouvoirs publics de leurs pays respectifs dans le domaine humanitaire et jouent un rôle unique dans le domaine du RLF à travers le monde. Elles organisent, en liaison avec les pouvoirs publics, différents services pour venir en aide aux victimes de conflits armés, de catastrophes naturelles et d'autres situations d'urgence pour lesquelles une aide s'avère nécessaire.

1.4 Principes et lignes directrices du Mouvement

1.4.1 Principes fondamentaux

Les responsables du traitement mènent leurs activités conformément aux principes fondamentaux qui guident le Mouvement : les principes d'humanité, d'impartialité, de neutralité, d'indépendance, de volontariat, d'unité et d'universalité. Tout traitement des données personnelles effectué par les services de RLF des responsables du traitement doit être compatible avec ces principes.

1.4.2. Ne pas nuire

Les services de RLF des responsables du traitement font tout ce qui est en leur pouvoir pour éviter de nuire aux personnes concernées lors du traitement de données personnelles les concernant.

1.4.3 Confidentialité ou règles applicables en matière de divulgation

Lorsque les personnes concernées fournissent des informations aux responsables du traitement en toute confiance, ceux-ci doivent respecter la confidentialité de ces informations et en assurer la protection.

Les responsables du traitement respectent toutes les obligations légales nationales, régionales ou internationales applicables, sous réserve des restrictions énoncées dans la présente section 1.4. Aux fins de déterminer les obligations applicables, il sera tenu compte : 1) de tous privilèges et immunités ou de toute exonération d'obligations dont jouissent les responsables du traitement dans le pays ou la région en question ; et 2) de toutes protections juridiques découlant du droit international, notamment du DIH, et du mandat conféré aux responsables du traitement par les Statuts du Mouvement.

1.4.4 Lignes directrices et directives opérationnelles existantes

Le traitement de données personnelles est effectué conformément aux lignes directrices du Réseau des liens familiaux en matière de RLF, telles que *Rétablissement des liens familiaux – Guide pour les Sociétés nationales de la Croix-Rouge et du Croissant-Rouge*[2] ; *Évaluer les besoins en rétablissement des liens familiaux – Manuel à l'intention des Sociétés nationales et du CICR* ; *Rétablissement des liens familiaux dans les situations de catastrophe – Manuel pratique* ; *Lignes directrices relatives au rétablissement des liens familiaux des personnes séparées par suite de migration*[3], et conformément aux *Standards professionnels pour les activités de protection*.

[2] En cours de révision.

[3] Les documents d'orientation pertinents peuvent être consultés sur l'extranet du Réseau des liens familiaux (en cours de construction).

2. Principes de base applicables au traitement des données personnelles et engagements du responsable du traitement

2.1 Finalité déterminée

Au moment de la collecte des données, le responsable du traitement définit et indique la ou les finalités spécifique-s, explicite-s et légitime-s en vue de laquelle/desquelles les données sont traitées.

Le traitement des données est effectué essentiellement dans le but humanitaire de rétablir les liens familiaux entre les personnes séparées en raison d'un conflit armé, d'autres situations de violence, d'une catastrophe, de la migration ou d'autres situations nécessitant une intervention humanitaire.

Les données peuvent être traitées à d'autres fins que celles qui sont initialement spécifiées lors de la collecte si ce traitement ultérieur s'avère nécessaire pour réaliser un objectif humanitaire compatible, comme des activités liées au RLF, et respecte en tout temps l'ensemble des lois applicables en matière de protection des données (pour plus de détails, voir l'annexe 1).

2.2 Traitement licite et loyal

Le traitement des données personnelles par le responsable du traitement se fonde sur un ou plusieurs des éléments suivants :

- le consentement de la personne concernée ;
- l'intérêt vital de la personne concernée ou d'autres personnes ;
- l'intérêt public ;
- l'intérêt légitime poursuivi par le responsable du traitement ;
- le respect d'une obligation légale.

2.2.1 Consentement de la personne concernée

Le consentement, l'option à privilégier : le consentement de la personne concernée est le meilleur fondement sur lequel puisse reposer le traitement de données personnelles. Il doit être donné sans équivoque, sous toute forme appropriée permettant une manifestation de volonté libre, spécifique et éclairée consistant soit en une déclaration écrite, orale ou autre, soit en un acte positif clair de la personne concernée – déclaration ou acte par lequel elle indique accepter que des données personnelles la concernant fassent l'objet d'un traitement. Le consentement donné vaut pour toutes les opérations de traitement effectuées dans le même but. La personne concernée doit recevoir les informations suivantes, formulées en termes simples :

- l'identité et les coordonnées du responsable du traitement ;
- la finalité du traitement auquel sont destinées les données personnelles la concernant, et des informations sur les risques éventuels et les avantages ;
- le fait que le responsable du traitement pourrait traiter les données personnelles la concernant à d'autres fins que celles qui sont initialement spécifiées lors de la collecte, pour autant que ce traitement soit compatible avec la finalité déterminée mentionnée plus haut ;

- les circonstances dans lesquelles il pourrait se révéler impossible de traiter de manière confidentielle les données personnelles la concernant;
- le droit de la personne concernée d'accéder aux données personnelles la concernant, d'en demander la rectification ou l'effacement et de s'opposer ultérieurement à leur traitement, ainsi que les limitations y afférentes ;
- une indication des mesures de sécurité mises en œuvre par le responsable du traitement pour le traitement des données ;
- le fait que le responsable du traitement pourrait devoir transférer les données vers un autre pays ; et
- une description de la politique appliquée par le responsable du traitement en matière de conservation des données (la durée pendant laquelle les données sont conservées et les dispositions prises pour s'assurer qu'elles sont exactes et à jour) ;

et il doit lui être demandé

- si les données personnelles la concernant peuvent être communiquées à d'autres organisations (notamment à d'autres composantes du Mouvement), aux pouvoirs publics du pays dans lequel les données sont collectées ou d'un autre pays, ou rendues publiques, et si elle approuve une telle utilisation des données personnelles la concernant.

Le consentement peut être donné avec des limitations. Les informations relatives au consentement donné, au niveau de confidentialité nécessaire et à toute limitation applicable sont inscrites et conservées, et accompagnent les données personnelles tout au long du traitement.

Autres possibilités que le consentement – en particulier lorsque le consentement ne peut pas être obtenu/raisonnablement obtenu, le traitement des données personnelles sera fondé sur l'un des motifs suivants :

- l'intérêt vital ;
- l'intérêt public ;
- l'intérêt légitime poursuivi par le responsable du traitement ;
- le respect d'une obligation légale.

En pareil cas, le responsable du traitement s'assurera, dans la mesure du possible, que la personne concernée a connaissance du traitement et qu'elle est en mesure s'y opposer si elle le souhaite.

2.2.2 Intérêt vital

Le traitement de données personnelles par les services de RLF du responsable du traitement en vue de rétablir les liens familiaux, d'élucider le sort de personnes disparues et de déterminer où elles se trouvent, ainsi que de fournir une assistance et une protection d'urgence, est présumé relever de l'intérêt vital d'une

personne concernée ou d'autres personnes dans certaines circonstances, notamment :

- lorsque la personne concernée est recherchée par des membres de sa famille, portée disparue, privée de liberté, victime de mauvais traitements, ou pourrait être décédée ;
- lorsque la personne concernée est particulièrement vulnérable et/ou n'est pas en mesure de donner un consentement libre et éclairé, ni d'anticiper ou de comprendre les risques et les avantages du traitement des données personnelles la concernant.

2.2.3 Intérêt public

Les activités de RLF et activités liées au RLF menées par le responsable du traitement sont d'intérêt public, étant donné leur finalité exclusivement humanitaire, comme indiqué à la section 1.3 ci-dessus (pour des exemples, voir l'annexe 2).

2.2.4 Intérêt légitime

Le traitement de données personnelles intervient aussi dans des circonstances dans lesquelles il est dans l'intérêt légitime du responsable du traitement de procéder à ce traitement, à moins que les intérêts ou les libertés et droits fondamentaux de la personne concernée ne prévalent (pour des exemples, voir l'annexe 3).

2.2.5 Respect d'une obligation légale

Le responsable du traitement procédera également au traitement de données personnelles pour respecter une obligation légale, telle que le respect de la législation nationale et régionale et des décisions de justice, sous réserve des Principes fondamentaux du Mouvement. Les obligations légales peuvent varier d'un pays et d'une situation à l'autre.

2.3 Engagements concernant le traitement des données personnelles

2.3.1 Obligations et responsabilités

Le responsable du traitement doit veiller à ce que toute personne ou entité ayant accès à des données personnelles et agissant sur ses instructions (de ce fait un sous-traitant) ne traite ces données personnelles que conformément aux prescriptions du présent Code de conduite. Il doit s'assurer également que les obligations qui incombent à chaque entité intervenant dans le traitement de données personnelles sont clairement définies et énoncées dans des clauses contractuelles appropriées. Voir la section 4 ci-dessous pour de plus amples renseignements sur le transfert de données à des tiers dans les cas où le tiers qui reçoit les données ne les traite pas strictement selon les instructions données par le responsable du traitement.

2.3.2 Traitement de données adéquates, pertinentes et à jour

Caractère adéquat des données – les données personnelles traitées par les services de RLF du responsable du traitement seront examinées périodiquement dans le but de s'assurer qu'elles sont adéquates, pertinentes et limitées au minimum nécessaire au regard des finalités pour lesquelles elles sont collectées et traitées, sauf lorsqu'elles sont traitées à des fins d'archivage.

Exactitude des données – les données personnelles doivent être suffisamment exactes, complètes et à jour au regard des finalités pour lesquelles elles sont collectées et traitées.

2.3.3 Protection des données dès la conception (by design ») et par défaut

Il conviendra de prendre des mesures techniques et organisationnelles appropriées pour se conformer aux prescriptions du présent Code de conduite lors de la conception des systèmes de gestion de données et de l'établissement des procédures applicables à la collecte de données personnelles.

2.3.4 Analyse d'impact relative à la protection des données (DPIA)

Lorsque le traitement est susceptible de présenter des risques particuliers pour les droits et libertés des personnes concernées, notamment dans le cadre de transferts, de la publication et de la divulgation de données, le responsable du traitement effectuera, dans la mesure du possible, une analyse d'impact relative à la protection des données (en anglais, *Data protection Impact Assessment* – DPIA) avant le traitement, en consultation avec la personne concernée et les autres parties prenantes, afin de déterminer et d'évaluer, notamment :

- les avantages du traitement des données ;
- l'origine, la nature, la probabilité et la gravité des risques ;
- les mesures qu'il convient de prendre pour démontrer que ces risques sont réduits au minimum et que le traitement des données personnelles respecte le présent Code de conduite et toute législation applicable.

Le résultat d'une analyse d'impact relative à la protection des données devrait être de réduire au minimum le risque de préjudice ou d'atteinte possible aux droits et libertés de la personne concernée. Le responsable du traitement inscrira ce résultat et les raisons pour lesquelles il a été obtenu, et conservera cette information. Il s'assurera également que les mesures prises à l'issue de la DPIA sont correctement appliquées et produisent l'effet escompté.

2.3.5 Tenue d'un registre des opérations de traitement

Le responsable du traitement doit veiller à ce qu'un registre électronique ou sur support papier soit tenu, où figurent : i) les bases de données dans lesquelles il traite des données personnelles, et ii) les principales étapes du traitement des données. Mention de ces étapes sera inscrite et conservée dans le fichier de la base de données/le dossier individuel de la personne concernée.

2.3.6 Conservation des données

Lorsqu'elles ne seront plus nécessaires au regard des finalités pour lesquelles elles ont été collectées, pour un traitement ultérieur ou pour un traitement reposant sur un autre fondement légitime/licite, les données personnelles seront archivées ou effacées conformément à la politique relative à la conservation des données pour les services de RLF établie par le responsable du traitement (voir aussi la section 3.3).

2.3.7 Sécurité des données

Des mesures de sécurité techniques, matérielles et organisationnelles raisonnables seront prises de façon systématique à toute étape du traitement de données personnelles en vue d'empêcher la perte, le vol, ou l'accès ou la divulgation non autorisés ou illicites. L'accès aux données personnelles est limité aux membres du personnel du responsable du traitement qui en ont besoin pour fournir un service spécifique ou exécuter une tâche particulière, et il est assorti de garanties et de limitations d'accès (pour plus de détails, voir l'annexe 4).

2.3.8 Violation de données personnelles

Le responsable du traitement doit avertir la personne concernée qu'une violation des données personnelles la concernant s'est produite lorsque cette violation est susceptible de porter atteinte aux droits et libertés de cette personne.

La notification à la personne concernée d'une violation de ses données personnelles vise à réduire au minimum le risque que cette violation lui porte préjudice.

Le responsable du traitement peut décider qu'il n'est pas nécessaire de communiquer une violation de données personnelles à la personne concernée si l'une ou plusieurs des conditions suivantes est/sont remplie-s :

- le responsable du traitement a mis en œuvre des mesures de sécurité organisationnelles, techniques ou matérielles appropriées, et ces mesures ont été appliquées aux données affectées par la violation des données personnelles ;
- le responsable du traitement a pris des mesures ultérieures qui garantissent que la violation de données n'est plus susceptible de porter gravement atteinte aux droits et libertés de la personne concernée ;
- cette communication exigerait des efforts disproportionnés, notamment en raison des conditions logistiques ou de sécurité ou du nombre de cas concernés. Dans de telles circonstances, le responsable du traitement déterminera s'il convient plutôt de faire une communication publique ou de prendre une mesure similaire qui permettrait aux personnes concernées d'être informées de manière tout aussi efficace ;
- cela porterait atteinte à un intérêt public important, notamment à la viabilité des opérations effectuées par le responsable du traitement ;
- en raison des conditions de sécurité qui prévalent, le fait de contacter la personne concernée pourrait mettre en danger cette personne elle-même.

3. Droits des personnes concernées

3.1 Information et accès

Au moment de la collecte de données personnelles, ou dès que possible par la suite, le responsable du traitement fournira à la personne concernée, sous réserve de contraintes logistiques et de sécurité, des informations sur le traitement des données personnelles la concernant, oralement ou par écrit, par le moyen le plus approprié (pour une liste des informations à fournir, voir l'annexe 5).

Les personnes concernées ont le droit d'obtenir à tout moment, sur demande, confirmation que des données personnelles les concernant font ou non l'objet d'un traitement. Lorsque des données personnelles les concernant font effectivement l'objet d'un traitement, ces personnes ont un droit d'accès à leurs données et à des informations sur la finalité du traitement, les destinataires des données personnelles et les garanties adoptées.

Sur demande, une copie du ou des documents qui contiennent les données personnelles les concernant leur est fournie.

Cette section ne s'applique pas lorsque l'accès aux données doit être limité :

- pour un motif d'intérêt public impérieux ;
- afin de sauvegarder les intérêts en matière de protection des données et les droits et libertés d'autrui ;
- parce que les documents concernés ne peuvent pas être expurgés de manière à satisfaire à la demande.

Le responsable du traitement tiendra un registre des demandes d'accès et de l'issue de ces demandes, y compris les catégories de données personnelles communiquées et/ou le refus d'accès aux données.

3.2 Communication à des membres de la famille et à des représentants légaux

Une demande de communication de données personnelles émanant d'un membre de la famille ou d'un représentant légal d'un enfant ou d'une autre personne concernée qui est dans l'incapacité de donner son consentement est présumée être dans l'intérêt supérieur de cette personne. Il y sera donc fait droit, à moins qu'il n'y ait des raisons suffisantes de penser qu'il doive en être autrement. Il convient de consulter la personne concernée, dans la mesure du possible, afin de déterminer si elle s'oppose à cette communication.

3.3 Rectification et effacement

Rectification – Le responsable du traitement répondra aux demandes de rectification de données personnelles, en particulier lorsque les données sont inexactes ou incomplètes. Il communiquera les

rectifications effectuées aux destinataires des données personnelles, à moins que la rectification ne soit pas importante ou que la communication exige des efforts disproportionnés.

Effacement – Une personne concernée a le droit de faire effacer les données personnelles la concernant des bases de données actives du responsable du traitement dans l'un quelconque des cas suivants :

- ces données ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou ne sont plus nécessaires en vue d'un traitement ultérieur ;
- la personne concernée a retiré son consentement au traitement des données personnelles la concernant, et il n'existe pas d'autre fondement juridique à ce traitement ;
- la personne concernée a fait valoir avec succès son opposition au traitement des données personnelles la concernant ;
- le traitement des données personnelles de la personne concernée n'est pas, à d'autres égards, conforme au présent Code de conduite.

La conservation des données personnelles d'une personne concernée au-delà de la durée initialement prévue est toutefois autorisée lorsqu'elle est nécessaire ou justifiée :

- à des fins historiques, statistiques ou scientifiques, notamment afin de conserver une trace écrite des mesures prises par un responsable du traitement dans l'accomplissement de son mandat au titre des Conventions de Genève de 1949, des Protocoles additionnels aux Conventions de 1977 ou des Statuts du Mouvement ;
- pour des motifs d'intérêt public dans le domaine de la santé publique ; ou
- en vue de la publication par toute personne de toute production journalistique, artistique ou littéraire, aux fins de l'exercice du droit à la liberté d'expression et d'information.

En outre, la conservation des données personnelles d'une personne concernée au-delà de la durée initialement prévue sera autorisée dans les cas prévus par la loi. Une personne concernée sera avertie de la décision prise au sujet de sa demande, et mention de cette décision sera inscrite et conservée par le responsable du traitement.

Le responsable du traitement se réserve le droit de rejeter une demande de rectification ou d'effacement émanant de la personne concernée s'il estime que cette demande pourrait avoir été faite sous une pression indue et/ou que l'effacement porterait atteinte à la sauvegarde des intérêts vitaux de la personne concernée.

Le responsable du traitement informera les destinataires de la suppression des données personnelles et leur demandera d'effacer tous les liens vers ces données et toute copie de celles-ci, à moins que les données effacées ne soient pas importantes ou que la communication exige des efforts

disproportionnés.

3.4 Opposition au traitement

Une personne concernée a le droit de s'opposer, pour des raisons tenant à sa situation particulière, à ce que des données personnelles la concernant fassent l'objet d'un traitement ayant pour fondement la réalisation d'intérêts légitimes du responsable du traitement ou l'intérêt public. Si une demande d'opposition est acceptée, les données personnelles concernées ne seront plus traitées, à moins que le responsable du traitement ne démontre que la poursuite du traitement s'impose pour des raisons légitimes impérieuses.

Si l'opposition est acceptée, le responsable du traitement communiquera cette opposition aux destinataires des données, à moins que cela n'exige des efforts disproportionnés.

3.5 Recours

Une personne concernée adresse sa demande au responsable du traitement, qui répond dans un délai raisonnable et en tout état de cause dans tout délai imposé par la loi.

Le personnel qui reçoit une demande d'une personne concernée pourra soit :

- accepter la demande et informer la personne de la suite qui a été ou sera donnée à sa demande ; ou
- faire savoir à la personne concernée pourquoi il ne pourra pas être ou ne sera pas donné suite à sa demande, et
- l'informer de la possibilité d'introduire une réclamation auprès du responsable du traitement.

4. Dispositions spéciales relatives aux transferts de données

4.1 Principes généraux

4.1.1 Contexte

Les activités de RLF et activités liées au RLF nécessitent souvent un transfert transfrontalier de données personnelles entre responsables du traitement.

Les services de RLF d'un responsable du traitement peuvent également avoir besoin de transférer des données personnelles à des entités telles que des organisations non gouvernementales (ONG), des organisations internationales, des autorités et d'autres tiers pour mener leurs activités de RLF et activités liées au RLF.

Ces transferts s'inscrivent dans le cadre des activités du Réseau des liens familiaux, décrites dans la section 1.3 ; à ce titre, ils sont effectués pour des motifs importants d'intérêt public et conformément aux principes et lignes directrices du Mouvement énoncés dans la section 1.4.

En outre, dans la plupart des cas, ils se feront sur la base du consentement et/ou en vue de sauvegarder les intérêts vitaux de la personne concernée ou d'autrui.

4.1.2 Principes généraux applicables aux transferts de données

Un transfert de données, que ce soit au sein du Mouvement ou en dehors, constitue un traitement. À ce titre, il est soumis aux principes de base énoncés dans le chapitre 2 et aux droits des personnes concernées énoncés dans le chapitre 3. Les transferts constituant toutefois une opération de traitement particulièrement délicate, certaines exigences en la matière sont d'autant plus importantes, telles que la réalisation d'une DPIA, les informations à fournir à la personne concernée et la sécurité des données. Comme indiqué dans la section 3.1 ci-dessus, le transfert à tout tiers raisonnablement prévisible est envisagé avant ou au moment de la collecte des données, et le consentement de la personne concernée au transfert de ses données personnelles est recueilli si cela s'avère possible.

Les données personnelles ne doivent être transférées à des personnes ou des organisations que si des garanties appropriées et proportionnées sont mises en place, en tenant compte du niveau de confidentialité des données, de l'urgence de l'action humanitaire et des contraintes logistiques et de sécurité, comme précisé dans le présent Code de conduite.

4.1.3 Analyse d'impact relative à la protection des données dans le cadre des transferts de données (DPIA)

L'obligation de réaliser une analyse d'impact relative à la protection des données est particulièrement importante dans le cadre des transferts de données. Par conséquent, lorsqu'un transfert de données est susceptible de présenter des risques particuliers pour les droits et libertés des personnes concernées, le responsable du traitement réalisera au préalable une DPIA (voir l'annexe 6 pour des éléments d'orientation), comme spécifié dans la section 2.3.4 ci-dessus.

4.1.4 Conditions

Les transferts de données doivent satisfaire à l'ensemble des conditions suivantes :

- le traitement par le destinataire est strictement limité aux finalités prévues des activités de RLF et activités liées au RLF, et à d'autres fins compatibles ;
- la quantité et le type de données personnelles sont strictement limités aux besoins du destinataire pour les finalités déterminées ou le traitement ultérieur prévu ;
- le transfert est compatible avec les attentes raisonnables de la personne concernée.

4.1.5 Tenue d'un registre des transferts de données

Le responsable du traitement s'assure qu'il est tenu un registre électronique/sur support papier des transferts (voir aussi la section 2.3.5).

Ce registre doit comprendre les informations suivantes concernant les transferts :

- le nom du destinataire ;

- la finalité prévue du transfert ;
- la date du transfert ;
- une description des catégories de données personnelles qui ont été transférées ;
- toutes limitations à l'utilisation des données acceptées par le destinataire.

4.1.6 Accords

Comme indiqué dans la section 4.1.2, un transfert de données personnelles peut avoir lieu si le responsable du traitement est convaincu de l'existence de garanties appropriées visant à assurer la protection des données personnelles par le destinataire. Des garanties appropriées peuvent être établies dans le cadre des accords relatifs au traitement des données personnelles qui sont conclus, dans la mesure du possible, avec des tiers extérieurs au Mouvement chaque fois que des transferts réguliers de données sont envisagés.

Même lorsque des accords ont été conclus, il se peut que le transfert de certaines catégories de données ne soit pas jugé approprié.

4.2 Méthodes de transmission

En cas de transfert, des mesures appropriées seront prises pour protéger la transmission de données personnelles à des tiers. Le niveau de sécurité défini et la méthode de transmission seront proportionnés à la nature et au caractère plus ou moins sensible des données personnelles, ainsi qu'aux risques mis en évidence par la DPIA.

5. Dispositions spéciales relatives à la publication de données

5.1 Principes généraux

La publication de données personnelles par le responsable du traitement constitue une opération de traitement. À ce titre, elle est soumise aux Principes généraux énoncés dans le chapitre 2 et aux droits des personnes concernées énoncés dans le chapitre 3. La publication constitue toutefois une opération de traitement particulièrement délicate. Une fois les données publiées, le responsable du traitement et la personne concernée n'ont plus, dans une large mesure, la possibilité de maîtriser la façon dont les données personnelles sont traitées. Il conviendra par conséquent d'appliquer les principes supplémentaires énoncés dans ce chapitre.

Sous réserve du résultat de la DPIA et des obligations légales applicables, les services de RLF du responsable du traitement peuvent publier des données personnelles en vue de rétablir les liens familiaux entre les personnes séparées par des conflits armés, d'autres situations de violence, des catastrophes naturelles et la migration. Ces données peuvent comprendre des noms, des photographies, des indications telles que « vivant et en bonne santé », « blessé », « décédé », « porté

disparu » ou « déplacé », et peuvent être publiées en ligne, dans les médias, sur des affiches, dans des brochures ou tout autre outil approprié.

Conformément à la section 2.2.1, le consentement de la personne concernée est le fondement à privilégier pour la publication de données personnelles.

5.2 Analyse d'impact relative à la protection des données dans le cadre de la publication de données

L'obligation de réaliser une DPIA, énoncée dans la section 2.3.4 ci-dessus et l'annexe 6, est particulièrement importante dans le contexte de la publication de données.

Outre les éléments précisés dans la section 2.3.4 ci-dessus, « Analyse d'impact relative la protection des données », dans le contexte de la publication de données la DPIA tiendra compte des éléments suivants :

- les dispositions législatives et règlementaires nationales en matière de protection des données qui s'appliquent à la publication de données ;
- les conditions de sécurité, le respect des droits de l'homme et du DIH, et la sécurité des personnes concernées dans un pays donné ;
- la question de savoir si des données anonymes/agrégées suffiraient ou s'il est nécessaire de publier les données personnelles, et la question de savoir si d'autres moyens de protéger l'identité des personnes concernées serviront la finalité visée par la publication (par exemple, ne pas associer une photographie à des noms/des signes distinctifs/ des lieux précis) ;
- la méthode et les conditions de publication ;
- la possibilité d'imposer l'obligation de limiter toute utilisation ultérieure à l'égard de tiers qui souhaiteraient utiliser les données publiées ;
- la possibilité de préciser la période pendant laquelle certaines données peuvent rester publiées sur un support médiatique particulier, et la méthode de destruction lorsque la finalité visée par la publication a été atteinte ;
- l'utilité et la pertinence des publications, déterminées au moyen d'évaluations périodiques effectuées par le responsable du traitement ;
- dans le contexte de la communication publique, l'importance de protéger les personnes vulnérables de la curiosité du public.

Si la personne concernée est une personne vulnérable, des considérations supplémentaires seront prises en compte s'il y a lieu, notamment des mesures additionnelles visant à protéger la confidentialité et l'anonymat. Le principe directeur de la protection des victimes est de « ne pas nuire » et d'agir dans l'intérêt supérieur des personnes concernées qui sont vulnérables.

5.3 Tenue d'un registre de la publication de données

Le responsable du traitement doit veiller à ce qu'il soit tenu un registre des publications effectuées.

Ce registre doit comprendre toutes les informations suivantes :

- la date de la publication ;
- le cas échéant, la date à laquelle le motif sur lequel se fonde la publication doit être examiné, conformément à la DPIA ;
- le cas échéant, la date à laquelle les données doivent être retirées de la publication ;
- une description des catégories de données personnelles qui ont été publiées ;
- dans la mesure du possible, des informations sur le support médiatique utilisé.

5.4 Données à publier pour le RLF

Les données qui peuvent être publiées doivent être définies pour chaque contexte donné, et des directives plus spécifiques peuvent exister pour certaines catégories de personnes concernées. Sur la base de la DPIA réalisée, des mesures d'atténuation particulières seront mises en œuvre, par exemple :

- la publication est limitée aux données strictement nécessaires pour permettre au lecteur/à l'auditeur d'identifier les personnes dont le nom/la photographie est publié-e et de rétablir le contact ;
- les photographies de personnes vulnérables ne sont pas publiées en association avec d'autres données personnelles (par ex. le nom), et l'adresse d'un mineur n'est jamais publiée.

5.5 Données à publier pour les archives publiques

Les données personnelles qui ont été archivées peuvent être rendues publiques conformément à la législation applicable.

5.6 Données à publier pour la communication publique

Les données personnelles peuvent être publiées à des fins de promotion des activités de RLF et/ou de sensibilisation à des situations préoccupantes, conformément à la législation applicable. La communication publique est aussi liée à la liberté d'information et d'expression et à la responsabilité envers le public. Toutefois, comme pour toute publication, les principes énoncés dans le présent Code de conduite seront appliqués et une DPIA sera réalisée.

5.7 Droit de retirer son consentement/de demander la suppression de données publiées

Lorsque la publication se fonde sur le consentement, une personne concernée peut à tout moment retirer son consentement à la publication de données permettant de l'identifier. En pareil cas, le responsable du traitement prend toutes les mesures raisonnables, compte tenu des difficultés inhérentes à la suppression de documents publics (en particulier en ligne), pour supprimer les données publiées et/ou empêcher leur publication.

Lorsque la publication repose sur un fondement autre que le consentement, il conviendra d'appliquer

les procédures énoncées dans la section 3.4 « Opposition au traitement ».

6. Application du Code de conduite

Un groupe chargé de l'application du Code de conduite soutiendra l'application du Code au niveau mondial en promouvant l'apprentissage et le développement continus.

Le présent Code de conduite doit être appliqué de manière effective par tous les responsables du traitement, dans le respect des dispositions de la législation nationale, comme indiqué ci-après :

- il est tenu compte du Code de conduite dans les politiques, lignes directrices et programmes de RLF ;
- le Code de conduite devient partie intégrante de la gestion et de la formation du personnel chargé du RLF pour chaque responsable du traitement ;
- un correspondant pour la protection des données dans le cadre du RLF est désigné et ses coordonnées sont communiquées ;
- les responsables du traitement participent à des enquêtes périodiques sur l'application du Code de conduite ;
- les responsables du traitement coopèrent avec le Groupe chargé de l'application du Code de conduite ;
- le suivi de l'application – qui implique autocontrôle, dialogue, examen par les pairs et autres formes d'examen – se fait sur une base volontaire en vue d'assurer une amélioration et un apprentissage organisationnel continus.

Le Groupe chargé de l'application du Code de conduite révisera et tiendra à jour ce Code selon que de besoin.

7. Références

7.1 Instruments juridiques/documents d'orientation

- Principes directeurs des Nations Unies pour la réglementation des fichiers informatisés contenant des données à caractère personnel, tels qu'adoptés par la résolution 45/95 de l'Assemblée générale de l'ONU du 14 décembre 1990 ;

- article 17 du Pacte international relatif aux droits civils et politiques ;

- International Standards on the protection of personal data and privacy, by the International Conference of Data Protection and Privacy Commissioners, 5 November 2009 (Standards internationaux en matière de protection de la vie privée et des données personnelles, Conférence internationale des commissaires à la protection des données

personnelles et de la vie privée, 5 novembre 2009) http://privacyconference2011.org/htmls/adoptedResolutions/2009_Madrid/2009_M1.pdf ;

- Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Conseil de l'Europe, (STE n° 108), 28 janvier 1981 ;
- Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, 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, *JO* L 281, 23 novembre 1995, p. 31 à 50 ;
- article 8 de la Convention européenne pour la sauvegarde des droits de l'homme et des libertés fondamentales, 4 novembre 1950 ;
- article 16 du Traité sur le fonctionnement de l'Union européenne (TFUE), 13 décembre 2007, *JO* C 326, 26 octobre 2012, p. 0001 à 0390 ;
- articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne, *JO* C 303/1, 14 décembre 2007 ;
- Organisation pour la coopération et le développement économiques (OCDE), Lignes directrices de l'OCDE régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel de 1980 (mise à jour de 2013), http://www.oecd.org/sti/ieconomy/privacy-guidelines.htm ;
- Lignes directrices de l'OCDE régissant la protection des consommateurs dans le contexte du commerce électronique, 9 décembre 1999, www.oecd.org/sti/consumer/34023811.pdf ;
- Cadre de protection de la vie privée de l'Association de coopération économique Asie-Pacifique (APEC), 2005, http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx
- Statuts du Mouvement international de la Croix-Rouge et du Croissant-Rouge, tels que modifiés en 2006 ;
- Résolution 4 du Conseil des Délégués sur la Stratégie pour le Mouvement international de la Croix-Rouge et du Croissant-Rouge relative au rétablissement des liens familiaux, 24 novembre 2007 ;
- Conférence internationale des commissaires à la protection des données personnelles et de la vie privée, résolution sur la protection des données personnelles et l'action

humanitaire internationale, Amsterdam (Pays-Bas), 2015, https://icdppc.org/wp-content/uploads/2015/02/FR-1.pdf

7.2 Doctrine

- COMITÉ INTERNATIONAL DE LA CROIX-ROUGE (CICR), *Rétablissement des liens familiaux dans les situations de catastrophe – Manuel pratique,* CICR, Genève, 2010, 215 p. ;
- COMITÉ INTERNATIONAL DE LA CROIX-ROUGE (CICR), *Évaluer les besoins en rétablissement des liens familiaux – Manuel à l'intention des Sociétés Nationales et du CICR*, CICR, Genève, 2010, 112 p. ;
- COMITÉ INTERNATIONAL DE LA CROIX-ROUGE (CICR), *Lignes directrices relatives au rétablissement des liens familiaux des personnes séparées par suite de migration* – Document à usage interne pour le Mouvement international de la Croix-Rouge et du Croissant-Rouge, CICR, Genève, 2010, 63 p. ;
- COMITÉ INTERNATIONAL DE LA CROIX-ROUGE (CICR), *Stratégie de rétablissement des liens familiaux, y compris références juridiques,* CICR, Genève, 2009, 72 p. ;
- MORGAN, O., M. TIDBALL-BINZ, et D. VAN ALPHEN, D. (directeurs de publication), *Management of dead bodies after disasters: A field manual for first responders*, Washington D.C., 2009, 53

ANNEXES

Annexe 1 – Activités de RLF et activités liées au RLF

Selon la situation et le contexte, les activités de RLF peuvent être de différents types :

- l'organisation des échanges de nouvelles familiales ;
- les recherches de personnes ;
- l'enregistrement et le suivi des personnes (enfants ou adultes) afin de prévenir leur disparition et de pouvoir informer leurs familles ;
- le regroupement familial et le rapatriement ;
- la collecte, la gestion et la transmission d'informations relatives aux personnes décédées ;
- la transmission de documents officiels, tels que des certificats de naissance, des papiers d'identité ou divers autres certificats émis par les autorités ;
- la délivrance d'attestations de détention individuelle et de documents attestant d'autres situations qui ont mené à l'enregistrement individuel ;
- l'émission de documents de voyage du CICR ;
- le suivi de l'intégration des personnes réunies avec des membres de leur famille ;
- la promotion et le soutien de l'établissement de mécanismes permettant de faire la lumière sur le sort des personnes disparues et de déterminer où elles se trouvent.

Voir aussi : http://familylinks.icrc.org

Les activités liées au RLF – d'autres services humanitaires en lien avec les activités de RLF sont mises en œuvre par le personnel chargé du RLF :

- le soutien matériel, juridique, psychologique et psychosocial aux familles de personnes disparues et aux autres personnes touchées par des conflits armés ou d'autres situations de violence, des catastrophes, la migration et d'autres crises humanitaires ;
- le soutien aux autorités compétentes pour la gestion des restes humains et l'identification médico-légale ;
- (l'orientation vers) des services de protection sociale ;
- des services de réinstallation ou (l'orientation vers) des services d'aide à la réinsertion pour les groupes vulnérables ;
- l'archivage (mémoire individuelle/familiale ; mémoire de l'humanité ; besoins administratifs individuels, responsabilité des parties, recherche historique, statistique et médicale) ;
- la communication publique pour la promotion des activités de RLF et liées au RLF.

Annexe 2 – Intérêt public

Exemples de motifs d'intérêt public :

- face à des crises de grande ampleur nécessitant une action immédiate et ne permettant pas d'agir sur la base du consentement, et lorsqu'il n'est pas possible d'établir clairement si le fondement légitime de l'intérêt vital s'applique. Par exemple, dans des situations où un grand nombre de migrants sont sauvés en mer ;
- lorsque les opérations de traitement sont très complexes et nécessitent l'intervention de différents sous-traitants externes et le recours à des technologies complexes, de sorte qu'il est difficile pour les personnes concernées de se rendre pleinement compte des risques et des avantages des différentes opérations et de prendre une décision en toute connaissance de cause sur cette base. Si l'intérêt vital de la personne concernée ou de toute autre personne ne peut pas être établi (soit parce que l'on n'est pas dans une situation d'urgence, soit parce que la personne concernée est recherchée), le traitement peut se fonder sur le mandat dont a été investi le responsable du traitement, à condition qu'une DPIA ait été réalisée et ait donné un résultat satisfaisant ;
- des distributions d'assistance, lorsque les circonstances ne permettent pas de recueillir le consentement de tous les bénéficiaires potentiels, et lorsque la vie et l'intégrité de la personne concernée ou d'autrui ne sont raisonnablement pas susceptibles d'être menacés (auquel cas l'« intérêt vital » peut être le fondement le plus approprié pour justifier le traitement) ;
- le traitement des données personnelles de personnes concernées qui se trouvent en détention. Cela peut se produire, par exemple, lorsqu'il faut traiter les données personnelles de personnes privées de liberté dans le contexte d'un conflit armé ou d'une autre situation de violence alors que le CICR (ou la Société nationale) n'a pas encore pu visiter ces personnes et recueillir leur consentement, et que les conditions de détention, en l'occurrence, ne permettraient pas de se fonder sur la base juridique de l'« intérêt vital ».

Annexe 3 Intérêt légitime

Exemples de traitement fondé sur l'intérêt légitime :

- traitement nécessaire pour permettre au responsable du traitement de s'acquitter efficacement de son mandat conformément aux Principes fondamentaux (notamment les principes de neutralité, d'indépendance et d'impartialité) et à ses modalités de travail habituelles ;
- traitement de données effectué dans la mesure strictement nécessaire pour garantir la sécurité des systèmes d'information et des informations, ainsi que la sécurité des services connexes offerts ou rendus accessibles via ces systèmes d'information, par des autorités publiques, des équipes d'intervention en cas d'urgence informatique (CERT), des équipes d'intervention en cas d'incidents de sécurité informatique (CSIRT), des fournisseurs de réseaux ou de services de communications électroniques, et des fournisseurs de technologies et services de sécurité. Il pourrait s'agir, par exemple, d'empêcher l'accès non autorisé à des réseaux de communications électroniques et la diffusion de codes malveillants, et de faire cesser des attaques par « déni de service » et des dommages touchant les systèmes de communication informatiques et électroniques ;
- traitement de données personnelles effectué dans la mesure strictement nécessaire pour prévenir, prouver et faire cesser le vol ou la fraude ;
- traitement de données personnelles visant à les rendre anonymes ou à les pseudonymiser ;
- traitement nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice, que ce soit dans le cadre d'une procédure judiciaire, administrative ou extrajudiciaire, ou à des fins de prospection (marketing direct) ou de communication publique.

Annexe 4 – Sécurité des données

Les données personnelles devraient être traitées de manière à garantir une sécurité appropriée, notamment afin de prévenir tout accès non autorisé à ces données et à l'équipement utilisé pour leur traitement ainsi que toute utilisation non autorisée de ces données et de cet équipement.

Toute personne agissant sous l'autorité du responsable du traitement et ayant accès à des données personnelles ne pourra traiter ces données qu'en conformité avec Code de conduite et la politique de sécurité des données applicable, comme spécifié dans la présente annexe.

Afin de préserver la sécurité et de prévenir tout traitement effectué en violation du présent Code de conduite, le responsable du traitement évaluera les risques particuliers inhérents au traitement et mettra en œuvre des mesures visant à les atténuer. Ces mesures devraient assurer un niveau de sécurité approprié (compte tenu des technologies disponibles, des conditions logistiques et de sécurité et du coût de mise en œuvre de ces mesures) au regard des risques que présente le traitement et de la nature des données personnelles à protéger. Il s'agit notamment de mesures concernant :

- la formation ;
- la gestion des droits d'accès à des bases de données qui contiennent des données personnelles ;
- la sécurité physique des bases de données ;
- la sécurité informatique ;
- les clauses de discrétion ;
- les méthodes de destruction des données personnelles ;

ainsi que de toute autre mesure appropriée.

Ces mesures ont pour objectif de garantir que les données personnelles seront conservées en toute sécurité, à la fois sur le plan technique et organisationnel, et qu'elles seront protégées par des mesures raisonnables et appropriées contre toute modification ou reproduction non autorisée, ainsi que contre la falsification, la destruction illicite, la perte accidentelle, la divulgation ou le transfert non autorisés.

Les mesures relatives à la sécurité des données seront fonction, entre autres :

- du type d'opération de traitement ;
- de la nature et du caractère plus ou moins sensible des données personnelles concernées ;
- de la forme ou du format de stockage ;
- de l'environnement/emplacement de ces données personnelles ; et
- des conditions logistiques et de sécurité qui règnent.

Les dispositifs de sécurité des données devraient être réévalués et mis à jour régulièrement afin d'assurer un niveau de protection adapté au niveau de sensibilité attribué aux données personnelles.

Le responsable du traitement est chargé de coordonner les activités suivantes :

- la mise en place d'un système de gestion de la sécurité de l'information. À cet effet, il doit établir et mettre à jour régulièrement une politique de sécurité des données fondée sur les standards acceptés internationalement et sur une évaluation des risques. Cette politique pourrait être constituée, par exemple, de lignes directrices relatives à la sécurité physique, d'une politique de sécurité informatique, de lignes directrices relatives à la sécurité des courriels, de lignes directrices relatives à l'utilisation du matériel informatique, d'une typologie du traitement de l'information, d'un plan d'urgence et de lignes directrices relatives à la destruction des documents ;
- la mise en place de l'infrastructure de communication et des bases de données en vue de préserver l'intégrité et la sécurité des données, conformément à la politique de sécurité établie ;
- l'adoption de toutes les mesures appropriées, conformément au présent Code de conduite, pour préserver la sécurité des données traitées dans le système d'information du responsable du traitement.

1. Droits d'accès aux bases de données

Le responsable du traitement est chargé :

- d'attribuer les droits d'accès aux bases de données contenant des données personnelles ;
- de la sécurité des dispositifs qui permettent au personnel autorisé d'avoir accès à ce système ;
- de veiller au respect des règles de sécurité énoncées dans cette annexe ;
- de faire en sorte que le personnel ayant accès aux données soit en mesure de se conformer au présent Code de conduite. Le personnel concerné doit être formé à cet effet et avoir signé l'engagement de confidentialité figurant dans le contrat de travail, avant de se voir accorder l'accès aux bases de données ;
- de veiller à ce que l'accès ne soit accordé que sur la base du « besoin d'en connaître » (c'est-à-dire uniquement au personnel qui en a besoin) ;
- de tenir un registre du personnel ayant accès à chaque base de données, et de le mettre à jour s'il y a lieu (par ex. lorsque des membres du personnel se voient attribuer des fonctions différentes pour lesquelles ils n'ont plus besoin d'un accès) ;
- dans la mesure du possible, et à des fins de responsabilisation, de tenir un journal d'activité des employé-e-s ayant eu accès aux bases de données et de le conserver aussi longtemps que les données traitées par ces employé-e-s sont présentes dans la base de données.

Le personnel traitera les données dans les limites des droits au traitement qui lui ont été accordés.
Le personnel ayant des droits d'accès plus étendus ou chargé de l'administration des droits d'accès peut être soumis à des obligations contractuelles supplémentaires en matière de confidentialité.

2. Sécurité physique

Chaque responsable du traitement est chargé :

- d'établir les règles de sécurité définissant des contrôles de sécurité techniques, administratifs et relatifs aux procédures qui permettent de garantir des niveaux de confidentialité appropriés et de préserver l'intégrité physique et l'accessibilité des bases de données (physiques ou informatiques), en fonction des risques recensés ;
- de veiller à ce que les employés soient informés de ces règles de sécurité et les respectent ;
- de mettre au point des mécanismes de contrôle appropriés pour préserver la sécurité des données ;
- de veiller à ce que des standards appropriés en matière de sécurité électrique et de sécurité incendie soient appliqués aux installations de stockage ;
- de faire en sorte que les volumes de stockage soient limités au strict minimum nécessaire.

3. Sécurité informatique

Le responsable du traitement doit :

- établir les règles de sécurité définissant des contrôles de sécurité techniques, administratifs et relatifs aux procédures qui permettent de garantir des niveaux de confidentialité appropriés et de préserver l'intégrité et l'accessibilité des systèmes d'information utilisés, sur la base d'une évaluation des risques ;
- mettre au point des mécanismes de contrôle appropriés afin de préserver la sécurité des données ;
- établir des règles de sécurité particulières pour une partie de l'infrastructure informatique et de communication, une base de données ou un service spécifique, s'il l'estime nécessaire.

Toute la correspondance électronique, interne et externe, qui contient des données personnelles doit être traitée sur la base du « besoin d'en connaître ». Les destinataires de courriers électroniques doivent être sélectionnés avec soin afin de prévenir toute diffusion inutile de données personnelles.

L'accès à distance aux serveurs et l'utilisation d'ordinateurs fixes ou portables au domicile des employés doivent respecter les normes de sécurité établies par le responsable du traitement dans le cadre de sa politique de sécurité informatique. À moins que cela ne soit strictement nécessaire pour des raisons opérationnelles, l'utilisation de points d'accès à Internet et de connexions sans fil non sécurisées pour télécharger, échanger, transmettre ou transférer des données personnelles est à proscrire.

Le personnel qui traite des données personnelles doit prendre toutes les précautions nécessaires lorsqu'il se connecte à distance aux serveurs du responsable du traitement. Les mots de passe seront toujours protégés et les employés s'assureront qu'ils se sont déconnectés correctement des systèmes

informatiques, et que les moteurs de recherche ouverts ont été fermés.

Les ordinateurs portables, les smartphones et autres appareils médias portables exigent des précautions particulières en matière de sécurité, notamment dans des environnements de travail difficiles. Les appareils médias portables seront conservés en lieu sûr en tout temps.

Les appareils portables ou amovibles ne devraient pas être utilisés pour stocker des documents contenant des données personnelles qui sont considérées comme étant particulièrement sensibles. S'il est impossible de faire autrement, les données personnelles devraient être transférées vers des systèmes informatiques et applications pour bases de données appropriés dès que cela est raisonnablement possible. Lorsque des mémoires flash telles que des clés USB et des cartes mémoires sont utilisées pour stocker temporairement des données personnelles, elles doivent être conservées en lieu sûr et les fichiers électroniques doivent être chiffrés. Les données doivent être effacées de l'appareil portable ou amovible dès qu'elles ont été stockées correctement, lorsqu'elles ne sont plus nécessaires sur ce support.

Récupération de données et sauvegarde

Des mécanismes de récupération de données et des procédures de sauvegarde efficaces devraient être mis en place pour l'ensemble des fichiers électroniques, et le ou la responsable des technologies de l'information et de la communication (TIC) doit s'assurer que des procédures de sauvegarde sont effectuées régulièrement. La fréquence de ces procédures dépendra de la sensibilité des données personnelles. Les enregistrements électroniques devraient être automatisés de façon à permettre de récupérer facilement les données dans des situations où les procédures de sauvegarde sont difficiles à mettre en œuvre, en raison notamment de pannes d'électricité fréquentes, de pannes du système ou de catastrophes naturelles.

Lorsque des fichiers électroniques et des applications pour bases de données ne sont plus nécessaires, le responsable du traitement doit veiller, en coordination avec le ou la responsable des technologies de de l'information et des communications, à ce qu'ils soient définitivement supprimés.

4. Obligation de discrétion et conduite du personnel

L'obligation de discrétion est un élément clé de la sécurité des données personnelles. Elle s'applique :

- à tous les membres du personnel et consultants externes ayant signé des engagements de discrétion et de confidentialité dans le cadre de leur contrat de travail/de consultant. Cette exigence va de pair avec celle qui prévoit que le personnel ne devrait traiter des données que sur instruction du responsable du traitement ;
- à tout sous-traitant externe lié contractuellement par des clauses de confidentialité. Cette exigence va de pair avec celle qui prévoit qu'un sous-traitant ne peut traiter des données que sur instruction du responsable du traitement ;

  et implique :

- l'application stricte de la Typologie du traitement de l'information, fondée sur le niveau de confidentialité des données ; et
- l'obligation de s'assurer que toutes les demandes de personnes concernées souhaitant que les données personnelles les concernant soient traitées d'une manière particulière, et notamment qu'elles soient considérées comme confidentielles et ne soient pas divulguées à des tiers, est effectivement inscrite et conservée dans le dossier de la personne concernée.

Afin de limiter les risques de fuites, seul du personnel autorisé sera chargé de la collecte et de la gestion de données provenant de sources confidentielles et aura accès aux documents, conformément à la Typologie du traitement de l'information applicable.

Le personnel est chargé d'attribuer des niveaux de confidentialité aux données qu'il traite en se fondant sur la Typologie du traitement de l'information applicable, et de respecter la confidentialité des données qu'il consulte, transmet ou utilise à des fins de traitement externe.

Le personnel qui a attribué à l'origine leur niveau de confidentialité aux données peut à tout moment le modifier, notamment en l'abaissant s'il estime que les données nécessitent un niveau de protection moins élevé.

5. Plan d'urgence

Le responsable du traitement est chargé d'élaborer et d'appliquer un plan pour l'évacuation des données en cas d'urgence.

6. Méthodes de destruction

Lorsqu'il est établi que la conservation de données personnelles n'est plus nécessaire, toutes les données et sauvegardes doivent être détruites ou rendues anonymes.

La méthode de destruction dépendra notamment :

- de la nature et du caractère plus ou moins sensible des données personnelles ;
- du format et du support de stockage ; et
- du volume de documents électroniques et sur support papier.

Le responsable du traitement doit évaluer le niveau de confidentialité des données personnelles avant leur destruction afin de s'assurer que des méthodes appropriées sont utilisées pour les supprimer.

Destruction des documents papier

Les documents papier seront détruits à l'aide de méthodes telles que le déchiquetage ou l'incinération, qui ne permettent pas de les réutiliser ou de les reconstituer.

S'il a été décidé de convertir les documents papier en fichiers électroniques, il faut détruire toutes traces des documents papier une fois cette conversion dûment effectuée, à moins que la conservation des dossiers sur support papier soit exigée par la législation nationale applicable ou qu'une copie papier

doive être conservée à des fins d'archivage.

Destruction des fichiers électroniques

La destruction des fichiers électroniques devrait être confiée au personnel compétent en matière de TIC, car les fonctions d'effacement que l'on utilise dans les systèmes informatiques ne garantissent pas nécessairement la suppression complète.

Sur instruction, le personnel compétent en matière de TIC doit faire en sorte que toutes les traces de données personnelles soient complètement supprimées des systèmes informatiques et autres logiciels. Les lecteurs de disque et les applications pour bases de données doivent être purgés, et tous les supports réinscriptibles, tels que les CD, les DVD, les microfiches et les cassettes vidéo et audio qui sont utilisés pour stocker des données personnelles, doivent être effacés avant d'être réutilisés. Les méthodes physiques de destruction des enregistrements électroniques tels que le recyclage, le broyage ou l'incinération doivent être strictement surveillées.

Registres de destruction

Le responsable du traitement s'assure que tous les contrats de service, protocoles d'accord, accords et contrats écrits de transfert ou de traitement pertinents prévoient une durée de conservation au-delà de laquelle les données personnelles doivent être détruites une fois atteinte la finalité poursuivie. Les tiers doivent restituer les données personnelles au responsable du traitement et certifier que toutes les copies des données personnelles ont été détruites, notamment les données personnelles communiquées à leurs agents et sous-traitants autorisés. Des registres de destruction indiquant la date et la méthode de destruction, ainsi que la nature des documents détruits, doivent être établis et joints aux rapports sur les projets ou aux rapports d'évaluation.

La destruction de volumes importants de documents papier peut être externalisée auprès d'entreprises spécialisées. En pareil cas, le responsable du traitement doit veiller à ce que le respect de la confidentialité des données personnelles soit garanti par écrit et à ce que la soumission de registres de destruction et la délivrance de certificats de destruction fassent partie des obligations contractuelles qui incombent aux tiers.

7. Autres mesures

La sécurité des données nécessite également des règles organisationnelles internes appropriées, notamment une diffusion régulière en interne, à l'ensemble du personnel, des règles applicables à la sécurité des données et des obligations qui incombent à toutes et tous les employé-e-s au regard de la loi relative à la protection des données, notamment leurs obligations en matière de confidentialité.

Désignation d'un-e responsable de la sécurité

Chaque responsable du traitement assignera la fonction de responsable de la sécurité des données à un-e ou plusieurs employé-e-s (éventuellement Admin/ Informatique) pour s'occuper des activités en matière de sécurité.

Le ou la responsable de la sécurité devra notamment :

- veiller au respect des procédures de sécurité énoncées dans le présent Code de conduite et les règles de sécurité applicables ;
- mettre à jour ces procédures, le cas échéant ;
- organiser d'autres formations sur la sécurité des données à l'intention des membres du personnel.

Annexe 5 – Informations à fournir

Informations à fournir	Consentement	Intérêts vitaux/Intérêt public	Intérêt légitime	Obligation contractuelle/ légale
Responsable du traitement/personnel chargé du traitement	Oui	Oui	Oui	Oui
Finalité du traitement	Oui	Oui	Oui	Oui
Sous-traitants externes envisagés	Oui	DPIA et politique en matière de respect de la vie privée, si possible	Oui	Oui
Transferts envisagés	Oui	DPIA et politique en matière de respect de la vie privée, si possible	Oui	Oui
Droits des personnes concernées (information, accès, rectification, effacement, opposition)	Oui	DPIA et politique en matière de respect de la vie privée, si possible	Oui	Oui
Le cas échéant, la fourniture de données est-elle une exigence règlementaire/ contractuelle ?	Sans objet	Sans objet	Oui	Oui

Annexe 6 – Quelques éléments d'orientation pour les DPIA

Une analyse d'impact relative à la protection des données (en anglais, *Data protection Impact Assessment* – DPIA) a pour objet de recenser, d'évaluer et de traiter les risques particuliers que peuvent comporter pour les données personnelles certaines activités de rétablissement des liens familiaux (RLF). Une DPIA devrait aboutir à des mesures permettant de prévenir les risques, de les réduire au minimum ou de les atténuer d'une autre manière. Les éléments d'orientation proposés ici visent à permettre au personnel chargé du RLF d'effectuer une DPIA. Un **modèle de DPIA pour les activités de RLF**, fournissant des exemples des différents types de risques et des mesures qui pourraient être prises pour les atténuer, **est mis à la disposition des Sociétés nationales dans un document séparé**.

Exemples de circonstances dans lesquelles vous devriez envisage d'effectuer une DPIA :

- Votre organisation conserve ses fichiers sur des CD et sur support papier, et vous souhaitez maintenant mettre en place un système central de stockage électronique des fichiers. Comment allez-vous déterminer où tel ou tel type d'informations sera le mieux conservé?
- Un tsunami balaie de la carte des dizaines de villages côtiers. Des milliers de personnes sont portées disparues. Quelle quantité d'informations personnelles devriez-vous recueillir auprès des familles des personnes disparues ? Beaucoup, ou le moins possible ? Devriez-vous collecter également des données sensibles (par ex. l'ADN, ou concernant la religion ou l'appartenance politique) ?
- Le gouvernement met en place un système pour centraliser toutes les informations relatives aux personnes disparues lors du tsunami. Il vous demande de lui communiquer toutes les informations dont vous disposez sur les personnes disparues lors de cette catastrophe. Quelle quantité de données personnelles devriez-vous lui communiquer pour la recherche des personnes disparues ? Sous quelles conditions des données personnelles devraient-elles lui être transmises ?
- Une autre organisation humanitaire vous demande de lui communiquer des données sur des personnes qui vivent dans un camp de réfugiés. Devriez-vous transmettre ces données ? Sous quelles conditions ? Quelles en seraient les conséquences ? Cette organisation prendra-t-elle les mêmes précautions que votre organisation à l'égard de ces données personnelles ?
- Pouvez-vous publier sur Internet des photographies d'enfants non accompagnés qui recherchent des membres de leur famille? Pouvez-vous faire des affiches d'enfants disparus ? Dans quelles circonstances et sous quelles conditions ?
- Un réseau social vous propose de vous aider dans votre activité de rétablissement des liens familiaux après une catastrophe. Comment pouvez-vous coopérer avec le réseau social sans compromettre la sécurité des données personnelles et des personnes concernées ?
- Demain, le CICR prévoit de visiter un lieu de détention où il semblerait que se trouve une personne recherchée. Étant donné l'urgence, pouvez-vous adresser une demande de recherches ou un message Croix-Rouge au CICR par courriel?

Dans certains cas, il se peut que vous n'ayez pas le temps d'effectuer une DPIA complète, ou que la complexité, le caractère sensible et l'ampleur de l'opération de traitement n'exigent pas que vous procédiez à une analyse d'impact en bonne et due forme. Le personnel chargé du RLF devrait néanmoins toujours penser à évaluer les risques en matière de protection des données (et inscrire et conserver cette information dans la mesure du possible) lorsqu'il prend des décisions ou transfère des données. Il faut par conséquent que les employé-e-s et volontaires chargé-e-s du RLF connaissent bien le processus de DPIA et se posent les questions indiquées ci-dessous.

Un **processus** de DPIA comporte généralement les **étapes suivantes**, qui doivent figurer dans le rapport de DPIA :

A. Étude préliminaire

1. Selon la complexité, le caractère sensible et l'ampleur de l'opération de traitement, déterminer :

- si une DPIA s'avère nécessaire ;
- qui effectuera la DPIA ;
- qui examinera et validera la DPIA.

2. Dans le contexte de l'activité de RLF en question, décrire comment les données personnelles sont collectées, utilisées, conservées et transférées. Il s'agira notamment d'établir une cartographie des parties prenantes et de décrire les flux d'information (quelles sont les informations collectées, auprès de qui et par qui ? Comment ces informations sont-elles utilisées ? De quelle manière, où et pendant combien de temps ces informations sont-elles conservées ? L'intervention de sous-traitants externes est-elle prévue ? Qui a accès aux informations ?).

3. Déterminer quelles parties prenantes il convient de consulter. Il pourra s'agir de parties prenantes internes (spécialiste des technologies de l'information, juriste, psychologue, experts des programmes…), ou de parties prenantes externes (autres organisations, organismes publics, travailleurs sociaux, chefs de communauté, représentants légaux…).

B. Évaluation

4. Recenser les risques que le traitement comporte pour les personnes concernées et les risques qui peuvent résulter d'un non-respect du Code de conduite relatif à la protection des données.

5. Évaluer les risques.

6. Définir les mesures visant à prévenir, à réduire au minimum ou à atténuer d'une autre manière les risques.

7. Proposer des recommandations.

C. Validation et mise en œuvre

8. Faire examiner et valider l'évaluation.

9. Mettre en œuvre les recommandations adoptées.

10. Mettre à jour la DPIA si des changements interviennent dans l'activité.

Si une DPIA est réalisée, elle doit faire l'objet d'un rapport (contenant des informations sur les points A), B) et C) ci-dessus). Selon la complexité, le caractère plus ou moins sensible et l'ampleur de l'opération de traitement, un **rapport** de DPIA (le résultat d'un processus de DPIA) peut être très bref, ou plus approfondi et détaillé. Il peut inclure le modèle mis à la disposition des Sociétés nationales dans un document séparé.

Annexe 7 – Respect d'une obligation légale

Selon les circonstances dans lesquelles opère le responsable du traitement il peut s'agir :

- du respect d'une législation nationale ou régionale, par exemple dans le domaine du droit du travail, de l'information financière, de la fraude ou du blanchiment d'argent ;
- du respect de décisions de justice.