Réseau des liens familiaux
Code de conduite relatif à la protection des données
Modèle pour l'analyse d'impact relative à la protection des données (DPIA)

Avant de réaliser une analyse d'impact relative à la protection des données (en anglais *Data Protection Impact Assessment* – DPIA), les Sociétés nationales devraient examiner les questions suivantes :

- Des consultations avec les parties prenantes internes ont-elles eu lieu au sujet des risques découlant du traitement et des risques de non-respect du Code de conduite ?
- Des consultations avec les parties prenantes externes ont-elles eu lieu ? Dans l'affirmative, avec quelles parties prenantes, quand et dans quel but ?
- En plus de recenser les risques, les consultations ont-elles porté sur les mesures visant à les prévenir ou à les réduire au minimum ?

Question relative à la protection des données	Code de conduite	Évaluation des risques	Mesures d'atténuation	Conclusion
<u>Détermination de la finalité</u> Les données à collecter seront-elles utilisées uniquement à une fin spécifique ? Les données collectées seront-elles utilisées à d'autres fins que la finalité déterminée ?	2.1 Finalité spécifique	**Exemple** : « détournement d'usage » – les Sociétés nationales pourraient vouloir tirer un plus grand parti des données qu'elles collectent. **Dans la pratique** : les Sociétés nationales peuvent ne pas avoir conscience ou ne pas tenir compte du fait qu'elles ne peuvent pas réaffecter des données personnelles à d'autres fins que celles pour lesquelles elles les ont recueillies à l'origine sans obtenir un	**Exemples** : ▪ Définir, et inscrire aux fins de conserver cette information, les finalités pour lesquelles les données personnelles seront collectées/utilisées. Faire mieux connaître le Code de conduite relatif aux activités de RLF (qui énonce le principe de détermination de la finalité et prévoit qu'il ne peut être effectué de traitement ultérieur à la collecte qu'à des fins compatibles avec les finalités spécifiées à l'origine).	Le risque est suffisamment atténué. Le risque n'est pas nécessairement atténué, mais il est accepté. Le risque n'est ni atténué ni acceptable.

		nouveau consentement. ➢ Il se peut que la Société nationale ne respecte pas le Code de conduite relatif aux activités de RLF.	▪ Améliorer la formation du personnel concernant la détermination des finalités et la compatibilité de tout traitement ultérieur avec ces finalités. ▪ Utilisation de la base de données : dans le cadre d'une approche fondée sur le principe de la protection des données personnelles dès la conception, insérer une note dans le fichier afin de s'assurer que la finalité des opérations de traitement des données est toujours indiquée. S'il y a lieu, créer également un lien entre cette finalité et le consentement qui a pu être donné.	
<u>Limitation des données</u> Toutes les données personnelles recueillies sont-elles nécessaires pour l'activité de RLF ? Lorsque des personnes prennent contact avec vous pour demander de l'aide, les informez-vous de l'utilisation qui pourrait être faite des	2.3.2 Traitement de données adéquates, pertinentes et à jour 2.3.1 Obligations et responsabilités 2.2.1 Consentement	**Exemple** : les Sociétés nationales peuvent collecter plus de données personnelles que nécessaire en vue de la finalité spécifique. **Dans la pratique** : s'il est révélé publiquement que des employés collectent plus de données personnelles qu'ils n'en ont réellement besoin,	**Exemples** : ▪ S'assurer que les employés ne collectent que les données qui sont nécessaires pour atteindre la finalité spécifiée initialement. ▪ Dans la mesure du possible, informer au préalable les personnes concernées des modalités/finalités de la collecte et du traitement des	Le risque est suffisamment atténué. Le risque n'est pas nécessairement atténué, mais il est accepté. Le risque n'est ni atténué ni acceptable.

informations personnelles qu'elles fournissent ?	de la personne concernée 3.1 Information et accès	cela pourrait nuire à la réputation des Sociétés nationales. ➢ La collecte d'un supplément de données personnelles augmente les risques pour les bénéficiaires/leurs familles/les témoins ou autrui si le système est piraté ou subit d'autres attaques (utilisation/communication non autorisées ou violation de la sécurité). ➢ Collecter plus de données que nécessaire accroît également le risque de vol ou d'usurpation d'identité.	données. Leur donner la possibilité de poser des questions et d'exprimer des objections sur la manière dont les données les concernant sont recueillies et traitées, et à quelles fins.	
<u>Droit à l'information</u> Les personnes sont-elles informées expressément des motifs pour lesquels les données personnelles les concernant sont recueillies et de l'usage qui pourra en être fait ?	3.1 Information et accès	**Exemple** : des Sociétés nationales ne fournissent pas d'informations claires et aisément accessibles concernant leurs politiques, procédures et pratiques de collecte de données. **Dans la pratique** : une personne souhaite rechercher un membre de sa	**Exemples** : ▪ Si les Sociétés nationales ont une page web dédiée, elles pourraient avoir un onglet qui mène la personne au Code de conduite relatif aux activités de RLF. ▪ Sinon, les Sociétés nationales pourraient élaborer des « Questions et réponses »	Le risque est suffisamment atténué. Le risque n'est pas nécessairement atténué, mais il est accepté. Le risque n'est ni atténué ni acceptable.

		famille, mais elle est réticente car elle ne connaît pas bien les procédures appliquées par la Société nationale pour le traitement/ l'échange de données. ➢ Si les normes et la procédure relatives à la collecte/au traitement de données ne sont pas transparentes, des personnes peuvent se méfier de l'organisation et s'abstenir de communiquer des données personnelles les concernant. ➢ La Société nationale peut ne pas respecter le Code de conduite relatif aux activités de RLF.	résumant le Code de conduite et en distribuer des copies papier aux personnes concernées. ▪ En outre, un lien devrait être créé sur le site web de RLF ou les sites web nationaux pour présenter l'ensemble des activités ainsi que des informations générales sur les modalités de collecte et de traitement de données.	
<u>Fondement juridique du traitement/transfert de données</u> <u>Consentement</u> Les personnes concernées sont-elles en mesure d'évaluer les conséquences les plus probables (y compris négatives) ? Le traitement nécessite-t-il une technologie complexe ? Les	2.1 Finalité déterminée 2.2 Traitement licite et loyal 2.2.1 Consentement de la personne	**Exemples** : ▪ Une ou plusieurs personnes peuvent menacer de révéler publiquement qu'elles n'ont pas donné leur consentement à ce que la Société nationale collecte des données	**Exemple** : ▪ Revoir la procédure d'obtention du consentement. Expliquer aux bénéficiaires ou à leurs familles, aux témoins ou à d'autres tiers concernés les conséquences qu'entraîne le fait de s'enregistrer auprès de la Société nationale, comment	Le risque est suffisamment atténué. Le risque n'est pas nécessairement atténué, mais il est accepté. Le risque n'est ni atténué ni acceptable.

personnes concernées ont-elles véritablement le choix de donner librement leur consentement ? Peuvent-elles refuser de fournir une partie ou l'intégralité des informations sans être pénalisées d'une quelconque manière ou privées d'une assistance que votre organisation pourrait autrement leur fournir ? De quelle manière expriment-elles leur consentement à la collecte des données les concernant ? Si le consentement n'est pas écrit, quels sont, selon vous, les risques que cela entraîne ? Le consentement est-il limité à une finalité spécifique? Si les données personnelles doivent être utilisées à d'autres fins que celles indiquées initialement (une finalité secondaire), faudra-t-il obtenir un nouveau consentement de la personne ? La personne a-t-elle accepté expressément l'usage qui pourrait être fait des données personnelles la concernant, ou leur communication à d'autres organismes ?	concernée 3.1 Information et accès	personnelles les concernant. ▪ Une organisation de défense des droits de l'homme peut découvrir que dans certains cas, la Société nationale n'a pas obtenu le consentement de la personne. ▪ Un employé malveillant peut divulguer des mémos montrant que la Société nationale n'obtient pas un consentement éclairé. **Dans la pratique** : ▪ La Société nationale n'obtient pas systématiquement un formulaire signé de la personne consentant à la collecte et à l'utilisation de ses données personnelles. ➢ Atteinte à la réputation de la Société nationale. ➢ D'autres informateurs potentiels estiment qu'il n'est pas prudent ni sûr	les données les concernant pourraient être utilisées dans la base de données et à qui elles pourraient être transmises ultérieurement. ▪ S'efforcer, dans la mesure du possible, d'obtenir un formulaire de consentement éclairé dûment signé. ▪ Il serait utile d'avoir sur la page web de la Société nationale un onglet menant à une explication de ce qu'est un consentement éclairé. ▪ S'assurer que le formulaire de consentement est harmonisé et accessible quelle que soit la méthode de collecte (par ex. formulaires sur papier/en ligne, téléphone). ▪ S'assurer que le formulaire de consentement existe dans un choix de langues adapté au groupe cible.	

Y a-t-il des cas ou des circonstances où une personne a consenti au transfert ou à la communication de données personnelles, mais où le personnel responsable estime que ce n'est pas judicieux ? <u>Autre fondement juridique</u> Des données sont-elles aussi recueillies au sujet de personnes qui ne sont pas présentes ?		de communiquer des informations à la Société nationale.	▪ S'il n'est pas possible d'obtenir un consentement éclairé : traiter/transférer les données personnelles en se fondant sur un autre motif juridique (intérêt vital, intérêt public, intérêt légitime, respect d'une obligation légale).	
<u>Droit d'accès/de rectification/d'effacement</u> Les personnes concernées peuvent-elles consulter leurs données personnelles et demander qu'elles soient rectifiées ?	3.1 Information et accès 3.3 Rectification et effacement	**Exemple** : des personnes peuvent se plaindre qu'il soit difficile de consulter et, s'il y a lieu, de faire rectifier (voire effacer) les données personnelles les concernant.	**Exemples** : ▪ Si les Sociétés nationales disposent d'une page web dédiée, elles pourraient y inclure un onglet qui mène les utilisateurs à un texte leur donnant l'assurance qu'elles	Le risque est suffisamment atténué. Le risque n'est pas nécessairement atténué, mais il est accepté.

Peuvent-elles demander la suppression d'une partie ou de la totalité des données personnelles les concernant ? Est-il nécessaire de restreindre l'accès à des données ? Dans l'affirmative, ces restrictions sont-elles bien circonscrites et expliquées ?		**Dans la pratique** : les Sociétés nationales peuvent ne pas avoir de procédures particulières/transparentes pour donner aux personnes concernées accès aux données personnelles les concernant. ➢ Atteinte à la réputation. ➢ Les plaintes de ces personnes pourraient parvenir aux médias ou à des organisations de défense des droits de l'homme.	les aideront dans leurs demandes d'accès aux données les concernant. ▪ La page Web pourrait aussi indiquer les modalités d'accès (sans préjudice de la confidentialité qui pourrait s'appliquer à certaines informations).	Le risque n'est ni atténué ni acceptable.
<u>Qualité et exactitude des données</u> Quels processus sont en place pour garantir la qualité des données, c.-à-d. qu'elles sont pertinentes, fiables, exactes et à jour ? Une politique ou une procédure est-elle en place pour rectifier des données déjà communiquées à des partenaires ou pour informer ceux-ci de mises à jour ?	2.3.2 Traitement de données adéquates, pertinentes et à jour 3.3 Rectification et effacement 3.4 Opposition au traitement	**Exemples** : ▪ Le personnel des Sociétés nationales n'a pas le temps de vérifier la fiabilité des informations qu'il reçoit des bénéficiaires, de membres de leur famille ou de témoins. ▪ Seules quelques personnes – quand ce n'est pas aucune – sont réellement témoins d'un incident, ou voient des personnes se faire enlever mais sans savoir	**Exemples** : ▪ Établir une procédure de contrôle de la qualité afin de réduire au minimum les erreurs ou les modifications non autorisées avant l'enregistrement des données. ▪ Dans la mesure du possible, recouper les informations fournies par une personne avec celles d'autres organisations qui pourraient aussi avoir eu un entretien avec cette personne ou d'autres témoins. ▪ Établir des procédures qui permettent de déterminer	Le risque est suffisamment atténué. Le risque n'est pas nécessairement atténué, mais il est accepté. Le risque n'est ni atténué ni acceptable.

		ce qu'il est advenu d'elles. Le personnel des Sociétés nationales doit s'appuyer sur des informations incomplètes ou n'est pas en mesure de vérifier les informations, n'ayant pas les ressources nécessaires pour cela. ▪ Certains membres du personnel peuvent estimer qu'il faut toujours venir en aide aux demandeurs, même s'il n'est pas possible de vérifier leurs allégations. **Dans la pratique** : la conversion de documents papier en documents électroniques ou en ligne, par transcription des données, accroît le risque d'introduire des erreurs. ➢ Il se peut que les Sociétés nationales prennent des décisions fondées sur des données incomplètes, non fiables ou erronées.	quand et à quelle fréquence les informations personnelles doivent être réexaminées et/ou mises à jour, et quand les données doivent être effacées ou archivées. ▪ Établir une procédure visant à ce que les destinataires de vos données soient informés de toute rectification dont celles-ci pourraient faire l'objet ultérieurement. ▪ <u>Distinguer entre sources primaires et sources secondaires de données et insérer dans le dossier un avertissement indiquant de quel type de sources il s'agit.</u>	

		➢ Des données de mauvaise qualité peuvent donner lieu à des décisions inappropriées, susceptibles de porter préjudice aux personnes concernées.		
<u>Mesures de sécurité appropriées</u> Quelles données personnelles doivent être collectées ? La divulgation de ces informations pourrait-elle mettre la personne en danger (par exemple des informations relatives à l'origine ethnique, à la religion, à l'orientation sexuelle, aux opinions politiques, à l'appartenance à un syndicat, etc.) Y a-t-il un risque que les données soient volées / perdues / altérées / rendues inaccessibles /que le système soit piraté/que l'organisation fasse l'objet d'une surveillance ? Quelles mesures préventives sont en place ? D'autres organisations ou des tiers interviennent-ils dans le traitement ? Cela accroît-il le risque de surveillance/de divulgation par le sous-traitant (licitement ou non)/de piratage/de vol de données/d'accessibilité ?	2.3.7 Sécurité des données 2.3.8 Violation de données personnelles 2.3.1 Obligations et responsabilités 6. Application du Code de conduite	**Exemples** : ▪ Des pirates informatiques extérieurs et des employés malintentionnés peuvent chercher à exploiter des données personnelles. ▪ Les gouvernements hôtes peuvent demander qu'on leur communique les données de toutes les personnes à qui le CICR fournit une assistance. ▪ Dans une situation de violence, les bureaux des Sociétés nationales peuvent être mis à sac. **Dans la pratique** : ▪ La Société nationale peut avoir omis d'inculquer à son personnel de bonnes	**Exemples** : ▪ Encourager le personnel à éviter d'utiliser des dispositifs de stockage amovibles non sécurisés, tels que des clés USB (en le mettant en garde contre ces dispositifs). ▪ Mettre au point des protocoles de contrôle d'accès solides qui limitent l'accès uniquement au personnel qui en a besoin. Les utilisateurs ne doivent avoir accès qu'aux données dont ils ont besoin pour s'acquitter de leurs fonctions légitimes. ▪ Établir clairement qui a le pouvoir d'attribuer, de modifier ou de révoquer des droits d'accès. ▪ S'assurer que tous les accès aux bases de données sont inscrits – aux fins de conserver cette information – dans un	Le risque est suffisamment atténué. Le risque n'est pas nécessairement atténué, mais il est accepté. Le risque n'est ni atténué ni acceptable.

L'accès aux données est-il limité uniquement aux personnes qui en ont réellement besoin ? Comment cette exigence est-elle mise en œuvre concrètement ? Est-il rappelé aux membres du personnel qu'ils doivent conserver en tout temps les dossiers papier, les CD et les clés USB avec eux ou enfermés à clef dans un meuble lorsqu'ils ne sont pas utilisés ? Les membres du personnel sont-ils encouragés à chiffrer les clés USB ? Des formations sont-elles dispensées à l'ensemble des membres du personnel sur les bonnes pratiques de protection des données et de sécurité de l'information ? Les courriels sont-ils chiffrés ? Quel type de chiffrement est utilisé ? Quelles mesures seront prises en cas de violation de données ? Les personnes concernées sont-elles informées en cas de perte, de vol ou d'autre atteinte à leurs données personnelles ? D'autres organisations		pratiques en matière de sécurité des informations. ▪ Elle peut omettre de prendre des mesures de précaution solides pour protéger l'accès à sa base de données. ▪ Des membres du personnel utilisent peut-être des mots de passe faibles ou ne chiffrent pas les données. ▪ Les données conservées sur un support papier (par ex. des carnets) ne sont pas toujours sauvegardées, et les dossiers peuvent n'être conservés que dans les bureaux. ➢ Les mesures de sécurité du système établies par la Société nationale ne sont pas respectées, et il y a un risque d'atteinte à la protection des données personnelles. ➢ La Société nationale ne sait pas à quel	registre des opérations de traitement. ▪ Mettre en place des procédures de notification des violations de données pour informer les personnes concernées.	

seront-elles informées ? Avez-vous envisagé les pires conséquences possibles s'il arrivait que les données personnelles collectées par votre organisation soient compromises ou effacées accidentellement ou délibérément ? Comment allez-vous déterminer quels risques sont les plus probables et lesquels sont susceptibles d'avoir le plus d'impact en cas de vol, de piratage ou d'altération des données personnelles ?		moment des données personnelles en sa possession sont compromises. ➢ Elle subit des atteintes à sa réputation. ➢ Les données compromises mettent des vies en danger.		
<u>Échange/divulgation/publication et/ou transfert de données</u> Les données personnelles seront-elles mises en commun avec – ou communiquées à – d'autres organisations, notamment d'autres Sociétés nationales ? Dans quel but ? Ces autres organisations ont-elles donné des assurances écrites qu'elles protègeront les informations et ne les transmettront pas ultérieurement ? Ont-elles une politique adéquate en matière de protection des données ? La personne concernée a-t-elle	4. Transferts de données 2.3.1 Obligations et responsabilités 1.4.3 Confidentialité 2.3.2 Traitement de données adéquates, pertinentes et à jour	**Exemple** : des membres du personnel peuvent échanger des données personnelles avec d'autres organisations ou avec les autorités sans avoir aucun contrôle sur les utilisations et transferts ultérieurs qui pourraient être effectués par ces autres organisations ou les autorités. **Dans la pratique** : les publications de photographies de mineurs non accompagnés pourraient attirer l'attention	**Exemples** : ▪ S'abstenir de transférer des informations personnelles à d'autres organisations ou aux autorités en l'absence d'un fondement juridique (consentement, intérêt public, etc.). En outre, n'échanger des informations personnelles avec d'autres organisations ou avec les autorités que si elles appliquent une politique de protection des données d'un niveau au moins équivalent à celui que prévoit le Code de	Le risque est suffisamment atténué. Le risque n'est pas nécessairement atténué, mais il est accepté. Le risque n'est ni atténué ni acceptable.

expressément consenti à la communication des données la concernant ? Si votre organisation réalise des vidéos promotionnelles, des brochures ou des reportages, rend-elle les informations personnelles anonymes, de telle sorte que, même si elles sont associées à d'autres données, il soit impossible d'identifier une personne ?	2.3.7 Sécurité des données 5. Publication de données	de trafiquants d'enfants. ➢ La personne concernée/sa famille peut être en danger si l'organisation ne traite pas les données conformément à des normes de protection des données adéquates. ➢ Des personnes peuvent se plaindre de la divulgation de données les concernant.	conduite relatif aux activités de RLF. ▪ Ne publier que la photographie et un numéro de téléphone central, sans donner d'autres détails. Avant d'accepter de rétablir le contact, vérifier la fiabilité des informations fournies par des personnes prétendant être des membres de la famille en les recoupant avec d'autres données disponibles et avec les informations fournies par les bénéficiaires eux-mêmes	
<u>Conservation de données</u> Des informations personnelles sont-elles saisies dans des bases de données ? Est-il nécessaire de conserver toutes les données qui sont traitées ? Des procédures sont-elles en place pour revoir la durée pendant laquelle les données doivent être conservées ? Existe-t-il une politique, une procédure, un principe directeur régissant l'archivage d'informations personnelles ?	2.3.6 Conservation des données	**Exemple** : les données personnelles recueillies initialement l'ont été sans que la durée de conservation soit précisée, et sont conservées pour une durée indéterminée. **Dans la pratique** : des volumes importants de données sont enregistrés dans la base de données de la Société nationale, mais ne sont plus nécessaires pour atteindre la finalité en vue de laquelle elles ont été recueillies.	**Exemples** : ▪ Limiter la conservation des données personnelles à la durée nécessaire pour atteindre des finalités spécifiques, explicites et légitimes. ▪ Utilisation de la base de données : dans le cadre d'une approche fondée sur le principe de la protection des données dès la conception, insérer une indication visant à ce que la période de conservation des données soit toujours précisée. En outre, lier	Le risque est suffisamment atténué. Le risque n'est pas nécessairement atténué, mais il est accepté. Le risque n'est ni atténué ni acceptable.

Y a-t-il trop de données conservées à des fins d'audit ? Serait-il possible d'en conserver moins ?		➢ Surcharge d'informations : la gestion des données dans ce contexte est chronophage pour la personne chargée du dossier, et cela n'en vaut peut-être pas la peine si les données ne sont pas nécessaires à des fins de RLF. ➢ La Société nationale ne respecte pas le Code de conduite relatif aux activités de RLF.	la durée de conservation des données à la finalité des opérations de traitement des données. Une durée de conservation initiale peut être prolongée si la conservation des données est jugée nécessaire pour atteindre la finalité en vue de laquelle elles ont été recueillies.	
<u>Risques pour les personnes</u> autres que les risques recensés ci-dessus L'activité en question est-elle, en soi, susceptible d'engendrer des risques d'atteinte à l'intégrité physique ou morale des personnes concernées ?				
<u>Responsabilité/mécanisme de contrôle</u> <u>Les normes et les procédures relatives</u>	6. Application du Code de conduite	**Exemple** : menace interne – comme personne ne s'est vu attribuer la responsabilité spécifique de protéger les		Le risque est suffisamment atténué. Le risque n'est pas

<u>à la protection des données sont-elles mises en œuvre efficacement ?</u> <u>Des mécanismes sont-ils en place pour contrôler les pratiques existantes et fournir des orientations à la Société nationale ?</u>		données personnelles, il se peut que des membres du personnel de la Société nationale collectent et utilisent de telles données sans se préoccuper des conséquences de leurs actes. **Dans la pratique** : ▪ Il se peut que la Société nationale n'ait attribué à aucun membre de son personnel la responsabilité de la protection des données. ▪ Personne n'a inscrit ni diffusé les politiques, procédures et pratiques en matière de protection des données. ▪ La Société nationale n'a pas attribué à un membre de son personnel la responsabilité du transfert à des tiers, et ne vérifie pas si les organisations à qui elle transfère des données personnelles se conforment aux standards de protection		nécessairement atténué, mais il est accepté. Le risque n'est ni atténué ni acceptable.

		des données de façon à assurer le même niveau de protection que celui que prévoit le Code de conduite. ➢ Manque de confiance/méfiance à l'égard des activités menées par la Société nationale.		