Family Links Network
Code of Conduct for Data Protection
Template for Data Protection Impact Assessment (DPIA)

Prior to conducting a DPIA, the following questions should be considered by National Societies:

- Have any consultations with internal stakeholders taken place with regard to risks arising from the processing operation and risks of non-compliance with the Code of Conduct?
- Have any consultations with external stakeholders taken place? If yes, who, when and for what purpose?
- In addition to identifying risks, have the consultations involved consideration of measures for avoiding or minimising the risks?

Data protection issue	Code of conduct	Assessment of risks	Mitigation measures	Conclusion
<u>Purpose specification</u> Is the data to be collected to be used only for a specified purpose? Will the data collected be used for anything other than the specified purpose?	2.1 Specified Purpose	**Example**: "Function creep" – National Societies may want to gain more value from the data they collect. **In practice:** National Societies may ignore or are not aware that they cannot repurpose personal data (i.e., to use the data they originally collected for some additional purposes) without seeking consent again. ➢ The National Society may not comply with the RFL Code of Conduct	**Examples:** ▪ Specify/document the purposes for which personal data will be collected/used ▪ Raise awareness on RFL Code of Conduct that provides for the purpose specification principle and for further processing only if for purposes compatible with the original purpose of data collection. ▪ Improve training of staff regarding purpose specification/compatible further processing. ▪ Use of database: As part of a privacy-by-design approach, insert reference in the file to ensure the purpose of the data	Risk sufficiently mitigated Risk not necessarily mitigated but accepted Risk neither mitigated nor acceptable

Data protection issue	Code of conduct	Assessment of risks	Mitigation measures	Conclusion
			processing operations is always specified. Where applicable, also link the purpose of the data processing operations to the consent that may have been provided.	
<u>Data limitation</u> Is all the personal data collected necessary for the RFL activity? When people engage with you seeking help, are they told how the personal information they supply will be used?	2.3.2 Processing adequate relevant and updated data 2.3.1 Responsibility and accountability 2.2.1 Consent 3.1 Information and access	**Example:** National Societies may collect more personal data than necessary for the specified purpose. **In practice**: National Societies may suffer reputational damage when it becomes publicly known that staff are collecting more personal data than they actually need. ➢ The additional personal data collected creates a bigger risk for the beneficiaries/ their families/witnesses/ or others if the system is hacked or otherwise compromised (unauthorized use/disclosure or security breach.) ➢ Collecting more detail than needed also	**Examples:** ▪ Ensure the staff collects only the pieces of data which are necessary to achieve the purpose specified originally ▪ If possible, give people prior notice regarding the modalities/purposes of the data collection and processing. Give individuals an opportunity to question the manner and purpose for which their data is collected and processed.	Risk sufficiently mitigated Risk not necessarily mitigated but accepted Risk neither mitigated nor acceptable

Data protection issue	Code of conduct	Assessment of risks	Mitigation measures	Conclusion
		increases the risk of identity fraud or theft.		
<u>Right to information</u> Are individuals explicitly informed about why their personal data is being collected and how it may be used?	3.1 Information and access	**Example**: National Societies do not provide individuals with clear and easily accessible information regarding their policies, procedures and practices on the collection of information. **In practice:** An individual would like to trace his/her relative but does not feel at ease in doing so as he/she is not fully aware of data processing/sharing procedures implemented by the National Society. ➢ If data collection/processing standards and procedure are not transparent, individuals may not trust the Organization and refrain from sharing their personal data. ➢ The National Society may not be compliant with the RFL Code of Conduct	**Examples**: ▪ Should National Societies have a dedicated web page, they could have a tab that links the individual with the RFL Code of Conduct. ▪ Alternatively, National Societies could develop Q&A summarizing the RFL Code of Conduct and make hard copies available to data subjects. ▪ In addition, a link should be created on the Family Links website or national websites to present general activities as well as general data collection/processing modalities.	Risk sufficiently mitigated Risk not necessarily mitigated but accepted Risk neither mitigated nor acceptable

Data protection issue	Code of conduct	Assessment of risks	Mitigation measures	Conclusion
<u>Legal basis for data processing/transfer</u> <u>Consent</u> Are individuals able to appreciate the most likely consequences (including negative)? Does the processing involve complex technologies? Does the person have a genuine free choice as to whether to consent? Are they able to refuse to provide some or all information without being penalised in any way or deprived of any assistance that your organisation might otherwise provide? How do individuals provide consent for their information to be collected? If consent is not written, do you see any risks involved? Is consent limited to a specified purpose? If the personal data were to be used for a purpose other than that originally specified (a secondary purpose), will a new consent be sought from the individual? Has the individual explicitly agreed to how their information can be used, or	2.1 Purpose specification 2.2 Lawful and fair processing 2.2.1 Consent 3.1 Information and access	**Example**: ▪ One or more individuals threaten to announce publicly that they did not give their consent to the National Society's collection of their personal data. ▪ An advocacy organization might discover instances where the National Society did not get the consent of the individual. ▪ A rogue employee leaks memos showing that the National Society does not get informed consent. **In practice:** ▪ The National Society does not routinely obtain a signed form from the individual consenting to the collection and use of his or her personal data. ➢ Damage to the National Society's reputation.	**Example:** ▪ Review the process by which consent is sought. Explain to beneficiaries or their families, witnesses or other relevant third parties the implications of registering with the National Society, how their data could be used in the database and to whom it could be further transferred. ▪ Attempt, where possible, to get a signed informed consent form. ▪ It would be worthwhile having a tab dedicated to what is informed consent on the National Society web page ▪ Ensure that the consent form is consistent and accessible across all methods of collection, including hard-copy/online forms and via telephone. ▪ Ensure that the consent form is available in an appropriate range of languages for the target group.	Risk sufficiently mitigated Risk not necessarily mitigated but accepted Risk neither mitigated nor acceptable

Data protection issue	Code of conduct	Assessment of risks	Mitigation measures	Conclusion
that it can be shared with other agencies? Are there instances or circumstances where an individual has consented to the sharing or disclosure of personal information, but where the staff in charge does not think it is wise to do so? <u>Alternative legal basis</u> Is data also collected of individuals who are not present?		➢ Other potential informants decide it is not prudent or safe to talk to the National Society.	▪ If it is not possible to obtain an informed consent: process/transfer personal data on an alternative legal basis (vital interest , public interest , legitimate interest, compliance with a legal obligation)	
<u>Right to access / Rectification / Deletion</u>	3.1 Information and access	**Example:** Some individuals may complain about how difficult it is to see and, if	**Examples:** ▪ Should National Societies have a dedicated web page, they could have a tab that links the	Risk sufficiently mitigated

Data protection issue	Code of conduct	Assessment of risks	Mitigation measures	Conclusion
Are individuals provided with the possibility to access and correct their personal information? Can they request the deletion of some or all of their personal information? Is it necessary to restrict access to data? If so, are these restrictions adequately circumscribed and explained?	3.3 Rectification and deletion	necessary, amend (or even delete) their personal data. **In practice:** National Societies may not have specific/transparent procedures to provide data subjects access to their personal data. ➢ Reputation damage ➢ individuals' complaints could reach the media or advocacy organizations.	individual with the assurance that they will help individuals in their requests for sight of their data. ▪ The web page could also specify the modalities of access (without prejudice to the confidentiality which may apply to certain pieces of information.)	Risk not necessarily mitigated but accepted Risk neither mitigated nor acceptable
<u>Information quality and accuracy</u> What processes are in place for ensuring information quality, i.e., that the information is relevant, reliable, accurate, actionable? Is there a policy or procedure in place to correct data that has already been shared with partners, or to notify partners about updates?	2.3.2 Processing adequate, relevant and updated data 3.3 Rectification and deletion 3.4 Objection	**Example:** ▪ National Societies' staff do not have enough time to check the reliability of the information they receive from the beneficiaries, their families or witnesses. ▪ Few or no people actually witness an event or only see individuals taken away, but with no knowledge of what happens to them. National Society staff have to rely on incomplete information or are unable to verify	**Examples:** ▪ Ensure a process of quality control to minimize errors or unauthorized modifications prior to recording the data. ▪ Where possible, cross-check information received from an individual with other organizations who may also have interviewed the individual or other witnesses. ▪ Establish procedures to determine when and how often personal information should be reviewed and/or updated and when data should be deleted or archived	Risk sufficiently mitigated Risk not necessarily mitigated but accepted Risk neither mitigated nor acceptable

Data protection issue	Code of conduct	Assessment of risks	Mitigation measures	Conclusion
		information. Staff have insufficient resources to verify claims. ▪ Some staff are of the view that people should be given assistance anyway even if it is not possible to verify claims. **In practice:** Migrating paper records to a digital or online format by transcribing data increases the risk of introducing inaccuracies. ➢ National Societies may take decisions based on incomplete, unreliable or false information. ➢ Poor quality information may lead to inappropriate decisions that have a negative impact on the individuals concerned.	▪ Establish a procedure to notify recipients of your data of subsequent corrections to the data. ▪ <u>Distinguish between primary and secondary sources of data and reflect this distinction in a caveat in the file.</u>	
<u>Appropriate security measures</u> What personal information is to be collected? Could disclosure of this information put the person in danger (for example information relating to ethnicity, religion, sexual orientation,	2.3.7 Security 2.3.8 Data breaches 2.3.1 Responsibility	**Example:** ▪ External hackers and rogue employees may seek to exploit personal data. ▪ Host governments may want details of all people	**Examples:** ▪ Encourage (warn) employees to avoid use of unsecured portable storage devices, such as memory sticks. ▪ Develop robust access control protocols which limit access on	Risk sufficiently mitigated Risk not necessarily mitigated but accepted

Data protection issue	Code of conduct	Assessment of risks	Mitigation measures	Conclusion
political views, trade union membership, etc.) Is there a risk of information being stolen / lost / altered / rendered unavailable / system hacked / organisation subject to surveillance? What preventative measures are in place? Does the processing involve external organisations or third parties? Does this increase the risk of surveillance / disclosure by the processor (whether lawfully or not) / hacking / data theft / availability? Is information limited to others on a "need to know" basis? How is this implemented in practice? Are staff reminded to keep paper files, CDs and/or memory sticks locked up or with them at all times when they are not in use? Are staff encouraged to encrypt memory sticks? Is training given to all staff on good data protection and information security practices?	and accountability 6. Application of the Code of Conduct	to whom the ICRC provides assistance. ▪ In a situation of violence offices of National Societies may be ransacked. **In practice:** ▪ The National Society may not impart to employees good information security practices. ▪ It may not put in place strong controls for access to its database ▪ Employees may use weak passwords or may not encrypt data. ▪ Some data (e.g., notebooks) in paper form is not backed up and may be found only in offices. ➢ The security controls of the National Society's system are breached and personal data is compromised. ➢ The National Society does not know when the personal data it holds is compromised.	a 'need to know' basis. Users should only have access to that portion of data they need to carry out their legitimate functions. ▪ Ensure clarity re who has the authority to assign, change or revoke access privileges. ▪ Ensure all accesses to the databases are logged into a register of processing operations. ▪ Set-up data breach notification procedures to inform the data subjects.	Risk neither mitigated nor acceptable

Data protection issue	Code of conduct	Assessment of risks	Mitigation measures	Conclusion
Are e-mails encrypted? What kind of encryption is used? What action will be taken if there is a data breach? Are individuals informed if their personal data is lost, stolen or other compromised? Will any other organisations be informed? Have you considered some worst-case scenarios regarding what might happen if the personal data collected by your organisation was compromised or deleted either by accident or purposely? How would you decide which risks are the most likely and those that are likely to have the greatest impact if the personal information were stolen, hacked, altered or stolen?		➢ It suffers damage to its reputation. ➢ Compromised data puts lives at risk.		
<u>Data sharing, disclosure/publication and/or transfer</u> Will the personal information be shared with or disclosed to other organisations, including other National Societies? Why?	4. Transfers 2.3.1 Accountability and Responsibility 1.4.3 Confidentiality	**Example:** Staff may share personal data with other organizations or authorities over which they have no control regarding how the other organizations or authorities may use that data or further share it.	**Examples:** ▪ Share personal information with other organizations or authorities only if a specific legal basis exists (consent, public interest etc.) Additionally, share personal information with other organizations or authorities	Risk sufficiently mitigated Risk not necessarily mitigated but accepted Risk neither mitigated nor acceptable

Data protection issue	Code of conduct	Assessment of risks	Mitigation measures	Conclusion
Have they provided written assurances that they will safeguard the information and not share it further? Does the organisation have an adequate data protection policy? Has the individual data subject explicitly agreed to the sharing of their data? Where your organisation develops promotional videos, brochures or press stories, has your organisation anonymised personal information so that even if it were linked to other data, it would not be possible to identify the person?	2.3.2 Processing Adequate Relevant and Updated Data 2.3.7 Data Security 5. Publication	**In practice:** Publications of photos of unaccompanied minors could attract attention of child traffickers ➢ The data subject/family can be put at risk if the organisation does not process the data according to adequate data protection standards ➢ Individuals may complain about the disclosure of their data	only if they observe adequate data protection to at least the same standard as the RFL Code of Conduct. ▪ Only publish the photo and a central phone number, no other details. Cross check reliability of alleged relatives against other data available and the beneficiaries themselves before accepting to restore contact	
<u>Data retention</u> Is personal information being entered into databases? Is it necessary to keep all of the data that is being processed? Are there procedures for reviewing how long data should be retained?	2.3.6 Data Retention	**Examples:** The personal data originally collected is collected without specifying the retention period and is kept for an unlimited period. **In practice**: Large amounts of data are recorded in the National Societies' databases but are not necessary anymore to fulfil the	**Examples:** ▪ Limiting the retention of personal data to what is necessary to fulfil specific, explicit and legitimate purposes. ▪ Use of database: As part of a privacy-by-design approach, insert reference in the file to ensure the data retention period is always specified. Also	Risk sufficiently mitigated Risk not necessarily mitigated but accepted Risk neither mitigated nor acceptable

Data protection issue	Code of conduct	Assessment of risks	Mitigation measures	Conclusion
Is there a policy, procedure, rationale for archiving personal information? Is too much data being kept for auditing purposes? Could this be minimised?		purpose for which they were originally collected ➢ Information-overload: data management in this context is time-consuming for the case worker and might not be worth it if the data is not necessary to carry out RFLactivities ➢ The National Society does not comply with the RFL Code of Conduct	link the data retention period to the purpose of the data processing operations. An initial retention period could be extended if it is considered necessary to keep the data to fulfil the purpose for which it was originally collected.	
<u>Risks to individuals</u> other than the risks identified above: Is the activity in question, in and of itself, likely to give rise to risks to the physical or moral integrity of the individuals concerned?				
<u>Accountability/Oversight mechanism:</u> <u>Are data protection standards and procedures effectively implemented?</u>	6. Application of the RFL Code of Conduct	**Example:** Insider threat -- Since no one may have the specific responsibility for safeguarding personal data, the National Society staff	**Example:** A data protection focal point is entrusted with the specific responsibility for ensuring the adequacy of national societies'	Risk sufficiently mitigated Risk not necessarily mitigated but accepted

Data protection issue	Code of conduct	Assessment of risks	Mitigation measures	Conclusion
Are oversight mechanisms in place to overview existing practices and to provide guidance to the national society?		may collect and use personal data without any concerns about the consequences of their actions. **In practice:** ▪ The National Society may not have assigned accountability to anyone for data protection ▪ No one has documented and communicated the data protection policies, procedures and practices ▪ The National Society has not assigned responsibility to a specific staff member for the transfer of personal data to a third party and does not verify that the organizations with whom it shares personal data comply with data protection standards to the same degree as the RFL Code of Conduct. ➢ Lack of trust/confidence regarding activities carried out by National Society	policies, procedures and practices with the RFL Code of Conduct.	Risk neither mitigated nor acceptable