APPENDIX 1

TEMPLATE FOR A DPIA REPORT

COVER PAGE

- Data Protection Impact Assessment on [name of activity]
- Contact person, title and email address
- Date

EXECUTIVE SUMMARY

If the DPIA is more than 20 pages, it should include an executive summary. The executive summary should include details of why the DPIA was undertaken, for whom and who conducted it. The executive summary should include the key findings and principal recommendations.

INTRODUCTION AND OVERVIEW OF THE DPIA PROCESS

The introduction should outline the scope of the DPIA, when, why and for whom it was performed and by whom. It should provide some information about the activity assessed. It should introduce the methodology employed in the DPIA (e.g. the method chosen to engage stakeholders).

THRESHOLD ASSESSMENT

This section should list the questions addressed by the Humanitarian Organization to determine whether a DPIA was necessary and what should be the scale of the DPIA.

DESCRIPTION OF THE ACTIVITY OR PROJECT TO BE ASSESSED

The description of the activity to be assessed should state who is undertaking the activity and when it is to be undertaken. It should state who will be affected by the activity, and who might be interested in or affected by the activity. The description should provide contextual information about how the activity fits in with the Humanitarian Organization's other services or activities.

INFORMATION FLOWS

This section should detail (at a minimum):

- the type of data to be collected;
- whether sensitive information will be collected;

- how the data will be collected;
- for what purposes the data will be used;
- how and where the data will be stored and/or backed up;
- who will have access to the Personal Data;
- whether Personal Data will be disclosed;
- whether sensitive Personal Data will be disclosed;
- whether any data will be transferred to other organizations or countries.

COMPLIANCE WITH LAWS, REGULATIONS, CODES AND GUIDELINES

The DPIA report should identify the laws, regulations, codes of conduct and guidelines with which the activity complies or should comply. At the global level, the privacy principles listed in the ISO/IEC 29100:2011 standard of the International Organization for Standardization (ISO)[1] are useful as a reference in a DPIA. In addition, the DPIA report should state how it complies with the Humanitarian Organization's confidentiality rules and codes of conduct, and how the Humanitarian Organization monitors compliance.

STAKEHOLDER ANALYSIS

The report should identify who are the principal stakeholders interested in or affected by the data Processing and how the DPIA or the Humanitarian Organization arrived at this list.

DATA PROTECTION IMPACTS (RISKS)

This section should detail the privacy risks identified in relation to the main privacy principles found in relevant legislation and the Humanitarian Organization's confidentiality rules and codes of conduct.

RISK ASSESSMENT

This section of the report should include details of how the risks were assessed and the results of any risk assessment undertaken.

1 International Organization for Standardization (ISO), "ISO/IEC 29100:2011 | Information Technology – Security Techniques – Privacy Framework," 2017, www.iso.org/standard/45123.html.

ORGANIZATIONAL ISSUES

The DPIA report should include a section that describes how senior management is involved in decision making related to data protection. This should include discussion identifying any organizational issues that are directly or indirectly affected by the data Processing activity. For example, it may become apparent that the data Processing requires putting in place an organizational mechanism for ensuring accountability, i.e. that a senior manager is responsible for ensuring that the programme does not negatively affect the Humanitarian Organization or its stakeholders.

In the course of the DPIA, it may become apparent to the DPIA team that the Humanitarian Organization needs to spend more time on raising the awareness of employees about privacy and/or ethical issues, and that the Humanitarian Organization needs to mainstream data protection in the organization. The report should state what the Humanitarian Organization does now to raise employee awareness of data protection and how it could improve.

The report should state how the Humanitarian Organization identifies, investigates and responds to data protection incidents, e.g. data protection breaches, how the Humanitarian Organization decides to notify affected parties and how it seeks to learn from an incident.

This section should also describe how the Humanitarian Organization responds to requests for access to personal information or to correct or amend the information it has gathered and to whom the data are transferred and what safeguards the Humanitarian Organization insists be in place before making a transfer.

RESULTS OF THE CONSULTATION(S)

The report should specify what efforts the Humanitarian Organization has made to consult with stakeholders, to gather their views and ideas about potential data protection impacts, how they might be affected by the data Processing (positively and/or negatively) and how negative impacts could be mitigated, avoided, minimized, eliminated, transferred or accepted.

The DPIA team should specify which consultation techniques were employed (surveys, interviews, focus groups, workshops, etc.), when they were undertaken, the results of each consultation exercise and whether differences in opinion were discovered when different techniques were used.

The DPIA should state who was consulted and what information materials the Humanitarian Organization provided to stakeholders, including families of the missing.

The DPIA should state whether the consultations yielded any new findings and what efforts the Humanitarian Organization had made to take into account stakeholder views and ideas in the design of the data Processing activity.

RECOMMENDATIONS

The DPIA team should set out their recommendations for avoiding, minimizing, transferring or sharing the data protection risks. Some risks may be worth taking and, if so, the DPIA should say why. The DPIA should be clear who will bear the risk (i.e. will it be the Humanitarian Organization or stakeholders or others?). The DPIA should also set out what further work is necessary or desirable to implement its recommendations (for example, the DPIA should mention the need for independent Third Party monitoring of its recommendations.

The DPIA should also make recommendations as to whether the DPIA report should be made public. There may be circumstances where it might not be appropriate to make the DPIA or parts of it public – e.g. there may be confidentiality or security reasons. Often the report can be redacted in places and then made public or sensitive parts can be placed in a confidential appendix. Alternatively, the Humanitarian Organization could provide a summary of the DPIA report.