CHAPTER 5

DATA PROTECTION IMPACT ASSESSMENTS (DPIAS)

5.1 INTRODUCTION*

The Processing of Personal Data can increase risks for individuals, groups and organizations, as well as society as a whole. The purpose of a Data Protection Impact Assessment (DPIA) is to identify, evaluate and address the risks to the Data Subject – arising from a project, policy, programme or other initiative. A DPIA should ultimately lead to measures that contribute to the avoidance, minimization, transfer and/or sharing of data protection risks. A DPIA should follow a project or initiative that requires Processing of individuals' data throughout its life cycle. The project should revisit the DPIA as it undergoes changes or as new risks arise and become apparent.

Here are examples of when a DPIA is appropriate:

- The offices of the Humanitarian Organization have been looted once too often. The Humanitarian Organization wants field offices either to dispose of their paper files or send them to headquarters and to rely instead on a cloud-based storage system. Should field offices do away with paper, CDs and flash drives?
- A local NGO or authority approaches a Humanitarian Organization saying it wants to reunite family members separated because of violence in the country. It wants the Humanitarian Organization to supply all the information it has on missing persons in the country. Should the information be shared? If so, how much personal information should be shared in order to trace missing persons? Under what conditions should personal information be disclosed?
- A tsunami sweeps away dozens of coastal villages. Thousands of people are reported missing. How much personal information should the Humanitarian Organization collect from the families of persons unaccounted for? Should it be as much information as is available, or should there be limits? Should it include information on health or genetic data, religious affiliation or political views, or other information which, if disclosed, could potentially give rise to significant harm to the individuals concerned?
- Should Humanitarian Organizations publish pictures of unaccompanied children who are unaccounted for on the Internet? Should the Humanitarian Organization produce posters with these pictures? Under what circumstances?

The DPIA can play a key role in determining who might be adversely affected by privacy or data protection risks, and how they might be harmed.

This chapter is a step-by-step guide for Humanitarian Organizations on how to conduct a DPIA and what should be included in a DPIA report. Appendix 1 contains a template for a DPIA report.[1] Although a DPIA report is not the end of a DPIA

[*] The author thanks Trilateral Research for permission to use their material on Data Protection Impact Assessments, and Alessandro Mantelero and Nahide Basri for their input and feedback.

[1] See Appendix 1 — Template for a DPIA report.

process, it is crucial to its success. The report helps the Humanitarian Organization identify the privacy impacts of a proposed project and what must be done to ensure that the project protects Personal Data. It also helps the Humanitarian Organization reassure stakeholders that it takes their rights to privacy and data protection seriously and that it seeks the views of those who might be affected by or interested in the programme. Humanitarian Organizations should consider making the DPIA report or, at least, a summary of it available to stakeholders.

5.2 THE DPIA PROCESS

This section provides a guide through the steps necessary to undertake a DPIA. There are different approaches to conducting DPIAs. The following guidance draws on best practices from a range of sources.[2]

5.2.1 IS A DPIA NECESSARY?

Any organization that collects, processes, stores and/or transfers Personal Data to other organizations should consider conducting a DPIA, the scale of which will depend on the severity of the risks assessed by the organization. A Humanitarian Organization may not be aware of all relevant data protection risks beforehand, and certain risks may only become apparent during the course of the DPIA. The Humanitarian Organization may view the risks as being so small that they do not justify a DPIA. Some risks may be real, but still relatively small, so the DPIA process and report may be correspondingly short. Other risks may be very serious, and the Humanitarian Organization will want to conduct a thorough DPIA. There is no one-size-fits-all solution.

5.2.2 THE DPIA TEAM

The second step involves identifying the DPIA team and setting the terms of reference. The DPIA team should include or consult the Humanitarian Organization's DPO. Depending on the scale of the DPIA to be undertaken, the DPIA team could include experts from the Humanitarian Organization's IT, legal, operations, protection, policy, strategic planning, archives and information management, and public relations groups. The team undertaking the DPIA should be familiar with data protection requirements as well as the Humanitarian Organization's confidentiality

[2] David Wright, "Making Privacy Impact Assessment more effective", *The Information Society*, Vol. 29, No. 5, 2013, pp. 307–15: https://doi.org/10.1080/01972243.2013.825687; Information and Privacy Commission New South Wales, *Guide to Privacy Impact Assessments in NSW* Information and Privacy Commission New South Wales, May 2020: www.ipc.nsw.gov.au/guide-privacy-impact-assessments-nsw; International Organization for Standardization (ISO), "ISO/IEC 29134:2017 | Information Technology – Security Techniques – Guidelines for Privacy Impact Assessment", 2016–2017: www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/06/22/62289.html.

rules and codes of conduct. Importantly, it should also include staff familiar with the planned project. Setting the terms of reference includes planning the time frame for the DPIA, the scope of the DPIA, the stakeholders to be consulted, the budget for the DPIA, and the steps that will be taken after the DPIA in terms of review and/or audit.

5.2.3 DESCRIBING THE PROCESSING OF PERSONAL DATA

The DPIA team should prepare a description of the programme or activity to be assessed. The description should include:

- the aims of the project;
- the scope of the project;
- linkages with other projects or programmes;
- the team responsible for the programme or activity;
- a brief description of the type of data that will be collected.

Mapping data flows is a key step of any DPIA. In mapping the information flows of a particular programme or activity, the DPIA team should consider the following questions:

- What type of Personal Data is being collected, from whom and why?
- How will that data be used, stored and/or transferred?
- Who will have access to the Personal Data?
- What security measures are in place to protect the Personal Data?
- For how long will those data be retained or when will they be deleted? Have different layers of data retention been identified? This can include steps such as (1) storing data deemed sensitive for up to X days, (2) pseudonymizing data then storing the data for a longer time period, and finally (3) full deletion of the data.
- Will the data undergo any aggregation, Pseudonymization, or Anonymization to protect sensitive information?

5.2.4 CONSULTING STAKEHOLDERS

Identifying stakeholders is an important part of conducting a DPIA. Stakeholders include anyone who is interested in or affected by a data protection risk, possible processors, and Sub-Processors. Stakeholders may be internal and/or external to an organization. The need for and value of consulting external stakeholders will depend on how serious the Humanitarian Organization considers the risk to be. For a Humanitarian Organization, consulting stakeholders is a way to identify risks and/or solutions it may not have considered. It is also a way of raising awareness about data protection and privacy issues. The views of stakeholders should be taken into consideration in the DPIA report and recommendations. In order to ensure that the consultation is effective, stakeholders should be provided with sufficient information about the programme and given the opportunity to express their views. There are different ways to engage stakeholders, so the DPIA team should determine the most appropriate one depending on the programme or activity.

5.2.5 IDENTIFY RISKS

One way to identify risks is to create a spreadsheet listing privacy and data protection principles, threats to those principles, vulnerabilities (susceptibility to the threats), and risks arising from the threats and vulnerabilities. A threat without a vulnerability or vice versa is not a risk. A risk arises when a threat acts to exploit a vulnerability.

5.2.6 ASSESS THE RISKS

A data protection risk assessment addresses the likelihood or probability of a certain event and its consequences (i.e. impact). One can assess the risks by undertaking one or more of the following steps:

- Consult and deliberate with internal and/or external stakeholders to identify risks, threats and vulnerabilities.
- Evaluate the risks against agreed risk criteria.[3]
- Assess the risk in terms of likelihood and severity of impact.
- Assess against the necessity, suitability and proportionality tests.

ASSESSING THE SEVERITY AND LIKELIHOOD OF ANTICIPATED RISKS: PRECAUTIONARY PRINCIPLE

The criterion of **severity of impact** refers to the "magnitude of the risk or its impact if it materializes".[4] The determination thereof involves asking various questions including but not restricted to: how many people will it put at risk? What kinds of risks may it generate (e.g. threat to the life, security, dignity and rights of individuals; discrimination; economic harm; reputational harm; risk that an individual may not be in a position to exercise a data protection right; risk that Third Parties may gain access to data, etc.)? What are the profiles of people to whom such risks might be posed (in particular, whether this would include vulnerable people, i.e. those belonging to groups that are particularly susceptible to harm)?[5]

It should be noted that in certain Humanitarian Emergencies, such as situations of armed conflict or violence, there can be an assumption that risks can have particularly severe impacts if they materialize.

The **likelihood** of potential risks refers to the chances that the risk will materialize, and that it will materialize with the possible severity identified under the above

[3] For definitions of risk terms, see International Organization for Standardization (ISO), *ISO Guide 73:2009(En), risk management – vocabulary*, 2009: www.iso.org/obp/ui/#iso:std:iso:guide:73:ed-1:v1:en.

[4] Centre for Information Policy Leadership, *Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR: CIPL GDPR Interpretation and Implementation Project*, 21 December 2016: www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_risk_white_paper_21_december_2016.pdf.

[5] Wright, "Making Privacy Impact Assessment more effective".

analysis. In Humanitarian Emergencies it is often difficult to assess the likelihood of a risk materializing, particularly taking into consideration the limited availability of incident documentation. This will often mean that there will be limited or no documented evidence of a risk materializing. Lack of evidence should not be taken to mean that a risk is unlikely to materialize or to materialize with the possible level of severity identified. On the contrary, the identification of a risk with possible significant impact, combined with the inability to determine the likelihood thereof in the absence of evidence, should itself be an indicator of a high risk that deserves careful mitigation as part of the DPIA. The possible severity of the risk if it materializes, the nature, context and the purposes of the Processing activity in a humanitarian context should therefore inform the way in which the criterion of likelihood is interpreted and applied.

In this regard, it is suggested that the precautionary principle should be taken into account in the framework of a DPIA. The precautionary principle is a principle commonly used in other sectors (such as regulation of the environment, health and pharmaceuticals, etc.), informing decision-making in risk management,[6] which calls for particular caution where "a phenomenon, product or process may have a dangerous effect, identified by scientific and objective evaluation" but the available evidence "does not allow the risk to be determined with sufficient certainty".[7] While this does not involve examining in depth every hypothetical risk, the precautionary principle requires that in the face of situations in which "there is uncertainty with regards to the existence or extent of risks ... protective measures ... [should be taken] ... without having to wait until the reality and seriousness of those risks become fully apparent"[8].

5.2.7 IDENTIFY SOLUTIONS

This step involves developing strategies to eliminate, avoid, reduce or transfer the privacy risks. These strategies could include technical solutions, operational and/or organizational controls and/or communication strategies (e.g. to raise awareness). The following example has been provided by OCHA's Centre for Humanitarian Data, and is based on their work on this subject.[9]

[6] European Commission, Communication from the Commission on the precautionary principle, available at: op.europa.eu/en/publication-detail/-/publication/21676661-a79f-4153-b984-aeb28f07c80a/language-en.

[7] Ibid.

[8] The Court of Justice of the European Union, the Judgement of the Court of 5 May 1998. *United Kingdom of Great Britain and Northern Ireland v Commission of the European Communities* Case C-180/96 ECLI:EU:C:1998:192.

[9] See OCHA Center for Humanitarian Data, "An Introduction to Disclosure Risk Assessment", The Centre for Humanitarian Data (blog), accessed 23 March 2022: https://centre.humdata.org/learning-path/disclosure-risk-assessment-overview.

EXAMPLE: STATISTICAL DISCLOSURE CONTROL IN HUMANITARIAN DATA MANAGEMENT

Data from household surveys, needs assessments and other forms of microdata are critical to determining the needs and perspectives of people affected by crises. This type of data also presents unique risks that should be identified as part of a DPIA process and mitigated before data sharing. Even after names, phone numbers and other direct identifiers are removed from microdata, it may still be possible, through the combination of key variables such as location or ethnicity, to reidentify individuals in the data set or disclose confidential information.

Statistical Disclosure Control (SDC) refers to a set of statistical methods used to assess and reduce the risk of Reidentification or the disclosure of confidential information in order to facilitate the safe sharing of microdata.

The SDC process includes three steps:

(1) **Assess the risk of disclosure**: Assess the probability that disclosure could occur for individual respondents within a given data set by conducting a disclosure risk assessment.
(2) **Reduce the risk of disclosure**: Lower the disclosure risk by applying one or more Statistical Disclosure Control techniques.
(3) **Quantify information loss**: Quantify the information loss and assess the utility of the treated data in line with the original purpose for which they were collected.

Assess the risk of Reidentification

The first step in the SDC process is to conduct a disclosure risk assessment. This helps determine the likelihood of a disclosure taking place and the type of mitigation measures that might be necessary before sharing the data. Conducting a disclosure risk assessment requires selecting the indirect identifiers that are most likely to lead to Reidentification or the disclosure of confidential information, and using statistical methods to calculate different measures of risk.

Common key variables found in humanitarian microdata include age, gender, ethnicity, marital status, religion, income, location and other forms of geographic information. Depending on the context, almost any variable could be considered an indirect identifier (referred to as key variables). Selecting key variables thus requires an understanding of the context and data environment in which the data were produced.

Common risk measures include k-anonymity, l-diversity and individual and global disclosure risk. The Humanitarian Organization will need to set thresholds to be reached for each of the risk measures in order to share the data.

Reduce the risk of Reidentification

The second step in the SDC process is to reduce the disclosure risk to below the agreed threshold. There are two main strategies for reducing disclosure risk. The first is through non-perturbative methods, which reduce the detail in the data through the suppression or data generalization. For example, continuous key variables such as age or income may be recoded into age or income brackets. This process of replacing a data value with a less precise one can be an effective method for reducing disclosure risk while maintaining the analytical power of the data. The second set of methods, known as perturbative methods, aims to limit disclosure risk by altering data values in order to create uncertainty around the true value. Because these methods deliberately change data values, they should be applied with caution.

Quantifying information loss

The application of SDC will always lead to some information loss. In some cases, the information loss would be so high that the data lose their utility. Information loss must be evaluated with respect to the intended uses of the data. In the final step of the SDC process, the disclosure risk is reassessed to determine whether the application of SDC techniques has reduced the disclosure risk to an acceptable level and to evaluate the information loss. The goal of the SDC process is to find the optimal point at which the utility of the data for the intended users is maximized while the disclosure risk is reduced to an acceptable level.[10]

5.2.8 PROPOSE RECOMMENDATIONS

The DPIA team should produce a set of recommendations based on the outcome of the previous steps. Recommendations may include a set of solutions, changes at the organizational level and potentially changes to the Humanitarian Organization’s overall data protection strategy or that of the programme. A set of recommendations should be included in the DPIA report.

5.2.9 IMPLEMENT THE AGREED RECOMMENDATIONS

The DPIA team should prepare a written report on the considerations and findings of the DPIA. As organizations will need to conduct DPIAs regularly, the length and level of detail of a DPIA report will vary greatly. For example, if an organization is considering publication of Personal Data for research purposes, it should produce documentation reflecting the full details of its data protection impact analysis. Conversely, an organization that is deciding whether to switch from using one brand

[10] For more information on SDC in the humanitarian sector, consult the following resources: OCHA Center for Humanitarian Data, “An Introduction to Disclosure Risk Assessment“; OCHA Center for Humanitarian Data, “Statistical Disclosure Control”, The Centre for Humanitarian Data (blog), accessed 23 March 2022: https://centre.humdata.org/guidance-note-statistical-disclosure-control; “Statistical Disclosure Control for Microdata: A Practice Guide for SdcMicro”, SDC Practice Guide documentation, accessed 23 March 2022: https://sdcpractice.readthedocs.io/en/latest.

of word-processing software to another should consider data protection issues, given that the software will be used to process personal information, but a detailed DPIA may not be necessary (unless the software involves new data flows in a cloud environment).

In addition to documenting and implementing data protection decisions, a Humanitarian Organization should consider whether it would be useful for Data Subjects or to the public to understand the considerations underlying its data protection decision-making. Accordingly, the organization might then share the report (in whole or in part) with relevant stakeholders. Sharing the DPIA report may also be a way of raising awareness and inviting further comments or suggestions from stakeholders. However, in some cases, the Humanitarian Organization may decide against sharing the DPIA report if it contains sensitive information (e.g. for reasons of physical security, continuity of operations, access, etc.). In such cases, the Humanitarian Organization could consider sharing a summary of the DPIA report or a redacted version.

5.2.10 PROVIDE EXPERT REVIEW AND/OR AUDIT OF THE DPIA

Humanitarian Organizations should ensure that a data protection expert, such as the organization's Data Protection Officer (DPO) or their staff, reviews or audits the implementation of the DPIA. In the interest of an accurate audit, the DPIA report must contain a methodology section.

5.2.11 UPDATE THE DPIA IF THERE ARE CHANGES IN THE PROJECT

The Humanitarian Organization should update the DPIA if the activity covered by it changes in some significant way or if new data protection risks emerge.