Logical Outcomes

Responsible Program Data Policy[1]

October 13, 2017

Introduction

LogicalOutcomes is committed to using data responsibly in order to uphold the rights of the individuals, groups, and organizations with whom we work. Using data responsibly is not just an issue of technical security and encryption but also of protecting the rights of people to be counted and heard; ensuring their dignity, respect and privacy; enabling them to make informed decisions; and not be put at risk, when providing data.

LogicalOutcomes recognizes that people have rights with regards to the information related to them and that LogicalOutcomes has a responsibility to uphold those rights. The rights that form the backbone of this policy are:

A Right to be counted and heard
B Right to dignity and respect
C Right to make an informed decision
D Right to privacy
E Right to not be put at risk

This policy should not be seen as limiting or discouraging; rather, it is used to make it easier for data to positively impact the work that we and our partners do. Many of the words that we use in this document are defined at the end in the ‘glossary’.

In this policy, we consider ‘data’ to be the physical representation of information which can be communicated, interpreted, or processed by human beings or by automatic means. Data may be numerical, descriptive, audio, or visual[2]. The formal term for individuals from whom data is collected is “data subjects”[2]. In this policy, however, we use the term “participants” and expand the definition to include any group, cooperative, or other entity about which LogicalOutcomes collects or maintains program data.

This document describes the policy for how program data will be managed by LogicalOutcomes throughout the data lifecycle from planning to collection through to disposal. This data may pose

[1] *This policy is based closely on Oxfam’s 2015 Responsible Data Policy, posted on* http://policy-practice.oxfam.org.uk/publications/oxfam-responsible-program-data-policy-575950. Used by permission.
[2] *See glossary for definition*

varying degrees of risk to different stakeholders, including but not limited to the people who provide data, those that collect it, and LogicalOutcomes; because of this, this policy includes definitions and requirements for managing high-, medium-, and low-risk data.

This policy applies to all of LogicalOutcomes's programs and services, including projects where LogicalOutcomes is the data controller[3]. As described in the associated Information Security Policy, each LogicalOutcomes project will carry out a risk assessment regarding responsible data use, and will define on a case by case basis how we will deal with potential ethical issues related to that project. For example, in situations where we do not have direct control over the data (e.g., when data is provided to or by external organizations that are not our contractors), LogicalOutcomes will inform the external organizations when we have concerns that this policy is not being followed. LogicalOutcomes is responsible for ensuring that its contractors comply with the policy.

Recognizing that the policy applies to a rapidly-changing technological context, LogicalOutcomes has a responsibility to be aware of the implications of these changes for its work. A set of minimum standards and guidelines accompanies this policy to provide details on how to operationalize the requirements and will be updated periodically.

Policy Elements

A. Right to be counted and heard

In order to ensure the rights of vulnerable and marginalized populations, it is important that they are able to be counted and adequately represented as part of the information LogicalOutcomes collects and uses.

1. Where appropriate and possible, LogicalOutcomes will make every effort to ensure that vulnerable groups are represented in data collection, and that the resulting datasets can be disaggregated by gender and other relevant categories.
2. LogicalOutcomes will make all reasonable effort to ensure the inclusion of participants from marginalized populations in decisions regarding data collection and interpretation.
3. LogicalOutcomes will be transparent about limits to the accuracy of data collected, stored, and used, and will make efforts to keep information accurate, up-to-date and relevant.
4. LogicalOutcomes will appropriately analyze and use the information it collects in order to promote participants' right to be heard, especially within marginalized populations. This should include efforts to communicate findings to the surveyed population through the partners who use LogicalOutcomes's services, and to promote feedback loops to engage participants in decision-making.

[3] *See glossary for definition*

B. Right to dignity and respect

LogicalOutcomes will ensure that a participant’s personal dignity is maintained and respected in all phases of the data lifecycle.

5. Data will be collected in a culturally and contextually appropriate way.
6. It is necessary to be aware that there may be laws in addition to standards that regulate how LogicalOutcomes works with participants.
7. LogicalOutcomes will intentionally plan the data lifecycle in such a way as to not create an excessive burden on participants, carefully considering what data are needed and why; how it will be used; and how to collect only the minimum data required to accomplish programmatic aims.

C. Right to make an informed decision

Participants have the right to be fully informed in order to make a decision about their participation in any data activity.

8. LogicalOutcomes and its agents will gain informed and voluntary consent[4] before obtaining any information from participants. Participants will be informed about why the data is being collected, for how long, and who will have access to it. Data will only be used for the purpose it was collected for.
9. All participants are free to choose whether or not to give their consent, without inducement or negative consequences should they choose not to participate.
10. All participants and are free to withdraw their involvement in the data activity at any stage without any negative consequences, including their participation in LogicalOutcomes programs.
11. If the data process involves children under the age of 18, LogicalOutcomes will get both their, and their parents’ or guardians’ consent, except in circumstances when it is inappropriate to do so.
12. Consent will be based on a transparent and accurate assessment about the use of data and context. If the use or the context changes, LogicalOutcomes will re-evaluate whether re-consent is needed.

D. Right to privacy

LogicalOutcomes will protect a participant’s right to privacy in the treatment of their data and has a responsibility to protect the identity of those providing data, unless otherwise outlined and agreed to in the informed consent.

13. LogicalOutcomes will attempt to ensure that, when appropriate, the process of data collection is

[4] *See glossary for definition*

conducted in an environment where the privacy of the participant (or group of participants in the case of focus group discussions) is upheld.

14. LogicalOutcomes and its agents will not discuss or share in any form, information gathered from participants with any unauthorized (by LogicalOutcomes) persons.
15. LogicalOutcomes will minimize the collection of personal data, only collecting it when absolutely essential for the data activity.
16. LogicalOutcomes will ensure that Personally Identifiable Information (PII[5]) data will be kept in a manner that allows the PII to be protected.
17. LogicalOutcomes will ensure limited access to identified data records and store them securely, according to LogicalOutcomes's security policy.
18. While LogicalOutcomes encourages data sharing for transparency and accountability purposes, data which are shared openly must be anonymized, unless specific consent from the participant has been obtained, and it does not place participants at risk.

E. Right to not be put at risk

LogicalOutcomes will not put participants in any security risk as a result of its data activity. These individuals/ groups will be protected when acting as private citizens and not in their official capacity.

19. LogicalOutcomes will not collect non-essential data that could put participants at risk without justification and a clear process for managing and mitigating that risk.
20. LogicalOutcomes will take all reasonable measures to ensure that the process of data collection and the totality of the data lifecycle have no negative physical, psychological, or political consequences for the participants. LogicalOutcomes will maintain a security policy that meets international standards for health research, and will follow the associated security procedures.
21. LogicalOutcomes will mitigate risk to all its participants, but especially participants from vulnerable populations and groups or any participants engaged in sensitive topics/activities. Such topics must only be approached by personnel with the appropriate training and experience.

Governance and implementation of the Policy

The Board of Directors have the final responsibility for this policy. At a maximum of 2.5 years after the date of this policy's approval, or sooner if prompted by new regulations or events, the Board of Directors will commission a review of, and seek recommendations on, potential updates to the Responsible Program Data Policy. This will ensure that the policy remains current and relevant, given the changing context in which LogicalOutcomes operates. Following any updates to the policy, the set of minimum standards will also be reviewed and updated as required.

[5] *See glossary for definition*

Policy implementation is the joint responsibility of the LogicalOutcomes Board of Directors and the Executive Director. Every two years, the Board shall commission a review of compliance with the policy, and seek recommendations on potential updates to the Responsible Program Data Policy.

Glossary

Anonymous data
Any information relating to a natural person where the person cannot be identified, whether by the data controller or by any other person, taking account of all the means likely reasonably to be used either by the controller or by any other person to identify that individual. **Anonymized data** would therefore be anonymous data that previously referred to an identifiable person, but where that identification is no longer possible. [8]

Data
The physical representation of information in a manner suitable for communication, interpretation, or processing by human beings or by automatic means. Data may be numerical, descriptive or visual. [9]

Data collector
A person or organization collecting data on behalf of the data controller.

Data controller
A party who, according to domestic law, is competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf. [10]

Data management
The development, execution and supervision of plans, policies and practices that govern data processing. [11]

Data processing
Any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction. [12]

Data Risk, High
High risk data includes personal data, including any information that requires privacy and security protections, where data confidentiality is required by law, policy, or contractual obligations. It also includes data collected in programmatic, environmental, or political contexts where disclosure could cause direct harm to participants or put them at risk of adverse effects.

Data Risk, Medium
Medium risk data includes business or strategic data, or any non-confidential internal data that should not be shared publicly, where unauthorized disclosure could cause material loss to the organization or brand risk. Includes aggregated data.

Data Risk, Low
Includes public data and data collected in low risk contexts, or information and programmatic, environmental, or political contexts where disclosure would not involve any risk to participants (would cause no adverse effect).

Data subject
The formal term for any individual who is the subject of personal data. See **participant** for an expanded definition.[13] [14]

Informed and voluntary consent
A process for getting willing (non-coerced) permission to collect data of any kind based upon a clear appreciation and understanding of the facts, implications, and consequences of any engagement from participants.

Marginalized populations
Marginalized populations are those excluded from mainstream social, economic, cultural, or political life.[7]

Participants
A preferred term for data subjects, expanded to include any group, cooperative, or other entity with which LogicalOutcomes works that provide program data.

Personal data
Any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. [15]

Program
A set of strategically aligned, mutually reinforcing interventions—by LogicalOutcomes and others—that contributes to sustained, positive impact on poor people's lives. For the purposes of this document, Programs are understood to be those that are defined as such in the respective JCASs (OCS LogicalOutcomes Country Strategy).[16]

Project
A group of activities or interventions with a well-defined target group and period for implementation aiming at achieving a set of outputs or outcomes that will contribute to bring about changes in people lives. They are designed and implemented by one or several partners, which might include LogicalOutcomes itself, and are aligned through outputs, outcomes, or objectives to an overall program. [17]

Responsible data
The duty to ensure people's rights to consent, privacy, security and ownership around the information processes of collection, analysis, storage, presentation and reuse of data while respecting the values of transparency and openness. [18]

Transborder flows of personal data
Movements of personal data across national borders. [19]

[7] Source: SAGE Encyclopedia of Qualitative Research Methods, October 2017, http://sk.sagepub.com/reference/research/n252.xm

[8] *Source: European Data Protection Directive 94/46/EC*
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf

[9] *Source: UNESCAP – for Data types see section 1 on risk level*
http://www.unescap.org/sites/default/files/4.Generic%20Statistical%20Information%20Model%20%28GSIM%29-Common%20Reference%20Model.pdf

[10] *Source: OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*
http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

[11] *Adapted from: An Overview of Data Management*
http://www.aicpa.org/InterestAreas/InformationTechnology/Resources/BusinessIntelligence/DownloadableDocuments/Overvi e w_Data_Mgmt.pdf

[12] *Source: Ireland Data Protection Commissioner Guidance on EU Directive 95/46/EC*
http://www.dataprotection.ie/docs/EU-Directive-95-46-EC-Chapter-1/92.htm

[13] *Source: OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*

http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

[14] *Source: Ireland Data Protection Commissioner Definitions*

http://www.dataprotection.ie/docs/Key_Definitions-Territorial_Effect/63.htm

[15] *Source: Directive 95/46/EC of the European Parliament and of the Council*

https://ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Data_Protection/Detailed_specialist_guides/PERSONAL_DATA_FLOWCHART_V1_WITH_PREFACE001.ashx

[16] *Source: Oxfam Common Approach to MEL and Social Accountability (CAMSA)*

http://www.oxfam.org/sites/www.oxfam.org/files/file_attachments/story/oxfam-program-evaluation-policy-oct13_1_0.pdf

[17] *Source: Oxfam Common Approach to MEL and Social Accountability (CAMSA)*

http://www.oxfam.org/sites/www.oxfam.org/files/file_attachments/story/oxfam-program-evaluation-policy-oct13_1_0.pdf

[18] *Source: Responsible Data Forum working definition, September 2014.*

[19] *Source OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*

http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm