Photo credit: Kieran Doherty/Oxfam

GOING DIGITAL

Privacy and data security under GDPR for quantitative impact evaluation

The Going Digital journey continues with our fourth instalment, which follows (1) Using digital technology to conduct Oxfam's Effectiveness Reviews, (2) Using and sharing real-time data during fieldwork and (3) Improving data quality with digital data collection. In this paper, we discuss privacy and data security from a rights-based perspective, with a focus on quantitative impact evaluation. We situate protocols we have developed within the context of the General Data Protection Regulation (GDPR), sharing relevant debates along the way. We hope that this overview will be useful for translating principles and regulations into everyday impact evaluation practice.

OXFAM

1 INTRODUCTION

This paper seeks to outline practical guidance on protecting privacy and data security while doing quantitative impact evaluation in an increasingly digital world. Oxfam has an existing Responsible Program Data Policy (RDP), which clearly defines our guiding principles for data collection and management. With the recent introduction of the General Data Protection Regulation (GDPR), we must continue to review and reinforce the ways we address security and privacy when working with personal information.

As an organization, we fundamentally believe in the right to privacy, regardless of the letter of the law. We see GDPR as complementary to our work and our principles, but at the same time we have faced many practical dilemmas in our day-to-day activities. For example, we work globally, with colleagues and through partner organizations, in over 90 countries. GDPR restricts international transfers of data containing personal information. Our quantitative impact evaluation uses large sets of data that usually contain personal information (necessary for tracking and analysis). Can we still do impact evaluation if we cannot share data across borders, including into and out of the EU? What if we need to use data our partners have collected? How about working with consultants on impact evaluations?

Data collection presents a risk to the right to privacy of individuals who share their personal information with us, and we take this very seriously. In 'complying with GDPR', we must not lose sight of what ultimately matters – ensuring that we never use anyone's personal information in a way that they do not want or in a way that could cause them harm.

1.1 WHAT IS GDPR? WHY DOES IT MATTER?

The General Data Protection Regulation (GDPR) is an EU directive that sets broad rules for how personal information can be processed, including how it is collected, analysed, disclosed, moved and stored. GDPR is based on the third-generation fundamental right to privacy in the EU Charter. Essentially, it is about transparency with individuals, accountability of organizations, strong governance requirements, and an enhanced emphasis on implementing safeguards to protect individuals and their personal information based on risk. It enforces the rights of people to choose what data they share about themselves, with whom, and for what purpose. As of 25 May 2018, the regulation applies to all EU entities that handle personal data in the context of their EU activities, including where this involves the personal data of individuals outside the EU.

1.2 WHAT DOES OXFAM'S RESPONSIBLE DATA POLICY SAY ABOUT PRIVACY?

Oxfam's Responsible Program Data Policy (RDP) describes our rights-based approach to safeguarding personal information in our programmes globally. It is built on the right to be counted and heard; the right to dignity and respect; the right to make an informed decision; the right to privacy and the right not to be put at risk. The policy covers all our programme participants – individuals, groups, other entities – that share their personal information with us. The level of risk they face defines how their data must be managed. Our RDP affirms our commitment to upholding the right to privacy of those we work with and handling information they share with us in an ethical manner.

1.3 OVERVIEW OF THE PAPER

Our principles are clear, but what practical steps can we take to live these principles in our everyday work? This paper attempts to address this question by reviewing key terms, system-wide controls and privacy throughout the data lifecycle. We also share several example protocols in the appendices. All content is based on the procedures used by Oxfam GB's impact evaluation advisers. We recognize there are many other ways to approach privacy and GDPR. We share our ideas for your reference and openly welcome all feedback and suggestions to continually improve our practices.

2 GLOSSARY

Please note the following key definitions:

- **Personal data** – information that relates to an identifiable individual (i.e., identification), either independently or in combination with other available information (e.g., name(s), address, phone number, email address, identification number, geographic location).[1]
- **Data subject** – a person whose personal information is collected and processed; referred to in this document as a 'Participant'.
- **Data controller** – an organization that defines how and why data are collected and processed and manages that data.
- **Data processor** – an organization that handles data on behalf of a data controller, and under the controller's instruction; data processors will normally have no independent reason to hold and process the data; they do so only to perform a service for a data controller.
- **Encryption** – the process protecting data by making it unreadable to anyone who has not been given the key.
- **Pseudonymization** – the process of replacing direct identifiers (e.g., name, phone number) in a dataset with numbers, nicknames, or other codes; the information that links the direct identifiers to the pseudonyms is kept separately from the main dataset.
- **Anonymization** – the process of removing enough detail from a dataset so that 'by all means reasonably likely'[2] individual persons can no longer be identified.
- **Informed consent** – affirmative oral or written agreement from a data subject to gather their personal information, which requires providing enough detail about the purpose and fate of the data; the data subject freely and knowingly chooses to share the information for the intended purpose.
- **Data breach** – unauthorized access, transfer, processing, or deletion of personal information.

3 SYSTEM-WIDE CONTROLS

Our specific impact evaluation protocols are situated within the broader context of Oxfam GB's system-wide controls. These controls include things like employment, partnership and consultancy contracts and agreements, mandatory training and IT infrastructure. All Oxfam confederation members have agreed to use standard contractual clauses when transferring personal data between themselves designed to meet GDPR requirements. Additionally, each member has a Data Protection Policy and a Data Protection Focal Point.

For example, employment contracts have clauses on confidentiality and property use and transfer (including data). Partnership and consultancy contracts include comparable clauses. Additionally, all staff must agree with and sign Oxfam's code of conduct, which refers to our information security policy. Beyond agreeing and signing, staff also participate in mandatory code of conduct and GDPR trainings to understand and discuss how to interpret and apply the principles and requirements.

As individual impact evaluation advisers, the computers, servers and software we use are part of Oxfam GB's wider IT system, which has its own set of privacy protocols (outside this paper's scope). To quickly summarize, our computers are set up with device (disk) encryption, password protection and antivirus protection by default. Additional encryption software (such as AES Crypt) is installed to allow us to encrypt and decrypt individual files and folders, as needed. While encryption is not mandated by GDPR, it is a recommended way to reduce risk when handling personal information.

4 PRIVACY THROUGHOUT THE DATA LIFECYCLE

This section shares key considerations for each stage of the data lifecycle, from creation to destruction. Although we use wide range of evaluation approaches in our work, this paper focuses on quantitative methods. Household and individual surveys are at the core of our quantitative impact evaluations. Such surveys allow us to compile large datasets for statistical and econometric analysis, based on structured interviews with many respondents. This analysis helps us measure the impact of our programmes for accountability and learning purposes and help to increase our impact in the future.

Our aim is to build privacy by design throughout the data lifecycle, which requires balancing careful planning at each stage with practical risk assessment. Note that the steps do not always follow the same sequence (e.g., certain aspects of storage and transfer usually occur both before and after certain aspects of processing). Below we review the data lifecycle in the following stages:

1. Collection and transmission (initial gathering and uploading of data, e.g., to a server)
2. Storage and transfer (including on servers, laptops, drives and sharing data with others, including consultants, interns and research partners)
3. Processing (cleaning and analysis, including pseudonymization and anonymization)
4. Publication
5. Retention
6. Destruction

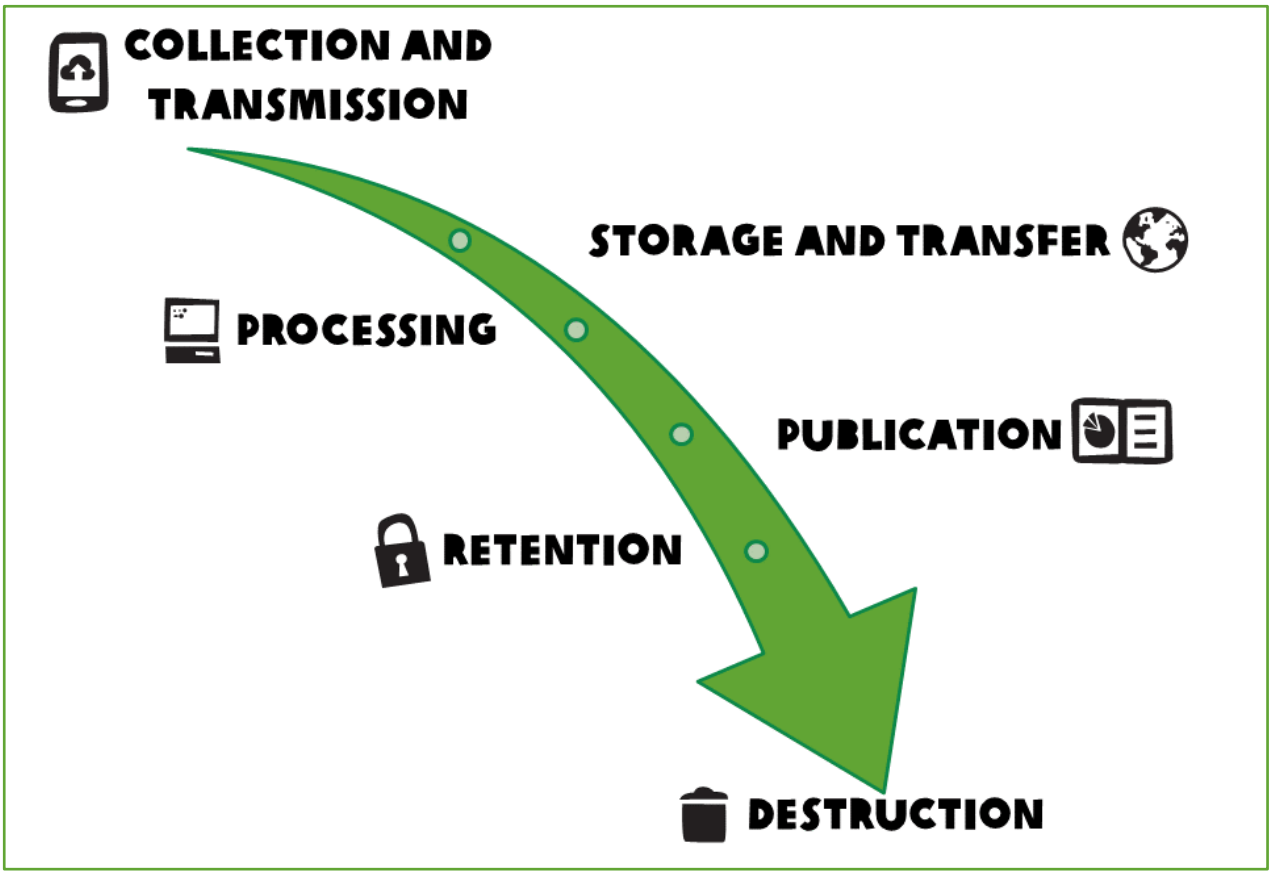

Figure 1. The stages of the data lifecycle reviewed in this paper

4.1 DATA COLLECTION AND TRANSMISSION

This paper is about 'Going Digital', so we focus on the digital aspects of data collection and transmission. We also include the interaction of paper-based data, as it is often used to complement or backup our digital tools. Collection and transmission involve interviewing people and making observations about them and their household, recording this information, and sending it to a centralized server (e.g., using SurveyCTO). The following are some key considerations to keep in mind during data collection and transmission:

- Data privacy knowledge of the data-collection team
- Informed consent
- Device and collection tool settings, including encryption
- Pseudonymization
- Handling of paper-based data

First, before we start collecting any personal data, we need to ensure the data collection team (e.g., enumerators and supervisors) are knowledgeable about data privacy matters. For example, we cover data privacy principles, regulations and protocols during enumerator training before data collection begins. For more detailed guidelines see Doing research with enumerators.

Next, we always obtain informed consent before collecting any data. From a research ethics perspective, informed consent means the respondent actively agrees to share their personal data with us based on a clear understanding of (1) the purpose and details of the research, (2) what is involved in participating, (3) the benefits and risks, (4) how their data will be used, stored, shared and destroyed, (5) steps that will be taken to assure ethical use of their data and (6) details of the

organization, including contact information to make a complaint and/or withdraw consent.[3] As far as GDPR is concerned, namely steps (4) and (6) are required.

Informed consent can be challenging in many contexts because of low literacy rates, lack of awareness of the right to privacy, variation in what privacy means and limited privacy protection at the national level. Bearing these challenges in mind, our standard informed consent protocol is as comprehensive as possible without being too long or complicated; an example is provided in Appendix 1. During the protocol, the enumerator reads the text out loud and gives each respondent a card or piece of paper with a summary and contact information or, even better, a proof of permission receipt. If possible, they can also show the respondent example publications (online or downloaded to the device) to give a better picture of how their data will be used. Consent is tracked by checking a box on the survey form. Instances of respondents who do not consent are also tracked (without recording any personal data).

In this paper, we share examples using SurveyCTO as our digital data-collection tool, although many features can also be applied across various digital data-collection tools. We have previously detailed our preference for SurveyCTO in our Going Digital series in Using digital technology to conduct Oxfam's Effectiveness Reviews and Improving data quality with digital data collection. In terms of data protection, our key requirements are (1) having servers hosted in the EU, (2) using encryption during transmission and (3) encrypting data from finalized questionnaires on mobile devices. Keep in mind that every digital data collection tool has its own unique data-protection features, which can vary based on the tool itself as well as the account type and account settings (e.g., even if encrypted transmission is possible, it is not necessarily by default).

Devices used for data collection should be set up in a consistent manner. When we own the devices, we follow the setup guidelines in Appendix 2. Our aim is to maximize battery life, ease navigation on the device itself and within applications, restrict usage of non-essential functions, enable tracking and location of devices, and maximize security of devices in case of theft or loss. By default, we use Android devices, which are widely available, compatible with the applications we use, and relatively affordable. Note that devices owned by others (partners, consultants, enumerators) are governed by a personal data processing agreement (see Appendix 3).

While encryption is not explicitly mandated by GDPR, it is recommended in most instances to reduce risk when handling personal data. At a minimum, all devices should be password protected as a first layer of defence, and survey forms containing personal data should be encrypted during transmission. Devices should also be encrypted (disk encryption) for an added layer of defence, other than in contexts where doing so would put programme staff or participants at risk.[4]

Pseudonymization is also not mandated, but again it can help with privacy protection. In practice, it means keeping directly identifiable information (names, phone numbers, etc.) separate from the rest of the data. For example, a list of respondent names with randomly assigned household identification numbers (the key) is kept separately (and securely). Then, only the random household identification number is used with the survey, making it difficult to identify who the respondents are without the key.

To complement pseudonymization, where the risk outweighs the need, we might also record nicknames rather than full legal names, avoid taking phone numbers, emails or detailed locations (e.g., GPS coordinates) and remove questions on sensitive topics (e.g., gender-based violence, political participation). We need to be extra cautious in countries with laws that restrict encryption. In the most severe cases, if the level of risk is too high to collect any personal information, the only options are to collect limited, anonymous information, rely on alternative data sources, or cancel the evaluation altogether.

Finally, even in the digital age, paper-based data collection is often still used for certain types of information alongside digital data collection (e.g., paper copies of survey forms used as backup in

case of issues with a device, and paper tracking lists of respondents to interview together with a survey form in SurveyCTO). Paper copies of personal data must also be handled securely – with a system of pseudonymization, a clear chain of custody while in transit (e.g., with enumerators in the field), and be carried in a way that prevents others from seeing the contents (in a folder, bag, etc.)

If the paper-based data are made digital at any point, data entry should be done in compliance with a personal data processing agreement (see Appendix 3).

4.2 DATA STORAGE AND TRANSFER

The next stage in the data lifecycle is storage and transfer. Data from digital data-collection tools (e.g., SurveyCTO) are stored on a server (with its own set of data security protocols). To access these data, we download it to an Oxfam GB computer. Because we use form encryption for data transmission, only those with access credentials to our server *and* the private encryption key can download the data. Once it is on our computers/servers, it is protected by device (disk) encryption, at a minimum. Data on paper should be stored in a locked drawer with controlled access only for those who are approved to use the data.

If we are doing the analysis ourselves, then we can proceed to the next stage in the data lifecycle (data processing). However, as we alluded to in the introduction to this paper, one of our biggest dilemmas involves data transfer (across national borders, into the EU and then out again). Indeed, at a certain point it seemed that GDPR's stance on international transfers meant that impact evaluation using personal data was no longer feasible. We think the crux of the issue is this – do people consent (in an informed way) to their personal data being shared with Oxfam GB and its partners, which means it will be transferred internationally?

To address this issue for new data collection, we have added international transfers (in basic terms) to our informed consent protocol by stating that personal information will be shared with Oxfam and providing a list of countries. We also clarify that the other information they share (non-personal data) will be shared more broadly, with partners and through publications, but in an anonymous way.

While we think that we have an acceptable solution for new data collection, we often need to use existing personal data (e.g., lists of programme participants) to contact respondents to request interviews in the first place (using random sampling methods). Sometimes Oxfam GB has these data, which is more straightforward, but these lists are frequently maintained by our partner organizations. Ideally, our partners' informed consent protocol explicitly includes sharing the data with Oxfam. However, if that is not the case for any reason, we must provide information to the individuals about the fact that we have their data and what we will do with it. This notification must happen either (1) within a reasonable period of time after obtaining the data (or at most a month) or (2) during the first communication if the data are to be used for communicating with them.

Complying with this notification requirement could be extremely challenging in many contexts, especially considering the random sampling methods we typically use for quantitative impact evaluation. One approach that avoids this requirement is asking the partner to carry out sampling 'pseudonymously'. This approach can use a list of participant data with direct identifiers removed or we can ask the partner for a list of identification numbers only.

However, in the worst case, if our partner shares a list of 10,000 programme participants with us and we randomly select 1,000 to invite for an interview, we might consider that GDPR requires us to notify the other 9,000 people that we have their personal data but do not plan to do anything with it. Notifying those 9,000 people could involve sending out team members to wander around communities across the country looking for them, at an enormous (and infeasible) expense. In carrying out the sampling, we process data for a short time period and in a way that poses minimal risk. The primary purpose is

analysis designed to subsequently delete these data shortly after obtaining it. Notifying affected people of this use might cause more disruption than any agency it enables. If no other options are available, and in this circumstance, we may in the worst case choose to work with these data while considering that additional notification would be disproportionate under these circumstances.

Finally, when we need to transfer digital data that we already have in storage externally (e.g., to a consultant or research partner, with a contract or agreement already in place), we first remove any non-essential information (i.e., not needed to carry out the contract/analysis work). Next, we ensure at least one layer of encryption for all data by sharing files via an encrypted service (e.g., Box[5]). We think this is sufficient for low-risk data, such as a list of names and which years they participated in the project under analysis. However, for more sensitive data – a full household roster, details of participation in political activities – we add a second layer of encryption to individual files or folders (e.g., using AES Crypt). As an extra precaution, the files are deleted from the encrypted service once the receiving party has finished the download.

4.3 DATA PROCESSING

Moving on to data processing – cleaning and analysis, which may also include pseudonymization and anonymization. It is important to maintain a record of our data processing activities for every impact evaluation, including data collection and analysis methods and tools (e.g., pre-analysis plans, survey forms, Stata do-files, codebooks), as well as reports and publications resulting from the data.

As with data collection, pseudonymization should be used during data processing whenever possible. This should be the first step of data processing if data were not collected in a pseudonymized form. Then the original data file can be stored in a separate (secure) location. The rest of the data processing is done using the pseudonymized dataset.

While pseudonymization provides added privacy protection, it does not necessarily equate to anonymization – that depends on what else is in the dataset. Anonymization is possible for much of the data we work with, considering that re-identification would not be possible 'by all means reasonably likely'.[6] Based on the ICO Anonymization Code, we have developed an anonymization protocol (see Appendix 4) to use if it is possible to anonymize a dataset.

In some cases, anonymization may not be possible, particularly in contexts where digital footprints are already large. Therefore, it is important to consider the data environment including, but not limited to, whether other data exists that could lead to re-identification and the relevant governance processes that control how data are managed in that environment.

4.4 DATA PUBLICATION

Beyond sharing the results of our impact evaluation internally for learning and to improve our own programmes, we also publish and share the results externally as much as possible. We want to be transparent about our successes and failures. In addition to publishing evaluation reports, we also aim to share full (anonymized) datasets when possible (e.g., via the UK Data Service).

The publication of any information, whether in a report or a dataset, must follow the same rule as our anonymization protocol – re-identification would not be possible 'by all means reasonably likely'. When we report information in any publication it should be aggregate-level; we also pay special attention to any potentially revealing combinations of specific regions and minority groups to maintain privacy and protect the people with whom and for whom we work.

4.5 DATA RETENTION

The next stage in the lifecycle is about what we do with data once the initial analysis is done and the main impact evaluation report is published. Personal data, including pseudonymized datasets, must be destroyed once no longer needed for the purpose for which consent was obtained,[7] with a maximum retention period of five years. Data retention beyond this five-year period must be approved by the Head of Programme Quality.

Whether we can keep personal data beyond the end of an impact evaluation depends on the informed consent protocol – did the respondents consent to share information for a specific evaluation or for research (more generally)? Did they consent to being contacted for a follow-up survey and are we planning one? It may be that the personal data needs to be deleted (as described in the next section); it may be that it can be retained for a specific period of time (e.g., five years). Note that anonymized data, particularly when used for statistical or research purposes, can be retained indefinitely. Once properly anonymized, our data no longer contains personal information and can be used and shared for further research.

Oxfam GB has a registry of the data we control and any relevant processing agreements. Our impact evaluation data, along with all monitoring and evaluation data, is represented as programme data about participants. Within our impact evaluation team, we keep a more detailed list to track all datasets we have containing personal data. The list includes a description of the data (including types of personal information and informed consent), an explanation of processing and retention plans.

4.6 DATA DESTRUCTION

At the end of the data lifecycle, data usually need to be destroyed. When personal data are deleted, we want to ensure that we destroy all copies and versions. Electronic data are deleted using a secure erasure programme (such as Eraser) that repeatedly overwrites files until the original data could not be retrieved forensically. Note that the recycle/trash bin should be emptied immediately before running a secure erasure programme. Also, before a device leaves the possession of the organization or individual (for destruction or sale), the hard disk should be completely erased using a secure erasure program. Paper data must be destroyed by shredding, preferably using a cross-cut shredder, once no longer needed.

4 CLOSING THOUGHTS

Having shared our principles, the privacy and GDPR dilemmas we have faced, and some of our key protocols, where do we go from here? We hope that this overview will be useful for translating principles and regulations into everyday impact evaluation practice, building on a rights-based approach. Along these lines, we cannot close without mentioning that we have been inspired by related guidance shared by others, especially Girl Effect. From here, we aim to continue learning and improving our practices going forward.

This paper has focused on quantitative impact evaluation, but we also use qualitative evaluation methods (and mixed/combined methods), across the Oxfam confederation. As a next step, we are preparing complementary guidance looking at additional types of data. Digital data collection of qualitative data – descriptive stories, audio recordings, video diaries – shares some of the same dilemmas, but also presents new ones. How we face these dilemmas for qualitative data, privacy and GDPR is another story.

APPENDIX 1: EXAMPLE INFORMED CONSENT PROTOCOL

Good morning/afternoon. My name is _____. I'm doing a survey on behalf of Oxfam GB. The purpose is to learn more about your experience with [topic of evaluation]. The information you share will be used to evaluate [a future/ongoing/former project] and hopefully improve other programmes in the future. No direct support or benefits will come to you or your household based on this survey; any information you share will only be used for research and evaluation purposes.

Your personal data will only be shared with Oxfam and [name of data collection consultant] in [country name(s)] to complete this and related studies. When the studies are done within [timeframe of studies], your personal data will be deleted. An anonymous version of the information you share with us will kept longer, but will only be shared in ways that do not allow anyone to know who you are. We will take all possible steps within our control to maintain your privacy, but cannot eliminate all risk.

Participation in the survey is optional, and you are free to not answer any of the questions. After the survey, you can remove your information or file a complaint at any time using the contact details I have given you [give contact card].

Are you willing to spend approximately _____ minutes/hour(s) with us for an interview?

☐Yes ☐ No

Would you also be willing to be contacted later for a follow-up survey?

☐Yes ☐ No

(If yes, for a follow-up survey) please share your phone number: _____

IF APPLICABLE: If you want to receive an electronic copy of the report produced from this survey please share your email address, which we will only use to send you the report:

_____

APPENDIX 2: EXAMPLE OXFAM DEVICE SETUP GUIDELINES

This document advises settings to use with mobile devices during digital data collection to:

- Maximize battery life
- Ease navigation on the device itself and within applications
- Restrict usage of non-essential functions
- Enable tracking and location of devices
- Maximize security of devices in case of theft or loss

Device Setup Checklist

☐ Add IMEI numbers and login details to a device asset log

☐ Set up Google accounts and add to the device asset log

☐ Encrypt the device (in the Settings menu, under Security)

☐ Enable a screen unlock password (six digits long)

☐ Apply a robust Oxfam logo sticker (for identification)

☐ Add an Oxfam wallpaper and screensaver

☐ Enable app settings from unknown sources

☐ 'Clean up' the home screen by removing all shortcuts

☐ Turn the device to silent mode

☐ Check that the date and time are correct (important if no SIM card)

☐ Adjust the time-out setting or 'sleep' setting to 2 minutes

☐ Fix the screen rotation (so that it does not rotate)

☐ Turn off any LED buttons

☐ Add the battery percentage setting

☐ Adjust brightness settings, as appropriate (set to dimmer or automatic, if possible)

☐ Install Meraki and enrol the phones (to allow remote data wiping in case of loss/theft)

☐ Install SurveyCTO, configure settings and add a shortcut to the phone dock

☐ Install Kids Place, configure settings and add a shortcut to the phone dock

Installing SurveyCTO

1. Add enumerator usernames and passwords via the SurveyCTO server.
2. On each device, log in with the password, which should be in the device asset log.
3. Install the 'SurveyCTO Collect' app from Google Play; select 'OK' to all messages.
4. If the device is set to block installation of apps obtained from unknown sources, go to Settings → Security → Allow installation of apps from unknown sources.

5. Launch the SurveyCTO app. Using the three dots in the top right corner of the screen, select ‘General Settings’.
6. Enter the server name along with the enumerator username and password.
7. Select the setting ‘Auto send with Wi-Fi’.
8. Change Navigation to the option of ‘Use forward/backward buttons’.
9. Change the text font size to ‘small’ if using a mobile device with a small screen.
10. De-select ‘Default to finalized’.
11. Go back to the three dots in the top right corner and select ‘Admin Settings’ and scroll to ‘User can access change settings items’; de-select all options.
12. Again within ‘Admin Settings’, go to the section called ‘user can access main menu items’ and de-select ‘get blank form’ and ‘delete saved form’. If enumerators are responsible for uploading forms ignore this instruction.
13. Finally, set an ‘Admin password’ within ‘Admin settings’.

Installing Kids Place

1. Install the ‘Kids Place’ app from Google Play; accept the licence agreement.
2. Set a password and add it to the device asset log.
3. Set the recovery email to the relevant person.
4. Set a hint for the password.
5. Select ‘Lock Home Button’, tap on the ‘Kids Place’ option and choose ‘Always’.
6. Select apps allowed by Kids Place – namely SurveyCTO;
    a. If enumerators need to make calculations, also select the Calculator app;
    b. If enumerators are responsible for uploading forms each evening, also select the Settings app;
    c. If going through a portal or entering a password on an internet browser is common, also select a web browser app.
7. Select the three dots in the top right corner and select ‘Settings’.
    a. Ensure the following are **selected**:
    i. Lock Home button
    ii. Auto restart apps
    iii. Block marketplace
    iv. Airplane mode (if enumerators are not uploading forms)
    v. Start on device reboot – select ‘yes’ to the prompt
    vi. Block unapproved apps
    vii. Lock device volume control
    viii. Lock notification bar
    b. Ensure the following are **de-selected**:
    ix. Allow Internet Connection (If enumerators are not uploading forms)
    x. Allow phone calls
    xi. Keep home screen on
    xii. Allow kids to switch users
    xiii. Display Plugins Shortcuts

xiv. Icon stretching

xv. Change Application Title

xvi. Display status bar

8. Exit Kids Place by selecting the door icon in the middle at the top of the screen

APPENDIX 3: EXAMPLE PERSONAL DATA PROCESSING AGREEMENT

This agreement is dated [DATE]

Between:

(a) [Oxfam] **[Oxfam]**

(b) [name of Partner, Consultant, Intern] **[Partner]**

Background:

1. The Partner has agreed to provide services to Oxfam under [*an agreement/MoU dated DATE*] (**Head Agreement**)

2. The Head Agreement may require the Partner to process Personal Data on behalf of Oxfam.

3. The parties agree that the processing of such Personal Data will be subject to the terms and conditions in this agreement.

1. Definitions

In this Agreement, unless the context otherwise requires:

'Data Protection Laws' means all legislation and regulatory requirements in force from time to time which apply to a party relating to the use of Personal Data or privacy.

'Personal Data' means information related to an identified or identifiable individual that is processed by the Partner on behalf of Oxfam, as detailed in Appendix 1.

'Process' means collect, record, structure, store, adapt, alter, retrieve, access, consult, use, disclose, transmit, erase, restrict or destroy, and 'processing' is to be construed accordingly.

'**Regulator**' means any regulator from time to time whose consent, approval or authority is required to lawfully process Personal Data in accordance with this Agreement.

2. Processing of Personal Data

2.1 The Partner shall process the Personal Data only to the extent, and in such manner as is:

2.1.1 necessary for the purposes of providing the services under the Head Agreement and in accordance with Oxfam's written instructions from time to time; or

2.1.2 required by applicable law (but only after notifying Oxfam of the legal requirement before processing).

3. Personnel Access to Personal Data

3.1 The Partner shall ensure that:

3.1.1 access to the Personal Data is limited to those personnel who need access to the data to provide the services under the Head Agreement.

3.1.2 all its personnel who have access to the Personal Data under paragraph 3.1.1 are under an obligation of confidentiality in relation to the data and are trained to process the data in accordance with the Partner's obligations under this Agreement and applicable data protection laws.

4. Information Security

4.1 The Partner shall have in place at all times appropriate technical and organizational measures against the unauthorized or unlawful processing of the Personal Data and against the accidental loss or destruction of, or damage to, the Personal Data having regard to:

4.1.1 the harm that might result from such unauthorized or unlawful processing or accidental loss, destruction or damage; and

4.1.2 the nature of the data to be protected.

4.2 Without limitation to paragraph 4.1:

4.2.1 the Partner shall, in the performance of the services, process all Personal Data either on an Oxfam laptop (preferable) or on an encrypted a password-protected and encrypted laptop, in which case all Personal Data must be deleted from this device using a secure erasure program immediately on termination of the Services for whatever reason. Before the device leaves the possession of the Partner (for destruction, recycling, sale, etc.), the hard disk must be completely erased using a secure erasure program.

4.2.2 the Partner shall, wherever possible, utilize anonymization or pseudonymization when processing Personal Data that is identified in Appendix 1 as special category personal data or data related to criminal offences.

4.2.3 [*detail any other specific IS requirements on Partner*]

5. Personal Data Breach

5.1 The Partner shall notify Oxfam as soon as reasonably practicable, but in any event within 24 hours, if it becomes aware of any breach of security leading to:

(a) unauthorized disclosure or access to the Personal Data; or

(b) destruction, loss, or alteration, of the Personal Data.

5.2 The Partner shall, in the event of a data breach described in 5.1:

5.2.1 take reasonable and prompt steps to mitigate the effects and minimize any damage from the breach;

5.2.2 promptly comply with any instruction provided by, and cooperate with, Oxfam in relation to the breach;

5.2.3 not inform any third party of the breach without Oxfam's prior consent, except where required by law.

6. Communications from Data Subjects or Regulators

6.1 The Partner shall:

6.1.1 promptly notify Oxfam if it receives any complaint, notice or communication from an individual or Regulator which relates to the processing of Personal Data regulated by this Agreement;

6.1.2 not respond to such communication without Oxfam's written consent unless required by applicable law;

6.1.3 provide such assistance as Oxfam may reasonably require, to enable Oxfam to respond to any complaint, notice or communication described in 6.1.1.

7. Sub-Processing of Personal Data

7.1 The Partner shall not disclose the Personal Data to any third party for processing ('sub-processor') without the prior written consent of Oxfam.

7.2 Where Oxfam authorizes disclosure of the Personal Data to a sub-processor, the Partner must ensure that it has a written agreement in place with the sub-processor on terms no less protective than provided in this Agreement.

7.3 The grant of any approval by Oxfam under this paragraph in respect of the disclosure of Personal Data to any sub-processor will not relieve the Partner from any liability under this Agreement and the Partner will remain responsible to Oxfam for the sub-processor's performance of its obligations.

8. International Transfers of Data

8.1 The Partner may not transfer the Personal Data outside of the country in which the services under the Head Agreement are being provided without Oxfam's prior written consent. Where that consent is given it may be conditional on such transfer or export being done in accordance with specific safeguards required under applicable Data Protection Laws.

8.2 Notwithstanding clause 8.1, the Partner may transfer the Personal Data to any jurisdiction in so far as it is:

(a) required to do so by applicable law; and

(b) having notified Oxfam of the legal requirement prior to transfer, unless such notification is prohibited for reasons of public interest.

9. Compliance

9.1 The Partner shall, upon reasonable request, provide evidence to Oxfam of the technical and organizational measures implemented by the Partner to comply with its obligations under this Agreement and applicable Data Protection Laws, including but not limited to allowing for audits, provided that the Partner shall not be required to disclose to Oxfam any information which is confidential or of a commercially sensitive nature.

9.2 The Partner shall inform Oxfam immediately if, in its opinion, compliance with any instruction of Oxfam would infringe applicable Data Protection Laws or if any law applicable to the Partner will require it to breach its obligations under this Agreement.

9.3 The Partner shall assist Oxfam, on reasonable request, with the conduct of any data protection impact assessment or consultation with Regulators in relation to Personal Data processing regulated by this Agreement.

10. Term and Termination

10.1 This Agreement will remain in force and effect so long as:

10.1.1 the Head Agreement remains in effect; or

10.1.2 the Partner retains any Personal Data regulated by this Agreement in its possession or control.

10.2 Any provision of this Agreement that expressly or by implication should come into or continue in force on or after termination of the Head Agreement in order to protect Personal Data will remain in full force and effect.

10.3 The Partner's failure to comply with the terms of this Agreement is a material breach of the Head Agreement and, in such an event, Oxfam may terminate the Head Agreement, or such part of the Head Agreement as authorizes the processing of Personal Data, effective immediately on written notice to the Partner without further liability of obligation.

11. Data Return and Destruction

11.1 On termination of the Head Agreement for any reason, the Partner shall, at the choice of Oxfam:

11.1.1 Transfer all of the Personal Data processed on behalf of Oxfam to Oxfam; or

11.1.2 Delete all Personal Data processed on behalf of Oxfam

unless retention is required under applicable law.

11.2 If any law or regulatory requirement requires the Partner to retain any Personal Data under 11.1, it will notify Oxfam of that retention requirement, giving details of the materials that it must retain, and the timeline for destruction once the retention requirement ends.

12. Conflict

12.1 If there is an inconsistency between the provisions of this Agreement and the provisions of the Head Agreement, the provisions of this agreement shall prevail.

13. Governing Law

13.1 This agreement and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) shall be governed by and construed in accordance with the law of [*INSERT*]

14. Jurisdiction

14.1 This Agreement shall be governed by and construed in accordance with the law of [*INSERT*] and the parties hereby submit for all purposes in connection with this Agreement to the non-exclusive jurisdiction of the courts of [*INSERT*].

Appendix 1

SUMMARY OF DATA PROCESSING

Subject matter of the processing	*Insert description of the services that involve the processing of personal data*
Duration	During the term of the Head Agreement and to deliver up to Oxfam and then arrange deletion of any copies held by the Partner on termination.
Nature and Purpose of the processing	The Personal Data will be processed by the Partner to perform the services under the Head Agreement.
Types of Personal Data processed	*e.g. categories – names, email addresses, photos, etc.* *The Personal Data will not include special category data.*
Categories of Data Subjects in relation to Personal Data processed	*[provide details] e.g. Oxfam staff; programme participants, etc.*

APPENDIX 4: EXAMPLE PSEUDONYMIZATION AND ANONYMIZATION PROTOCOL

The steps for **pseudonymization** of datasets are as follows:

1. **Delete** all information that directly identifies someone
   a. Names of respondents, other household members, enumerators, etc.
   b. Contact details (e.g., phone numbers, emails)
   c. Exact location (e.g., addresses, GPS coordinates)
   d. Ensure that all unused value labels are **deleted**

Continuing from the steps above, further steps for **anonymization** of datasets are as follows:

2. **Delete** unique identification numbers (e.g., household IDs)
3. **Delete** all open-ended responses containing details that could be used to identify someone
   a. Reasons why a respondent could not be located
   b. 'Other' (specify) variables that contain personal and/or detailed descriptions
   c. Stories or explanations that contain personal and/or detailed descriptions
4. **Delete** all information of a sensitive nature (e.g., gender-based violence)
5. **Recode/Delete** information that could be used in combination to uniquely identify someone
   a. Geographic information below the regional level (e.g., village name, school name)
      i. **Randomly encode** variables, only if details that could be used to recreate the original variable are not published (e.g., number of respondents by village name)
      ii. **Delete** variables if detailed information that could be used to recreate the original variable has been or ever will be published
   b. **Delete** information related to religion, ethnicity, political affiliation, etc. (any identifying information of a sensitive nature) if any group contains less than 5% of the observations ('Other', when unspecified, is an exception to this rule)
   c. **Recode** age information into age ranges (e.g., 0–4, 5–9 . . . 95–99, 100+)
   d. **Recode** information such as household size into ranges for values below the 1st percentile and above the 99th percentile (e.g., Less than 3, 3, 4 . . . 9, 10, More than 10)
6. Ensure that all unused value labels are **deleted**
7. **Request review and sign off** for the anonymization by another member of the team. This sign off should be noted in the data processing record (e.g., in a README file).

REFERENCES

1. Croome, A. & Mager, F. (2018). *Doing Research with Enumerators.* Oxford: Oxfam GB. https://policy-practice.oxfam.org.uk/publications/doing-research-with-enumerators-620574
2. European Commission (2019). *Data protection: Rules for the protection of personal data inside and outside the EU.* https://ec.europa.eu/info/law/law-topic/data-protection_en
3. Global Partners Digital (2019). *World map of encryption laws and policies.* https://www.gp-digital.org/world-map-of-encryption/
4. Hastie, R. & O'Donnell, A. (2017). *Responsible Data Management training pack.* Oxford: Oxfam GB. https://policy-practice.oxfam.org.uk/publications/responsible-data-management-training-pack-620235
5. Information Commissioner's Office (ICO) (2012). *Anonymisation: managing data protection risk code of practice.* https://ico.org.uk/media/1061/anonymisation-code.pdf
6. Lombardini, S., Pretari, A. & Tomkys Valteri, E. (2018). *Going Digital: Improving data quality with digital data collection.* https://policy-practice.oxfam.org.uk/publications/going-digital-improving-data-quality-with-digital-data-collection-620522
7. Lombardini, S. & Tomkys Valteri, E. (2017). *Going Digital: Using and sharing real-time data during fieldwork.* Oxford: Oxfam GB. https://policy-practice.oxfam.org.uk/publications/going-digital-using-and-sharing-real-time-data-during-fieldwork-620432
8. Mourby, M., Mackey, E., Elliot, M., Gowans, H., Wallace, S.E., Bell, J. Smith, H., Aidinlis, S. & Kaye, J. (2018). Are 'pseudonymised' data always personal data? Implications of the GDPR for administrative data research in the UK. *Computer Law & Security Review, 34*(2), 222–233.
9. Oxfam International (2015). *Oxfam Responsible Program Data Policy.* Oxfam International. https://policy-practice.oxfam.org.uk/publications/oxfam-responsible-program-data-policy-575950
10. Raftree, l. (2018). *Digital safeguarding tips and guidance.* Girl Effect. https://www.girleffect.org/stories/digital-safeguarding/
11. Tomkys Valteri, E. & Lombardini, S. (2015). *Going Digital: Using digital technology to conduct Oxfam's Effectiveness Reviews.* Oxford: Oxfam GB. https://policy-practice.oxfam.org.uk/publications/going-digital-using-digital-technology-to-conduct-oxfams-effectiveness-reviews-578816

NOTES

1 Definition of personal data according to the European Commission in reference to GDPR: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en

2 See GDPR regulation clause 26 (p. 5)

3 https://www.ukdataservice.ac.uk/manage-data/legal-ethical/consent-data-sharing/consent-forms and https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/what-information-must-be-given-individuals-whose-data-collected_en

4 https://www.gp-digital.org/world-map-of-encryption/

5 https://community.box.com/t5/How-to-Guides-for-Account/Data-Encryption-at-Box/ta-p/32.

6 https://ico.org.uk/media/1061/anonymisation-code.pdf

7 See GDPR Article 5(e).

This publication was written by Jaynie Vonk. It is part of a series of papers and reports written to inform public debate on development and humanitarian policy issues.

For further information on the issues raised in this publication please email jwhinnery1@oxfam.org.uk.

The information in this publication is correct at the time of going to press.

Published by Oxfam GB for Oxfam International under
ISBN 978-1-78748-521-1 in October 2019. DOI: 10.21201/2019.5211
Oxfam GB, Oxfam House, John Smith Drive, Cowley, Oxford, OX4 2JY, UK.

OXFAM

Oxfam is an international confederation of 19 organizations networked together in more than 90 countries, as part of a global movement for change, to build a future free from the injustice of poverty. Please write to any of the agencies for further information, or visit www.oxfam.org.

Oxfam America (www.oxfamamerica.org)

Oxfam Australia (www.oxfam.org.au)

Oxfam-in-Belgium (www.oxfamsol.be)

Oxfam Brasil (www.oxfam.org.br)

Oxfam Canada (www.oxfam.ca)

Oxfam France (www.oxfamfrance.org)

Oxfam Germany (www.oxfam.de)

Oxfam GB (www.oxfam.org.uk)

Oxfam Hong Kong (www.oxfam.org.hk)

Oxfam IBIS (Denmark) (http://oxfamibis.dk/)

Oxfam India (www.oxfamindia.org)

Oxfam Intermón (Spain) (www.oxfamintermon.org)

Oxfam Ireland (www.oxfamireland.org)

Oxfam Italy (www.oxfamitalia.org)

Oxfam Mexico (www.oxfammexico.org)

Oxfam New Zealand (www.oxfam.org.nz)

Oxfam Novib (Netherlands) (www.oxfamnovib.nl)

Oxfam Québec (www.oxfam.qc.ca)

Oxfam South Africa (http://www.oxfam.org.za/)

Observers
KEDV (Oxfam Turkey)