Responsible Data Management Guidelines

Role of Data in GFEMS' Work

Limited and inconsistent data collection and availability of useful data are major barriers to informing and implementing strategies that effectively leverage resources and sustainably disrupt modern slavery. GFEMS is designed to respond to this constraint and is committed to building the evidence base and making data-informed programming decisions. The Fund will work to ensure robust measurement of prevalence and intervention effectiveness across our portfolio. Data collection, analysis, storage, sharing, and dissemination of research and knowledge products therefore play a vital part in the operations of GFEMS.

Importance of Responsible Use of Data

GFEMS respects the rights of individuals and dignity of research participants through the entire data processing lifecycle. Data safeguarding and the principle of "do no harm" is critical to our work. The Fund works through subrecipients, third party research contractors, and consultants (collectively referred to as 'GFEMS Partners' or 'Partners' in this document) to collect, analyze, and share data for research purposes. This is done in an effort to better understand the prevalence of modern slavery and to develop solutions to eliminate it. In doing so we hold ourselves and our Partners to high standards in handling data with integrity and protecting individuals right to make an informed decision about how and if their data is used, their right to privacy, and their right not to be put at risk.

The Fund also works with local entities to implement projects and appreciates that different contexts have varying data use laws. We expect GFEMS Partners to comply with the local laws and apprise us on aligning with contextual best practices. While the Fund is a US-based entity, it recognizes the General Data Protection Regulations in EU law on data protection and privacy for all individual citizens of the European Union (EU) and the European Economic Area (EEA) as consisting of one of the strongest legislations protecting data subjects, and many of its principles are infused in this GFEMS Responsible Data Management (RDM) Guidelines. If the Fund directly or indirectly through its Partners collects information from any EU or EEA citizens, it will be fully compliant with this legislation. Failure to comply can result in hefty fines and GFEMS will hold Partners accountable for compliance. GFEMS will include clauses in its contracts to this effect and assess Partners' compliance efforts during all research efforts in the national contexts in which they work.

The Fund will have each of its contracted prevalence estimation and knowledge, attitudes, and practices (KAP) studies reviewed by both an Institutional Review Board (IRB) in the country of study as well as the country of the lead research institution, provided it is outside of the country of study. For any research conducted by implementing partners, the Fund requires that these partners communicate with GFEMS its proposed plans. For any planned research activities involving human subjects and/or personally identifiable information (PII), partners should be prepared to identify an ethical review board and plan for a 2-3 week period of review. GFEMS can assist implementing partners with determining which research endeavors require ethical review as well as identifying a review board.

How to Use this Document and to Whom Does It Apply?

These protocols apply to GFEMS internal staff as well as Partners as they engage with data as well as its subjects (research participants) throughout the lifecycle from collection to disposal. GFEMS staff and GFEMS Partners are required to adhere to and use this document as minimum guidance and as well as to complement their own internal policies and local laws on the responsible use of data. This document does not aim to replace or substitute any practices which are already in use but to further strengthen them and to enhance their efficacy.

The Data Lifecycle — Steps and Protocols

1. Before Collecting Data

GFEMS commissions and provides oversight to its field research studies, which includes conducting surveys with research participants face-to-face or through phone and social media. GFEMS Partners are to incorporate data protection into their research methodologies in writing to prevent risks and potential breach of confidentiality prior to beginning any research with participants. GFEMS will provide oversight and guidance throughout the data processing cycle. These steps will also be captured in the ethical review submissions which will detail the research design including information to specify who is being researched, how many research subjects will participate, why, and what tools will be used. GFEMS and its Partners are responsible for protecting people's personal data throughout the entire data lifecycle.

To best protect participants and personal data, use the following guidelines:

a. Understand the local context, review existing domestic legislation around data privacy and protection, and develop appropriate research design protocols and supporting documents to submit **for ethical review** and approval from GFEMS.

b. While developing the research design, take into consideration vulnerable/marginalized populations and their **right to be heard and included** in the research, while also balancing the need to protect their privacy

and ensuring that collecting their data does not cause them further harm. There should also be no discrimination in the distribution of research benefits.

c. Data collection needs to have a **specified purpose** which should be clearly defined during the research design and later communicated to the research participants before obtaining consent. GFEMS and its Partners should also practice **data minimization** (i.e. limiting the collection of data, especially personal identifying information to that which is deemed fully necessary for the purposes of research and evaluation). Personal identifying information is data which concerns natural persons such as name, identity numbers, and details such as ethnicity and union membership. This excludes non-persons and also groups of people like corporations. Sensitive data such as race, ethnicity, religious or political views are a subset of personal data.

d. Consider **data sensitivity**[1] and carry out a **risk assessment** to weigh the benefits versus the impacts of collecting certain data, as well as the method(s) of data collection and how the data and any identifying information will be stored and used. Some questions to consider prior to processing any data include, for example:

- Could any data point be exploited to cause harm? How?;
- Could the planned methods of collecting data harm the collector and the research participants? In what way or ways?;
- Do the storage devices used have adequate protection of identifying information or sensitive data?;
- Does the benefit of releasing certain data outweigh the potential harm it can cause?

2. Collecting Data

GFEMS recognizes the importance of data quality and integrity to ensure respect for an individual's rights, autonomy, and dignity. Any research and subsequent data collection will be conducted only after it has been approved by an ethical review board. GFEMS does not directly collect data, rather it does so through its Partners. The FUND will oversee and coordinate with these Partners to ensure that the following steps are considered and enforced while collecting data:

1 For example, UN Development Group (UNDG) in a guidance note defined 'sensitive data' to include race or ethnic origin, political opinions, trade union association, religious or other beliefs, physical or mental health or condition, sexual orientation, any info on judicial proceedings, any financial data, any info on children, and vulnerable groups that could cause them harm (physical, emotional, economic). Similarly, GFEMS and its Partners should assess what, if any, sensitive data needs to be collected in our research studies.

a. Voluntary participation needs written[2] informed **consent** to be obtained from potential research participants prior to the start of any data collection cycle, and these participants should be informed of their right to withdraw from the research at any time without any penalty. This is consistent with GDPR guidelines as well. The terms of consent must be clear, and a template can be found in the appendices to this document. The condition and legal capacity of vulnerable groups and individuals should be taken into consideration. GFEMS views obtaining consent as a way to give power to participants in the research process and as a means to hold ourselves accountable to them. The informed consent process applies not just to research participants from whom data will be collected, but also to any persons who may wish to participate in GFEMS programs as volunteers or informers to assist with data collection.

b. **Transparency** about the **purpose** for which data is being collected, how it will be used, and with whom it will be shared should be clearly specified during the consent process. The data should only be used for this original specified purpose or in compatibility with the original specified purpose, unless **express consent** is acquired for additional use.

c. Any personal data collected should be **limited** to the specified purpose of data collection and research. The least amount of data should be collected to accomplish goals. Personal information need not be collected or retained unless deemed absolutely necessary for the research or project.

d. Any personal information should be **anonymized or de-identified**, and the risk of re-identification or piecing together even aggregated statistics needs to be taken into consideration before collecting data so as to assess possible harm this can cause to an individual's **privacy**.

e. Partners will **train enumerators** on proper processes for collecting data from research subjects, capturing and entering that data accurately and safely onto a secured device, as well as uploading and backing up that data in an encrypted online server.

f. Partners are also responsible for properly training enumerators/interviewers on working with and surveying vulnerable populations using a **Trauma Informed Approach**. Any interaction with research participants who are victims or survivors of modern slavery should prioritize their wishes, safety, and well-being. Interviewers need to exercise extensive sensitivity, patience, empathy, and compassion and ensure use of victim and survivor-centered care and practices.

2 For participants that are not literate, they may indicate their consent via a thumbprint as an alternative to a signature.

g. **Standard Operating Procedures** should be in place for any Partners using the services of call center operators, information managers, case management systems and so on. They must follow best practices and uphold the highest standards to ensure data security.

h. The **contact information** of the lead investigator/researcher and any other helpline numbers should be shared with the research participants so they can call to access assistance, for general information about the research, or to give feedback or lodge a complaint. Any participant or potential participant has the right to enquire further about how their data will be used and for what purpose.

3. Managing, Using and Storing Data

GFEMS takes the secure storage of data and its ethical use and re-use very seriously. Whether data is collected manually or digitally, its use and storage are governed by the guidelines provided here.

a. As stipulated during the data collection process for which consent was obtained from research participants, the data will be used for that **specified purpose** only. Personal data will be used in a way that meets the reasonable expectations of the research participants and in consistence with the stated purpose of research, without causing harm or violating their rights.

b. Data collectors and processors will **anonymize** any personal data collected and remove identifiers, unless needed for specific purpose for which express consent should be obtained.

c. Partners will maintain a high **quality** of data so that research participants are not misrepresented; care should be taken to ensure their data is accurate and up to date. Integrity of the data collected should also be guaranteed by checking that those hired or tasked with handling data are equipped with information management/protection competencies. They should be appropriately **trained, impartial/unbiased,** and should not tamper with the data.

d. **Privacy and confidentiality** of any personal data is to be ensured, and this can be done in a variety of ways. Data should be inventoried and then categorized by risk (provisionally), then a specific written control plan should be put in place that addresses personnel management and training, restriction of access, asset/device management, physical security, behavioral controls, device security, network security, communication, travel, incident reporting, and disposal or continuous monitoring. Partners may also choose to have all persons handling data sign a confidentiality agreement. Even if select data has been shared publicly within the allowance of its research purpose, its

subsequent use depends on the context and situation, and the data is still governed by privacy and confidentiality considerations to meet the expectations and rights of the research participants as per original purpose.

e. GFEMS is taking steps to ensure that reasonable **physical and technical security safeguards** are in place to protect data, such as encryption, virus protection, the enforcement of these RDM guidelines and the Information Security Guidelines, among others. GFEMS conducts staff training on how to securely store data in devices and on good practices when handling potentially sensitive data. GFEMS expects its Partners to take similar measures to train their staff on secure data storage and handling of sensitive data. GFEMS currently stores its low-impact data on a professional GSuite drive protected by AES-256 encryption for file transfers and AES-128 encryption for files at rest. Files are then backed up across Google's data centers. For each new dataset, an evaluation of its impact level is conducted and a work plan is defined to best mitigate the theoretical impact of a breach.

Because the world today is more digitized than ever before, the privacy and security risks associated with electronically captured data have increased. Taking these risks into consideration, in addition to these broad Responsible Data Management (RDM) guidelines, GFEMS has also developed Information Security Guidelines which guide our staff and Partners on using available tools to store and transmit data securely online. GFEMS is committed to embedding RDM practices and behavior within its own operations and work culture while also advocating for better policies and actions around RDM amongst Partners.

4. Sharing and Transferring Data

GFEMS' efforts to end modern slavery will require the sharing and publishing of its findings on the prevalence of modern slavery so that greater awareness, transparency, efficiency and coordinated action to fight this menace is made possible. Thus, data sets may need to be shared with and between Partners for the purpose of analyzing and synthesizing the data to formulate actions and solutions to eliminate modern slavery. Depending on the risk category of data, its access will be restricted on a need to know basis. Anyone authorized to access and process personal data will be bound by applicable laws and contractual terms.

We also aim to minimize duplicate collection efforts to ensure efficiency and collaboration in the modern slavery sector, hence it will be important to open data to others. GFEMS and its Partners will only make this decision to open and share data after assessing its value to the common good which should outweigh any potential risks, and within the parameters of express consent acquired from research participants for its specific purpose and use. We will work to minimize collection of identifying information and will anonymize it before any data is opened or shared.

a. The purpose and use of data, including plans to share data, will be communicated to research participants before and during the data collection process and their voluntary consent will be obtained.

b. Where relevant, GFEMS expects its Partners to use and sign **Data Sharing Agreements** as a good practice to map and monitor use of any data shared between Partners and/or GFEMS and to guarantee adequate safeguards to protect the confidentiality and integrity of personal data so that rights and interests of research participants are not breached. GFEMS will be kept informed by Partners if any data is to be shared between them and will provide oversight to check if such practices meet quality and security standards.

c. **Research and implementation:** Partners who plan to share data to track and solve forced-labor cases will first assess their referral pathways to clearly identify with whom the data needs to be shared, and what the risks of this referral would be. GFEMS will assess if Partners have responsible data management protocols in place, and whether they have done a **referral mapping** to identify secure pathways and risk of exposure. GFEMS will work with weaker Partners to bring their referral and data processing quality up to par.

d. If working with government authorities as partners, local laws may necessitate the sharing of perpetrator data. In addition, victim data may be shared unless there is 1) no clear benefit to the research participants and/or 2) a significant risk to them. Such data sharing and use is required to be specified in writing during the research purpose, and the research participants' express consent must be obtained.

e. When data is shared with GFEMS and handled by our staff, we will use reasonable security measures to protect the data, such as those described in our Information Security Guidelines. GFEMS will also strive to create policies which limit individual employees' discretion on data-sharing.

f. Data that is **transferred across borders** and stored in different countries' servers and falls within the purview of local surveillance laws and policies is subject to risks in terms of privacy security and exposure. GFEMS is mindful of this challenge and seeks to continue to learn of the implications of local laws on the rights of research participants through the guidance of its local Partners. GFEMS expects the initiator and recipient of international data sharing to have appropriate safeguards that demonstrate compliance with core data protection principles.

g. If GFEMS or any of its partners possess identifiable data which is requested by data subjects and users, it will be exported in a commonly used format so that data portability is a smooth process.

5. Closing the Feedback Loop

Research participants have the right to be heard and responded to when they reach out to inquire about any concerns or to provide feedback about the research study or project in which they participated. Lack of responsiveness from GFEMS or its Partners in a timely manner may cause further distress or trauma to the research participants, and hence it is of utmost importance that their voices are promptly heard and their right to information is commensurate with their participation in a research study/project.

a. GFEMS and its Partners will provide respondents with **contact details** of the Principal Researcher/Investigator and/or helpline number (if any). The Fund also aims to set up other feedback mechanisms, where possible, to give respondents multiple communication and feedback options.

b. Research participants have the **right to access their data** and to request its rectification (if inaccurate or out of date) and erasure. They should be able to communicate with the data controller using the contact information shared during consent and data collection process and be provided with a response within a reasonable time through accessible methods (call back, mail, or other mechanism). If rectification or erasure of data is denied by data controller, clear and acceptable reasons need to be given, and any charge to send requested data to subject should be reasonable.

c. In projects and contexts where there are longer-term **beneficiary feedback mechanisms** in place for research participants to call and provide feedback and ask for help—such as hotlines, feedback desks and boxes, or community representative or group meetings—these mechanisms should be well-equipped, carefully managed and data should be securely collected, stored, referred and responded to in a timely manner. Referral pathways should be pre-mapped, clearly identified and secured to minimize risk of misuse and breach of data shared.

d. During the research study and data collection process, the persons conducting the research should not make **promises of benefits** that were not planned for nor can realistically be provided. Whether or not any benefits and remuneration would be available for participating in a research project should be clearly stated in the design and purpose of research and communicated to the research participants during the consent process. Deviation from and delay in delivering benefits which were initially promised may lead to false

expectations and distress on part of the research participants and would be a violation of their rights.

6. Disposal of Data Once Purpose is Met

In an effort to minimize the amount of data held at any given point of time, GFEMS and its Partners will not hold data for longer than that necessary for the purpose it was obtained for, and will aim to securely delete information in a timely manner.

a. GFEMS and its Partners will review the **length of time** necessary to keep personal data, consider the purpose for holding information and for how long, on a case-by-case basis for each research study and project.

b. GFEMS and its Partners will make it a common practice to regularly delete sensitive data where retention is not legally required.

c. GFEMS aims to acquire technical expertise on best practices in effectively **destroying data** so that it cannot be pieced together by any party, internal or external to GFEMS and its partners, and will develop practices around secure data disposal and deletion. GFEMS Partners are expected to do the same.

d. Research participants have the right to withdraw at any time during a research study they initially consented to participate in, and also to later request **access to their data and for it to be deleted** (similar to GDPR's 'Right to be Forgotten'). For research on aggregated subjects while using methodologies like Network Scale-Up Method (NSUM), for example, GFEMS and its Partners will anonymize data before processing, in which case it will not be possible to withdraw as an individual's data will not be linked to any identifying information. For individual victim data, if GFEMS and its Partners are ever in possession of it, the data should be maintained in a way that will allow for withdrawal. Unless and until such a request is made, data collected until that point will be kept for the length of time deemed necessary on a case-by-case basis for each research study and project.

7. Data Breach

Data breaches affect people disproportionately—those with the least power and control are often harmed the most. In the event of a data breach, GFEMS and its Partners must take immediate and adequate measures for containment and learn from the experience to prevent any repeat occurrences. A data breach will be grounds to end a contract with a partner.

a. In case of any internal incidents of loss or theft of data or equipment containing personal information, staff must report the incident and all possible details to GFEMS management and designated IT personnel immediately.

b. GFEMS' Partners are required to inform the Fund of data breaches without delay after becoming aware and they hold the responsibility of notifying affected research subjects and any third-tier subcontractors. Once GFEMS learns of a data breach, it will also act swiftly to notify all relevant external parties within shortest time possible but within at least 72 hours of becoming aware, which is consistent with GDPR guidelines.

c. The following information should be provided to GFEMS to investigate a data breach: 1) the nature of personal information exposed, 2) the number of individuals affected by the breach and who they are, 3) when and where the breach occurred, 4) how the breach was discovered, and 5) who may have gained unauthorized access to personal information.

d. Risks associated with the breach must be assessed and the severity of the breach determined. To mitigate the damage and protect research participants from further harm, Partners will consider involving Compliance, Legal, HR and Communications personnel.

e. GFEMS Partners will inform and discuss mitigation measures with individuals affected by the breach to ensure their safety and take all possible measures to protect them from harm.

f. As a contingency plan, GFEMS and its Partners will have back-up mechanisms and security measures in place to wipe out data remotely. GFEMS and its Partners will put in place a case management system in order to register, handle and follow up on incident reports.

Governance and Implementation of the RDM Policy

GFEMS holds itself and its Partners accountable for complying with the law, complying with these RDM guidelines, complying with their own data protection and privacy policies, and for acting in the best interest of the research participants. Implementing the guidance provided for responsible data use is country context-dependent but the spirit of this guidance is to be adhered to by all GFEMS staff and GFEMS Partners in conducting research studies and projects involving data processing of human subjects.

Effective compliance and commitment to responsible data management and use requires an organizational culture that puts the individual's right to consent, privacy and security at the forefront. Practicing responsible data is not a task solely for those directly collecting and processing data, but rather it permeates daily operations, and everyone from leadership to staff will be involved in the process of creating a plan for responsible data management. GFEMS and its Partners will strive to create an enabling environment by investing in knowledge sharing and capacity building about data protection to facilitate the necessary change in behavior, practices and decision making. The Fund will designate a data protection officer to manage this RDM

Guidelines and provide Fund level support to GFEMS staff and its Partners related to the processing and collection of data.

GFEMS will review these RDM guidelines annually so as to address any gaps that become evident during operationalization of Partner projects. GFEMS will also develop supporting tools to share with its Partners to facilitate the application and implementation of these guidelines.

ANNEX 1: RDM Checklist for GFEMS Partners

The Data Lifecycle — Steps and Protocols

1. Before Collecting Data

- Review local legislation around data privacy & protection
- Consider vulnerable/marginalized populations' right to be heard and included in research, and balance with their right to privacy and security
- Define specified purpose of research and plan for data minimization
- Consider data sensitivity and carry out risk assessment to ensure no harm is caused
- Develop research design protocols and supporting documents
- Obtain guidance and approval from GFEMS
- Submit these to local and US Institutional Review Boards for approval

2. Collecting Data

- Obtain informed and voluntary consent from potential research participants
- Be transparent about purpose of research and data collection
- Collect data for original specified purpose only, or obtain express consent for further use
- Limit the collection of personal data
- Train enumerators on proper process for data collection, capturing and storage
- Train enumerators/interviewers on using Trauma Informed Approach
- Establish/use standard operating procedures (SOPs) for call center operators, information managers, case management systems etc.
- Share contact information of lead investigator/researcher with research participants

3. Managing, Using and Storing Data

- Use the collected data in consistency with stated specific purpose of research
- Anonymize or de-identify personal information
- Maintain high quality of data (accuracy, up to date, unbiased)
- Train/equip those handling data with information management/protection skills
- Ensure privacy and confidentiality of any personal data
- Ensure reasonable physical and technical security safeguards to store data

4. Sharing and Transferring Data

- Share and transfer data in accordance with specified purpose/use, and previously obtained consent
- Use Data Sharing Agreements as relevant
- Carry out a referral mapping and identify secure pathways and risk of exposure
- Ensure core data protection principles and safeguards while transferring data across borders and complying with local laws

5. Closing the Feedback Loop

- Provide research participants with contact information of Principal Researcher/Investigator and other options (like helpline) to reach project implementer for concerns/feedback
- Respond to participants' concerns/questions/feedback within a reasonable time (specified)
- Clearly state any benefits/remuneration that participants can expect from partaking in study
- Do not make promises which cannot be met, and do not set false expectations

6. Disposal of Data Once Purpose is Met

- Review and consider length of time to keep personal data for each research study/project
- Regularly delete sensitive data where retention is not legally required
- Comply with participant's request to withdraw from a research or to have their data deleted
- Acquire necessary expertise and practices to effectively destroy data

7. What to Do in Case of Data Breach

- Report to GFEMS of data breaches without delay after becoming aware
- Notify affected research subjects and any third-tier partners
- Provide necessary information to investigate a data breach
- Assess risks associated with breach and determine severity
- Involve essential personnel/departments to resolve the breach
- Take necessary measures to ensure safety and protection of individuals affected by breach
- Consider back-up mechanisms and security measures to wipe out data remotely

ANNEX 2: Information Sheet for Quantitative Survey Participant

Methodology Name and Research purpose

As a participant in the research listed above, you will be asked to answer a series of questions about your experiences in XXXX.

What is the purpose of the study? Name of Organisation is doing a study to find out more about XXXX using XXXX method via survey questions administered to type/# of participants in Location/City/Country over a period of days/weeks/months/years. We will be speaking to persons who are above 18 years of age.

What is the process? You will be given the choice to participate in this study, and if you agree you can select the consent check box online or via enumerator prior to taking the survey. Explain further steps and process details.

Confidentiality All information which is collected in the research will be kept strictly confidential. No one will have access to the database except the research team. If we publish the results of this research, your name and other identifying information will not be included.

What are the benefits? The information collected in this study will help us and others to understand XXXX so that we can apply the learnings to plan and improve XXXX for future individuals/groups/programs. However, there is no direct benefit or compensation to you or your family by agreeing to participate in this study.

What are the risks? There are XXXX (list any risks here). OR There are no perceivable risks in this study as it involves answering survey questionnaires only. Participation is purely voluntary and the decision not to partake in this study will not have any negative consequences. Taking part in this research will not lead to any added costs to you.

Do I have to take part? No. Your participation in this research is voluntary. You have the right to withdraw at any point during the study, for any reason, and without any prejudice. If you decide to take part in this research, you can express this by selecting the check box online or via enumerator after reading the consent section prior to starting the survey. Your alternative is to not take part in the research.

If you have any further questions about the study that are not answered here or if you require any further information or explanation please contact:

Name, Principal Investigator (Email:@@@ / Phone:###)

>> Insert any other Help Line details here if available <<

Statement of Informed Consent:

We are interested in understanding XXXX in Location. Please be assured that your responses will be kept completely confidential.

These questions should take you around ##time to answer. Your participation in this research is voluntary. You have the right to withdraw at any point during the study, for any reason, and without any prejudice. If you would like to contact the Principal Investigator in the study to discuss this research, please let the enumerator know and he/she will provide you with the principal investigators contact information. For this study, the principal investigator is Name.

By continuing with this survey, you acknowledge that your participation in the study is voluntary, you are 18 years of age or older, and that you are aware that you may choose to terminate your participation in the study at any time and for any reason.

Do you wish to continue with this survey? Yes No

_____ _____
Participant Name (Printed) Date

_____ _____
Participant Signature (or thumbprint) Date

RESOURCES CONSULTED:

In developing this document, GFEMS referred to numerous resources and existing policies of various organizations for guidance, and adapted the content to suit its organizational mandate.

Organizational Policies:

- Oxfam Responsible Program Data Policy (Feb 2015), < https://policy-practice.oxfam.org.uk/publications/oxfam-responsible-program-data-policy-575950 >
- WFP Guide to Personal Data Protection and Privacy (June 2016), < https://docs.wfp.org/api/documents/e8d24e70cc11448383495caca154cb97/download/ >
- IOM Data Protection Manual (2010), < http://publications.iom.int/system/files/pdf/iomdataprotection_web.pdf >
- CRS , Responsible Data: Values & Principles (September 2017 draft)
- Girl Effect's Digital Safeguarding Tips and Guidance (May 2018), < https://prd-girleffect-corp.s3.amazonaws.com/documents/Digital_Safeguarding_-_FINAL.pdf >
- ICRC Handbook on Data Protection in Humanitarian Action (July 2017), < https://reliefweb.int/sites/reliefweb.int/files/resources/4305_002_Data_protection_and_humanitarian_action.pdf >

Other Websites, Reports, and Articles:

- Responsible Data Hackpad, curated by participants of MERL Tech, < https://paper.dropbox.com/doc/Responsible-Data-Hackpad-SA6kouQ4PL3SOVa8GnMEY >
- UK DFID, Safeguarding for External Partners, < https://www.ukaiddirect.org/wp-content/uploads/2016/04/Enhanced-Due-Diligence-Guide-for-external-partners-June-2018.pdf >
- Responsible Data Forum < https://responsibledata.io/ >
- The Digital Principles- Principle 8, < https://digitalprinciples.org/ >
- U.S. Department of Health and Human Services <https://www.hhs.gov/ohrp/regulations-and-policy/regulations/45-cfr-46/index.html>
- EU GDPR Rules: < https://ec.europa.eu/info/law/law-topic/data-protection_en >
- MERL Tech, <http://merltech.org/how-to-develop-and-implement-responsible-data-policies/ >
- Center For Democracy & Technology (CDT), Responsible Data Frameworks: In Their Own Words (June 2018), < https://cdt.org/insight/responsible-data-frameworks-in-their-own-words/ >