Humanitarian Data Governance Frameworks: Guide and Literature Review

i. Introduction: A Plethora of Practical Guidance in Search of "Best Practice"

Rationale

The goal of this document is to provide guidance to organizations that are developing ethical frameworks for humanitarian use of digital data and Information Communication Technologies (ICTs). It is built on research capturing both the current state of ethical frameworks for governing the use of data and ICTs by humanitarians, as well as identifying what approaches should be replicated, refined, further studied, and scaled (*See detailed methodology at end of this section)*.

Humanitarian governance of digital data and ICTs is a particularly complex and inter-disciplinary challenge by its very nature to a degree not confronted by the many, other sectors grappling with digitization. Humanitarian data governance is a unique amalgamation of multiple fields - international humanitarian and human rights law, international privacy and data security standards, humanitarian ethics, technical standards for analog, often cluster-based activities, and, in many cases, domestic laws and regulations governing data and telecommunications.

This study is premised on the reality that no single organization possesses the diverse set of competencies to accomplish humanitarian data governance alone. Thus, the development and upkeep of every and any humanitarian data governance framework is increasingly a process dependent on relationships and partnerships with other actors and sectors to be successful on a day-to-day basis.

Humanitarianism, it must be clearly stated at the outset, is now a field of professional practice deeply defined by an inexorable and increasing reliance on the creation and collection of digital data. Digital data generation, online connectivity, and the use, by both responding organizations and targeted populations alike, of ICTs have become core features within the past decade of how humanitarian aid is both theoretically conceptualized and actually delivered in the field.

From beneficiary registration to supply chain management, cash disbursement to non-cash distribution, and rapid needs assessment to monitoring and evaluation activities, humanitarian action in the early 21st Century is truly a digitally driven enterprise. This process of digitization has been occurring as a result, in large part, of the broader global process of digital transformation[1] that has been impacting all sectors, not just humanitarianism. Additionally, the

[1] *"Unlocking Digital Value to Society: A new framework for growth",* WEF/Accenture, January 2017, available at

parallel emergence of the "humanitarian innovation narrative" [2] as a powerful force from donor governments and other funding partners within the past seven years or so appears to have prioritized adoption of digital technologies to a demonstrably acute degree that is arguably unique to the humanitarian field.[3]

While these statements of fact may appear to be obvious ones, the past decade plus has been an iterative and, sometimes, painful process of reckoning by humanitarians, crisis-affected communities, governments, and private sector entities. This diverse community of stakeholders have all been attempting to determine simultaneously, often in competing, uncoordinated, and conflicting ways, what this process of digitization fundamentally does means (and should mean) for both the foundational values and daily work of humanitarians. Perceptions of what constitutes either the potential or already manifest implications of digitization have surfaced a complex tangle of ethical, operational, and legal challenges for individual agencies, networks of humanitarian actors, and the sector writ large - many of which have still not been fully expressed, let alone addressed.

Dozens of ethical frameworks, codes of conduct, handbooks, technical guides, and other documents have thus already been generated in response to the emerging reality of digital reliance by humanitarian actors since at least 2010. The Standby Task Force Code of Conduct, for example, one of the earliest "digital humanitarian" codes of conduct, originating around 2010.[4]

More such frameworks - many more - should be expected to come in the following years. While these frameworks broadly seek to provide some form of practical guidance for either a specific organization or sub-sector activity of humanitarian action, such as biometrics[5] or mobile surveys, [6] there is no currently available overall summary of what constitutes generally cross-cutting best

---

http://reports.weforum.org/digital-transformation/wp-content/blogs.dir/94/mp/files/pages/files/dti-unlocking-digital-value-to-society-white-paper.pdf

[2] Nathaniel A. Raymond and Stuart R. Campo, "*The Case Against Humanitarian Innovatio*n", International Review of the Red Cross, (Forthcoming) Spring 2019.

[3] Elrha, "*Global Prioritisation Exercise for Research and Innovation in the Humanitarian System: Phase One Mapping*", Phase One Mapping, Elrha, Global Prioritisation Exercise for Research and Innovation in the Humanitarian System, 2017, available at: http://www.elrha.org/wp-content/uploads/2017/03/Elrha-GPE-Phase-1-Final-Report_Nov-2017.pdf (all internet references were accessed in May 2019).

[4] Standby Task Force, "*Code of Conduct"*, n.d; available at https://standbytaskforce.wordpress.com/our-model/code-of-conduct/

[5] Zara Rahman, Paola Verhaert and Carly Nyst, "*Biometrics in the Humanitarian Sector*", The Engine Room and Oxfam: Biometrics in the Humanitarian Sector: March 2018, available at https://policy-practice.oxfam.org.uk/publications/biometrics-in-the-humanitarian-sector-620454

[6] WFP, *"Conducting Mobile Surveys Responsibly - A Field Book for WFP Staff"*, May 2017, available at https://documents.wfp.org/stellent/groups/public/documents/manual_guide_proced/wfp292067.pdf

practices to follow when developing any form of ethical guidelines for humanitarian use of data and ICTs.

This document has been created to capture what the ethical state-of-the-art currently is for the humanitarian use of digital data and ICTs, while also charting a course forward for improving future frameworks based on a clear summary of best past practice. This study recommends that, going forward, the humanitarian community should build on this document through regular efforts to collaboratively continue to identify effective practices for ethical governance of humanitarian information activities (or "HIAs") in a formal and routinely iterative way.[7]

It also calls for the governors of the humanitarian system - OCHA and key donors - to invest in the neutral coordination of data governance for the common good. A central function of this coordination of the increasingly complex and overlapping patchwork of governance frameworks is to develop, agree, and promulgate "Common Core Components" (CCC) that should be standard parts of all frameworks across organizations.

These CCC include common interpretations of international humanitarian and human rights law, data protection regulations (such as the GDPR), and critical sources of humanitarian ethics, such as the the core humanitarian principles, as they relate to HIAs. This step is essential for humanitarian action to adapt to the network age and remain anchored in the humanitarian principles.

Methodology

The methodology of this study was a one month qualitative desk review of six governance frameworks for data-related activities produced by United Nations agencies and non-governmental organizations engaged in humanitarian response. These frameworks were all written in at least approximately the past decade (2013 to 2019). The six frameworks were selected based on the following three criteria - 1) The framework is intended to serve as an organization's stated policy on humanitarian data-related issues, 2) the document includes ethical obligations as part of its scope, and 3) the guidelines cover specific operational activities, rather than serving as a general "Code of Conduct" document alone.

The goal of this review is to provide an easy to access resource for organizations developing frameworks for the ethical conduct of Humanitarian Information Activities (HIAs) that provides an overview of emerging best practice, trends, and gaps, as well as a central repository for examples of recent frameworks by UN agencies and NGOs. The summarized literature review of the frameworks, while not intended to be exhaustive, provides short assessments of the

[7] Faine Greenwood, Caitlin Howarth, Danielle Escudero Poole, Nathaniel A. Raymond, Daniel P. Scarnecchia, *"The Signal Code: A Human Rights Approach to Information During Crisis",* 2017, available at https://signalcodeorg.files.wordpress.com/2017/01/signalcode_final7.pdf (4)

frameworks, highlighting their scope, use of existing sources of legal, human rights, and ethical standards, and how these frameworks are intended to apply and be used within organizations.

Resources and handbooks not designed to be a single organization's policy on the issue, such as the ICRC Data Protection Handbook and the *Signal Code* resources, were not considered to be within the scope of this study. The key findings and recommendations presented below are derived from the review of these frameworks and seek to encapsulate core themes found from reading these documents in reference to one another.

ii. Key Findings and Recommendations

This study identifies six key findings and recommendations based on evidence of emerging best practice within the field, gaps that must be addressed in future iterations of current guidance and the development of additional guidance, and trends that appear to be occurring across agencies and contexts engaged in making and onboarding these frameworks. While continued more detailed and longitudinal study is required of ethical frameworks in this area of humanitarian practice, these findings aim to represent a useful snapshot of the ethical standards currently in play within the humanitarian sector as of this writing.

This study focuses on six major ethical frameworks - each specific to one organization, some even specific to certain technical functions within an organization - as examples of current practice. This number does not include cross-cutting translative and summary resources, such as the Signal Code (volumes I and II) and the ICRC Data Protection Handbook. While the full number of frameworks is certainly much larger, this study selected examples of documents that appear to be foundational and/or representative of the broader sectoral process of ethical guidance development.

From review of these six frameworks, the study concludes that there is a clear presence of an emerging human rights focused approach to data governance; that organizations are developing tailored frameworks, rather than adopting one common ethical standard - and that this trend is happening without central coordination; that there are critical gaps in critical incident management and private sector partnership governance; contextually-specific, often technical guidance is becoming more and more common; and that cross-pollination of concepts across frameworks, as well as common translation of analog legal, ethical and regulatory frameworks, are occurring through a diverse network of non-traditional humanitarian actors, including research institutions.

A) Frameworks are increasingly rights-based, but lack intended outcomes for populations

Frameworks by leading humanitarian organizations reviewed in this study appear to increasingly be including language that seeks to articulate the rights of crisis-affected populations in the context of being data subjects of humanitarian interventions. This is an important trend to

recognize because it demonstrates that there is an emerging concordance (if not agreement) across organizations that how data is collected, processed, analyzed, and shared across the data life cycle has implications for the human rights and human security of populations beyond the responder-centric efficiency implications of conducting specific operational activities.

This trend is positive because it shows an initial translation of the RBA (Rights-Based Approach) of the Humanitarian Charter and other outputs of the response to the 1994 Great Lakes Crisis is occurring to some extent. Efforts such as the Signal Code's human rights approach in its two volumes of ethical guidance for practitioners, while itself not intended as a direct cut and paste organizational framework, has likely helped encourage and support this trend.[8] Examples of human rights frameworks cited by frameworks examined in this study include the Convention on the Rights of the Child and the International Covenant on Civil and Political Rights.

However, there is a clear lack of metrics that articulate and assess what the intended outcomes for populations when the frameworks are implemented and adhered to should be. The emerging concept of "Digital Dignity" that is put forward by this document (*See Section iii below*) is intended to provide the beginning of an outcomes based approach to developing humanitarian data and ICT governance frameworks.[9]

At present, the approach to framework development is still largely rooted in an organizational focus on legal and reputational liability limitation and mitigation posture for humanitarian actors, rather than a set of intended outcomes of data responsibility for affected populations. The fostering of an "intended outcomes" approach, conversely, attempts to ground frameworks in declaring what an optimal state of ethical compliance should provide as measurable benefits for groups covered by the scope of the frameworks.

This markedly different approach may represent a potentially important evolution of the application of RBA to humanitarian data governance through using metrics of Digital Dignity to measure whether an optimal state of ethical adherence is actually being achieved. A danger of the current approach is that frameworks may sometimes exist simply as a series of boxes to be checked by practitioners, rather than guidelines serving as an active tool for measuring real time impacts of data governance on affected communities.

B) No "one size fits all" framework does (or should) exist for every organization

---

[8] Faine Greenwood, Caitlin Howarth, Danielle Escudero Poole, Nathaniel A. Raymond, Daniel P. Scarnecchia, *"The Signal Code: A Human Rights Approach to Information During Crisis",* 2017, available at https://hhi.harvard.edu/sites/default/files/publications/signalcode_final.pdf (NOTE: One of the authors of this study, Nathaniel A. Raymond, is also a co-author of the two volumes of the *Signal Code*.)

[9] AUTHOR'S NOTE: The term "*Digital Dignity*" was coined by Markus Geiser of ICRC in conversations with Nathaniel A. Raymond at Harvard University in June 2018.

This analysis concludes that there is an emerging sectoral consensus, as evidenced by the actions of organizations producing ethical frameworks for humanitarian use of data and ICTs, that there is no one size fits all framework for each and every organization. It can be assumed that if a common framework covered the needs of all organizations that there would be evidence of widespread adoption of one or more overarching frameworks or codes across agencies, contexts and networks. No such evidence is apparent.

In fact, what a close reading of six major frameworks launched over the past half decade appears to demonstrate is that organizations are developing individual codes of conduct, guidelines, or other forms of standards to meet specific organizational and operational contexts. This trend is important to recognize because it shows organizations are taking pieces of other organizations' guidance for incorporation into their own, a trend this study calls "cross-pollination" (*See "Finding E"),* while also developing specific guidance tailored to their needs and challenges.

The phenomena of organizationally bespoke guidance creation, which also begins to reference an emerging corpus of common standards, is generally consistent with the "ecosystem" assessment of data governance identified by the 2016 OCHA (United Nations Office for the Coordination of Humanitarian Affairs) Think Brief, *Building Data Responsibility into Humanitarian Action*, which stated, that:

> Importantly, participants in the humanitarian data ecosystem will need to look beyond their own organization to ensure that their broader environment is adhering to the principles and practices of humanitarian data responsibility. Without a holistic, ecosystem-wide approach, humanitarian data use will only be as responsible as the weakest link in the data chain.[10]

As the above quote notes, however, [11]

C) Absence of "critical incident" definition and coordinated critical incident management

A major gap observed across the frameworks reviewed by this study is the absence of any clear definition of what constitutes a "critical incident" - i.e. an event resulting from negligence, malice, and/or unintended consequences of how ICTs are used and/or how data is collected, handled, shared, and deployed that may cause tangible harm to affected populations, humanitarian actors, or others. While the March 2019 OCHA *Data Responsibility Guidelines*

[10] Nathaniel A. Raymond, Ziad Al Achkar, et al, *"Building data responsibility into humanitarian action",* OCHA Policy Development and Studies Branch (PDSB), May 2016, available at https://www.unocha.org/sites/dms/Documents/TB18_Data%20Responsibility_Online.pdf

[11] Christopher Kuner and Massimo Marelli, *"Handbook on Data Protection in Humanitarian Action",* ICRC, July 2017, available at https://www.icrc.org/en/publication/handbook-data-protection-humanitarian-action

working draft mentions critical incidents at least 13 times, for example, there does not appear to be an identified definition or basis for assessing what may constitute a critical incident.

Thus, in the absence of a defined concept of critical incidents, there can be no common protocols for coordinated critical incident management within individual organizations and across groups of humanitarian actors. It can be reasonably assumed that, when critical incidents occur, they will likely often affect multiple agencies simultaneously, especially given the entwined nature of humanitarian data sharing and the use of increasingly interconnected data storage systems and operational platforms.

This one area represents a significant and urgent gap in current frameworks, requiring the development of a common definition and best practice standard for joint management of critical incidents across current and future data governance guidelines that is common to all organizations. This gap, paradoxically, is occurring at a moment where organizations are publicly committing in their frameworks to "do no harm" but have not intentionally begun a process of ensuring that they will be able to document and share evidence of what that harm may be.

To date, defining what events should constitute a critical incident which humanitarian actors have an ethical duty to prevent, mitigate, and be accountable for addressing has been, understandably, a sensitive and politically fraught issue. Humanitarian actors have been reticent to publicly disclose retrospective evidence of potential critical incidents for a variety of likely reasons, including concerns about the impact such disclosures may have on financial support by donors, operational access to crisis-affected populations, and the security of vulnerable communities.

However, without a common understanding of how incidents resulting from HIAs that may cause harm occur and present themselves in field environments, true ethical adherence to any framework is almost impossible. As individual agencies continue to develop organizationally-specific guidelines, the area of critical incident definition, documentation, and coordinated management represents an arena where joint efforts are required to address this serious gap.

D) Contextually specific guidance matters more than comprehensive guidance alone

Another trend noted in this study is the presence of increasingly contextually specific guidance within the past approximately three years. Examples of contextual, as opposed to general or comprehensive data frameworks, includes the World Food Programme's (WFP) *Conducting Mobile Surveys Responsibly* guidance from May 2017. Contextually specific guidance can be defined as a framework that covers one specific operational activity, demographic cohort, and/or geographic or operational setting. As cross-pollination of other organizational frameworks

continues to occur instead of a trend towards adoption of common code, it is logical that there is an apparent appearance of more and more activity and setting specific guidance for narrowly defined technical functions. This trend may likely continue, presenting both opportunities and challenges for the development of best practice.

The opportunities represented by an increasingly rich body of contextual guidance are clear. As cross-cutting technical areas are intentionally addressed by one, often leading organization in the space, the likelihood that other organizations that are seeking to frame how they conduct that single HIA-related task in an ethical way will fully adopt and/or partially incorporate that guidance increases. Additionally, technically specific guidance from one organization may be refined or applied within another distinct geographic or operational context by another organization, deepening and enriching available guidance.

The challenges of a contextual approach, however, are also becoming clear as well. There is a danger in a increasingly contextually and technically specific guidance of ethical frameworks becoming both increasingly utilitarian in nature and potentially conflicting in interpretations of how to apply pre-existing legal and regulatory standards, such as around interpretations of human rights issues, GDPR (General Data Protection Regulations) of the European Union, and the Red Cross/NGO Code of Conduct.

It will be critical to support and reinforce the promulgation of common sources of interpretation for core ethical and regulatory standards, such as human rights and GDPR, within contextually specific frameworks, regardless of their operational focus. Organizations such as OCHA, the Sphere Project, and cluster leads will play a unique and important role in identifying what interpretations of cross-cutting legal and ethical pillars should apply to technically specific ethical guidance.

E) Cross-pollination and "translation" is occurring, and that's positive

The phenomena of cross-pollination referenced in the preceding findings is definitely occurring, and this trend is a positive one because it demonstrates an awareness and literacy across organizations of emerging best practice in the space. Cross-pollination, the adoption of components and fragments of other organizational frameworks and interpretations, has been encouraged by the work of a diverse set of organizations with the mandate and capability to engage in the development of public facing and accessible sector-wide resources, rather than organization-centric activities alone.

The concept of "translation" in this study refers to the effort to interpret analog legal, ethical, and regulatory standards into the context of HIA-related operations by humanitarians. The Signal Code, for example, is an effort to translate human rights standards into the context of HIAs. While related, cross-pollination and translation are distinct and separate functions of ethical

framework development. Cross-pollination is the act of applying relevant data-specific past practices and frameworks to new guidelines, creating cross-reference and coherence between them as a result. Translation is the act of repurposing and repositioning previously extant ethical and legal concepts through the specific lens of HIAs. It is clear from this analysis that, though crucial, the capacity for cross-pollination and translation has been an ad hoc, rather than an intentional, function within the humanitarian sector.

Examples of groups that have supported both cross-pollination and translation include GAHI and Elrha, the ICRC, Engine Room, Leiden University's Center for Innovation, the Signal Program on Human Security and Technology at the Harvard Humanitarian Initiative, NYU's GovLab, Data and Society, and others. As evidenced by the list above and as shown in the summaries of specific frameworks below, these organizations have also been able to play critical roles in advising organizations developing ethical guidance and in conducting field and desk research around specific challenges and case studies. It can be argued that the positive trends in this study have integrally depended on the engagement of this constellation of often (in many cases) non-traditional humanitarian actors.

Thus, the humanitarian community has been a major beneficiary of research institutions, consortia, and larger, better resourced organizations, such as ICRC and OCHA, who have been able to play convening and coaching roles with smaller, often more local NGOs and civil society members. It is important that further attention and study is given to how funding mechanisms and mandates have and have not helped incubate and encourage the ability of these groups to perform as a somewhat coherent connective tissue across multiple organizational frameworks.

The critical function that this ecosystem of cross-pollinating and translation supporting organizations has played should not be underestimated or taken for granted as the sector continues to evolve its ethical guidance for HIAs. Supporting the continued ability of this web of cross-pollinating and translating entities to engage in multiple ways with the framework development and maturation process of the sector should be an intentional and clear priority of donors and humanitarian leaders itself as a best practice.

F) Clear lack of guidance exists for governing private sector partnerships

Another major gap identified by this study is common best practice for the governance of third party, often private sector partnerships. In the wake of recent controversies about private sector partnerships in the data space by humanitarians, most notably WFP's public announcement in February 2019 of a partnership with Palantir, it is incumbent upon the sector to intentionally identify best practice for how these increasingly common agreements should be ethically designed and managed.

This study found no evidence of any specific guidance for how the ethical obligations of humanitarians should be protected and delineated from the interests of private sector actors when engaging in data-related partnerships. This issue and the absence of critical incident management definitions and procedures identified above are the two most major gaps in current practice identified by this study.

There are multiple examples of operationally integral, increasingly common, and often long-standing partnerships between the humanitarian space and the private sector - IOM and Flowminder, Mastercard Aid Network, commercial satellite imagery providers and UNOSAT, and WFP's work with a variety of telecommunications companies. However, the field has so far failed to directly address the ethical and operational dangers of these partnerships - dangers that can manifest themselves simply through the optics such partnerships may create in certain sensitive operational settings.

Creating a process for developing best practices and "bright line" standards for how the ecosystem-wide implications of these partnerships should be assessed and governed is an essential requirement of the next generation of ethical frameworks. Engaging in an open and candid process around this issue can encourage cross-pollination of these best practices in both currently extant and future ethical frameworks.

iii. Defining "Digital Dignity"

The word "dignity" is frequently used by humanitarian actors as an aspirational term that is often attached to descriptions of both how aid will be provided by humanitarians, as well as to the end state that the intended outcomes that humanitarian assistance should help achieve. The concept is incorporated into humanitarian ethical practice through the "Common principles, rights, and duties" section of the *Humanitarian Charter*, which is derived from the concept of the "right to life with dignity" from provisions in international law.[12] Dignity is explained in the Charter as follows:

> Dignity entails more than physical well-being; it demands respect for the whole person, including the values and beliefs of individuals and affected communities, and respect for their human rights, including liberty, freedom of conscience and religious observance.[13]

However, there is a general lack of clarity about what achieving the "dignity" of affected populations that humanitarians seek to serve actually entails. Mosel and Holloway's March 2018 report, *Dignity in humanitarian action and displacement*, discusses the lack of clarity about what dignity actually means in the humanitarian context:

---

[12]Sphere Project, *"Sphere Handbook: Humanitarian Charter and Minimum Standards in Disaster Response",* 2018, available at https://www.spherestandards.org/wp-content/uploads/2018/07/the-humanitarian-charter.pdf

[13] *Ibid* (12).

> Dignity is a frequently invoked concept in humanitarian action and human rights. Yet, despite its widespread appearance in humanitarian policy and programme documents, advocacy campaigns and donor requirements, it remains a word with positive connotations but little agreement as to what it exactly entails. Without a clear agreement on what dignity means, it is difficult to know whether a response will uphold or undermine someone's dignity.[14]

Thus, the challenge of defining what constitutes a person's "digital dignity" when developing ethical frameworks for HIA's is complicated by the absence of specificity about what the analog concept of "dignity" truly means operationally for humanitarians. It is with these limitations in mind, though, that this document proposes a definition of "digital dignity" as the intended end state effect that ethical frameworks for the humanitarian use of data should seek to achieve. "Digital Dignity" is defined herein as follows:

> Digital Dignity is the state when the agency, autonomy, and identity of individuals, as well as the communities they are a part of, is respected, enhanced, and empowered through how data that is both derived from them and pertaining to them (inclusive of any interventions that utilize this data) are collected, handled, and employed in ways that realize the human rights and enhance the human security of these individuals and their communities.

The purpose of providing this definition of Digital Dignity is to provoke a dialogue in the sector about what effective ethical frameworks for data governance should seek to achieve for the individuals and populations that may potentially be affected - both negatively and positively - by HIAs undertaken by humanitarian actors. In many cases, these frameworks have been focused on what they seek to prevent or mitigate, rather than articulating what ethical data responsibility practice by humanitarians should seek to achieve.

The logical next step from this definition is the creation and agreement of a set of intended outcome metrics that assess the degree to which a state of Digital Dignity is being realized, critical steps that humanitarians must take to respect the Digital Dignity of individuals and populations, and what mechanisms in ethical frameworks correspond to these metrics and actions. The "quality criteria" included in the *Signal Code: Ethical Obligations for Humanitarian Information Activities* may serve as the starting point of this matrix.[15]

iv. Literature Review of Recent Ethical Frameworks

---

[14] Irina Mosel and Kerrie Holloway, *"Dignity and humanitarian action in displacement"*, March 2019, available at https://www.odi.org/sites/odi.org.uk/files/resource-documents/12627.pdf

[15] Stuart R. Campo, Caitlin N. Howarth, Nathaniel A. Raymond, Daniel P. Scarnecchia, *"The Signal Code: Ethical Obligations for Humanitarian Information Activities",* May 2018, available at https://hhi.harvard.edu/sites/default/files/publications/signal_obligations_final_05.24.2018.pdf

Prior to this research, the most comprehensive study on comparing humanitarian data frameworks available is the *Mapping and Comparing Responsible Data Approaches* (Berens, Mans, Verhulst - June, 2016), which was commissioned by OCHA.[16]

The authors study encompassed seventeen separate data responsibility policies from a wide swathe of NGOs, governmental organizations as well as public-private partnerships, specifically Médecins Sans Frontières *Data Sharing Policy* (2013); Oxfam *Responsible Program Data Policy* (2015); UN Population Fund *Information Disclosure Policy* (n.d.); UNOCHA *Humanitarian Data Exchange Terms of Service* (n.d.); UNHCR *Policy on the protection of Personal Data of Persons of Concern to UNHCR* (2015); LIRNEasia Draft *Guidelines for Third-Party Use of Big Data Generated by Mobile Network Operators* (2014); GSMA *Guidelines on the protection of privacy in the use of mobile phone data for responding to the Ebola outbreak* (2014); White House Precision Medicine Initiative; *Privacy and Trust Principles* (2015); UN Global Pulse *Privacy and Data Protection Principles* (2015); UN Office for Outer Space Affairs I*nternational Charter for Space & Major Disasters* (2000); UNOCHA *Humanitarian Principles* (1991, 2004); Digital Impact Alliance *Principles for Digital Development* (n.d.); European Union Draft *General Data Protection Regulation* (2012); International Organization for Migration *Data Protection Policy* (2010); UNICEF *Information Disclosure Policy* (2011); USAID *ADS Chapter 508 Privacy Program* (2014); International Committee of the Red Cross *Rules on Personal Data Protection* (2016).

While Berens, Mans and Verhulst offered an important overview of commonly covered topics in the policies, their study was broad and included such organizations as GSMA. For the purposes our study, we wanted to look at foundational examples of specific NGO and/or UNA policies. Further, we wanted to examine our chosen policies in particularly greater depth as to how the policies embed or fail to embed law and rights with respect to affected populations into their frameworks.

IOM Data Protection Manual

MSF Data Sharing Policy

OCHA The Working Draft Of The OCHA Data Responsibility Guidelines

Oxfam Responsible Program Data Policy

UNHCR's Policy on the Protection of Personal Data of Persons of Concern

WFP Conducting Mobile Surveys Responsibly

[16] Jos Berens, Ulrich Mans, Stefaan Verhulst, *"Mapping and Comparing Responsible Data Approaches",* OCHA, 2016, available at http://www.thegovlab.org/static/files/publications/ocha.pdf

IOM

Policy Title: Data Protection Manual

Published - 2010

Page Length: 152

How is it updated: Updates built directly into compliance: *"Advocating awareness and implementing continuous training; Circulating comprehensive questionnaires to map data processing practices at the various IOM Field Offices; Conducting routine internal audits by circulating checklists at periodic intervals; Submitting assessment reports for annual data protection audits;"* (98)

Inclusion: Staff: Author-Ruzayda Martens, Legal Officer IOM Geneva. Acknowledgements: current and former IOM colleagues who pioneered the Technology Application and Migration Management (TAMM) Data Protection Project, a joint effort between the Department of Migration Management, the Department of Information Technology and Communications, and the International Migration Law and Legal Affairs Department. The Project benefited from the experience and expertise of a wide range of IOM colleagues, both in the Field and at Headquarters. Project Team members: Shpëtim Spahiya for his contribution and support in the timely completion of the project and to Chiara Frattini, Jacqueline Straccia and Elif Celik for their research assistance. Working Group members for their commitment and detailed feedback, Valuable comments were also received from various missions and individual colleagues;

Scope: Scope is everything involved with IOM data and legit fills every page with useful info- from basic terms to info on data cycles (collection 19, processing (15) , retention (79), etc) to explanation of roles and who can fill them explicitly (18), how to determine the sensitivity of data (15), to when derogation should happen/how it should be considered (103). "The international standards for collecting and processing personal data are acknowledged worldwide. However, the lack of a binding international instrument has been the subject of much debate.

At the 31st International Conference of Data Protection and Privacy Commissioners, a resolution was adopted by a number of States calling for a universal convention and recognizing that data protection and privacy are fundamental rights attributed to all individuals, irrespective of nationality or residence." (3), even budgeting for training and tools to keep compliant and ensure IOM standards (98), Compliance (12), "Personal data should only be transferred to third parties with the explicit consent of the data subject, for a specified purpose, and under the guarantee of adequate safeguards to protect the confidentiality of personal data and to ensure that the rights

and interests of the data subject are respected. These three conditions of transfer should be guaranteed in writing." (11)

Rights are surprisingly foregrounded and data subjects are included as much as possible in Risk-Benefit process, as well adequate training of IOM staff to perform stated goals with data (37). Compliance with IHL must be considered. (21, 28).

Applicability: Applies to all IOM staff "Training is a vital tool that should be used to introduce a "culture of data protection" throughout IOM." (97) and third parties/contractors "In the absence of donor requirements and written contractual obligation to hand over personal data, data controllers should assert and incorporate an ownership clause41 into donor contracts, contracts of service, MOUs and sub-agreements. Written contracts with agents (service providers/consultants), implementing partners, and other third parties should include ownership and destruction clauses.

It should also clearly specify that personal data collected on behalf of IOM should be returned to IOM." (93). Colors of law: 1989 Convention on the Rights of the Child (13, 47). Article 12 of the 1989 Convention on the Rights of the Child, This principle is reiterated in the following instruments: 2007 Paris Principles and Guidelines on Children associated with Armed Forces and Armed Groups; 2005 Committee on the Rights of the Child General Comment No. 6 on the Treatment of Unaccompanied and Separated Children outside their Country of Origin; United Nations Children's Fund (UNICEF) Principles for Ethical Reporting on Children http://www.unicef.org/media/media_tools_guidelines.html 2006 UNICEF Guidelines for the Protection of the Rights of Children Victims of Trafficking in Southern Europe; 1994 United Nations High Commissioner for Refugees (UNHCR) Refugee Children Guidelines on Protection and Care; and 2008 UNHCR Guidelines on Determining the Best Interests of the Child. (37) . "Compliance with national data protection legislation should not be automatic. Whether or not IOM complies with national data protection legislation will depend on the circumstances of the particular case and whether the law in question is consistent with the IOM principles and guidelines. Guidance should be sought from LEG as situations arise, particularly in the event of conflict, inconsistencies or doubt. It should be noted that compliance with relevant national data protection legislation should not detract from the Organization's privileges and immunities. IOM's privileges and immunities vary from country to country depending on the status agreement that IOM has with the government." (21)

There's an exhaustive annex of national data protection legislation. Internally displaced persons (IDPs) cites Guiding Principles on Internal Displacement, UN Doc E/CN.4/1998/53/Add.2. (113). HR Definition: "Human rights means those liberties and benefits based on human dignity which, by accepted contemporary values, all human beings should be able to claim "as of right" in the society in which they live. These rights are contained in the International Bill of Rights,

comprising the Universal Declaration of Human Rights, 1948, the International Covenant on Economic, Social and Cultural Rights, and the International Covenant on Civil and Political Rights, 1966 and have been developed by other treaties from this core (e.g. The Convention on the Protection of All Migrant Workers and Members of Their Families, 199)." (113) "Armed conflict means "all cases of declared war or of any other armed conflict which may arise between two or more…[States], even if the state of war is not recognized by one of them" (Art. 2, Geneva Conventions I-IV, 1949). (111). "An armed conflict exists whenever there is a resort to armed force between States or protracted armed violence between governmental authorities and organized armed groups or between such groups within a state" (Prosecutor v. Dusko Tadic, No. IT-94-1-AR 72, International Criminal Tribunal for the Former Yugoslavia Appeals Chamber). (111) "Refugee" definition (Art. 1(A)(2), Convention relating to the Status of Refugees. Art. 1A(2), 1951 as modified by the 1967 Protocol)." (112) "Repatriation" definition (Geneva Conventions, 1949 and Protocols, 1977, the Regulations Respecting the Laws and Customs of War on Land, Annexed to the Fourth Hague Convention, 1907, human rights instruments as well as customary international law)" (112). "Separated children" definition Statement of Good Practice, 2004 in the Separated Children in Europe Programme (SCEP) (115). "Victim of human trafficking/trafficked person" definition Article 3(a) of the United Nations Protocol to Prevent, Suppress and Punish trafficking in Persons Especially Women and Children, Supplementing the United Nations Convention against Organized Crime, 2000. (116).

Key Takeaways: While the Microsoft paperclip style visuals and cover make it look quite dated/the length seems daunting, its comprehensive and easy for the intended all staff audience to skip through to where they need to learn and find applicable info without sacrificing hardly any specifics. I expected this guide from 2010 to need a major overhaul and its actually still quite current. Needs a bit of updating for roles, terms, types of data/tech deployed, how data cycles, etc are now understood but IOM -more comprehensive/readable than many of the policies/guidances that came after it. Includes many legal refs in bibliography/colors of law that one would expect to see in more docs… Exhaustive documented legal research. This should be/is a landmark that, if heeded and more prolifically taken on board, would have saved many organizations time and money in creating the myriad of data policies. Great template for what should be expected from a responsible data policy.

Médecins Sans Frontières

Policy Title: MSF Data Sharing Policy

Published - December 2013 - Approved ExCom February 6, 2013

Page Length: 15

How is it updated? Not Listed

Inclusion: Unclear of authorship- seems to be internal "'Custodian' means the organisation or committee, who has formal responsibility for a specific MSF Dataset at the time a request for access is received. The Custodian is accountable for maintaining the integrity and security of the MSF Dataset and for providing access under whatever sharing terms may be in place. The Custodian may or may not be MSF-Epicentre." (2)

Scope: "All health data generated in MSF programs or sites, where MSF acts as a Custodian for such data. It includes but is not limited to data generated from: health information systems, patient records, surveillance activities, quality control activities, surveys, Research, patients/ Research Participants' Human Biological Material." (4) "Intellectual Property" means any patentable inventions or any other proprietary rights that are conceived or reduced to practice by or on behalf of Recipient, in connection with or by use of the requested MSF Dataset(s) (hereafter "Inventions"), and (ii) anydata, results, know-how, and other intellectual property that are not Inventions and that are generated by or on behalf of Recipient, in connection with or by use of the requested MSF Dataset(s) (hereafter "Know-How')." (2) Interesting to note due to human sample/biotech/medical implications.

Applicability: Color of Law: 'Host Country Ethics Committees' or 'HCECs' are the organs responsible for overseeing Research in Host Country(ies)." (2) "MSF data sharing practices will comply with the various international and national legal obligations applicable, notably those relative to medical ethics, medical law, Research and privacy law." (6). "Publication of Results of secondary analyses in peer-reviewed journals is expected to be done in a manner consistent with MSF scientific publishing policy which promotes open access publishing; to that extent, the Recipient shall use its best efforts not to enter into any copyright agreement that unreasonably restricts Page 7 of 15 MSF Data sharing policy Dec 2013 access in any way to electronic versions of any Publications, notably in light of potential public health benefits of releasing results immediately and without restrictions. It is understood that proper acknowledgement of the original researchers will be made." (6-7). Data Handling fees mentioned along with one of only links in paper. "4.7 Protection of medical confidentiality and privacy." (12). "The Recipient shall comply with all the laws, governmental rules, regulations and guidelines which are applicable to the use of MSF Datasets, including without limitation, Host Country(ies) and international best standards and rules relating to medical confidentiality, medical ethics and medical research." (11) "MSF, as an international medical humanitarian organization, and Epicentre, its Research affiliate, are committed to share and disseminate health data from their programs and Research in an open, timely and transparent manner in order to promote health benefits for populations while respecting ethical and legal obligations." (4) The ethical and legal

obligations, along with data transfer processes and guidances/accountability/roles should be outlined but are not. Rights only mentioned in terms of intellectual rights (2, 5, 12) proprietary rights (2), voting rights and modalities for consensus-based decisions (14) and publication rights (15). “Secondary data users will respect the rights and obligations relative to MSF Datasets and its Custodian(s) and are expected to add value to the MSF Datasets they use. Researchers creating new data sets for secondary analysis from shared primary MSF Datasets are expected to share those new data sets and act with integrity.” (6)

Key Takeaways: Empty of real guidance, no laws cited just colors of law pointed to- intellectual property, medical confidentiality, patent, privacy, ethics with little to no explanation. Rights not outlined or pointed to with links or resources. Policy seems to concern itself very little with those whom data is collected from. There isn’t even a Table of Contents. Can’t find referred to draft which may be more comprehensive, only link on the cartography NGO Cartong’s website. All data collection under the control or process of MSF will follow the guidance outlined in the MSF Data Protection Policy (currently in draft form)," (7). [17]

UN OCHA Data Responsibility Guidelines Working Draft

Published - March 2019

Page Length: 37

How is it updated: Working Draft status, Chief of IMB and head of IM Function Provide semi-annual report on implementation of the Data Responsibility Guidelines to the ASG. (41) Functional Leads, Directors and Branch Chiefs-Conduct an assessment of the effectiveness of the implementation of the Guidelines after two years. (41)

Inclusion: OCHA partnered with the NYU Governance Lab (GovLab) and Leiden University, Centre for Humanitarian Data. (2) “Core audience for the Guidelines is OCHA staff involved in managing humanitarian data across OCHA’s core functions of coordination, advocacy, policy, humanitarian financing and information management, with a primary focus on the field.” (2)

Scope: “...all humanitarian data managed directly by OCHA, processed on OCHA’s behalf, or processed by humanitarian actors coordinated by OCHA in different contexts. OCHA’s “corporate” data, including data related to internal financial management, human resources & personnel, and other administrative functions are not covered by the Guidelines. For example,

[17] Draft form non-extant as of this publishing, only evidence of ongoing draft is this Powerpoint deck: Megan McGuire, *“Health Data Protection”,* Médecins Sans Frontières| Doctors Without Borders eHealth Unit – New York, October 2018, available at https://cartong.org/sites/cartong/files/1-%20MSF%20HealthDataProtection_CartOng_102918.pdf

data generated internally by Umoja is not covered by the Guidelines, while data from the Country-Based Pooled Funds (CBPF) is covered.“ (10). “all OCHA staff and supporting personnel (e.g. contractors, stand-by partners, and secondments), who are authorized to manage humanitarian data and related resources across the organization. Although effective implementation of the Guidelines requires action from all OCHA staff, accountability for adherence to the Guidelines rests with senior managers at Headquarters and Field Office level.” (41). “Chief of the Information Management Branch (IMB) and Lead for the IM Function is accountable for the adoption of the Guidelines and their implementation across the organization. The Centre for Humanitarian Data will convene a cross-functional Data Responsibility Advisory Group (DRAG) to track and support the implementation of the Guidelines and monitor critical incidents. “The Centre will serve as the Secretariat for the DRAG.” (41). “At the field-level, Heads of Office (HoO) are responsible for ensuring adherence within their office. This means that, for example, the HoO for a Country Office that processes sensitive data should make sure that the required infrastructure for secure processing is in place.” (41). “Unit Heads are responsible for ensuring the appropriate application of the Guidelines in OCHA’s day-to-day data management work. For example, when a new data management process is started, the Head of the Unit managing the data should be aware of the ensure that a Data Responsibility Plan is prepared before the process begins.” (41). Rights: 4. International Committee of the Red Cross, “Professional Standards for Protection Work Carried out by Humanitarian and Human Rights Actors in Armed Conflict and Other Situations of Violence,” 2018. https://shop.icrc.org/professional-standards-forprotection-work-carried-out-byhumanitarian-and-human-rightsactors-in-armed-conflict-andother-situations-of-violence-2540. (8) UDHR (11). IASC Policy on Protection, October 14th, 2016 IASC Policy on Protection in Humanitarian Action, 2016 - Inter-Agency …(14). DPIA is necessary (48). Has similar learning mandates for staff as IOM 2010 below (42). Accountability and Corrective action explicitly mentioned (42). “For OCHA, guidance is most needed for the management of non-personal but still sensitive humanitarian data. For example, when managing data on critical infrastructure such as hospital locations in conflict areas, data protection and privacy law will not provide some lessons will be valuable guidance since it is focused on protecting the rights of data subjects. The Guidelines therefore cover a broader scope of data.” (16) Provides flexible visualizations that can be utilized for a variety of project types and notes some steps can be omitted/occur out of order but outlines steps that can be expected: “Planning, Collecting and Receiving, Storing, Cleaning, Transfer, Analysis, Communicating and Disseminating, Feedback and Evaluation, Retention and Destruction.” (18). “In particular, developing the Data Responsibility Plan is essential for a clear understanding of required capacities and resources, and to identify potential design or process flaws.” (18). Provides checklist/visualization for developing “Key Actions and Outputs for Data Responsibility” highlights: suggests completing a DRP, goes through PIA to Planning, Collecting and Receiving, String, Cleaning, Transfer, Analysis, Communicating and

Disseminating, Feedback and Evaluation, Retention and Destruction, outlines required skills and training, information sharing protocols, tools for data management, data ecosystem map (19-22).

Applicability: Color of Law: Charter of the United Nations June 26th, 1945. (11) Universal Declaration of Human Rights, December 10th, 1948. (11). General Assembly Resolution 46/182, December 19th, 1991. (11). "EU General Data Protection Regulation (GDPR) which came into effect in May 2018, served as another source of inspiration in drafting the Guidelines." (15).

Key Takeaways: Accountability a huge strong point,, very operational/user-friendly tools such as checklist/charts, etc make this pack and play. Predict: High uptake and alleviation for other orgs with less capacity to build own structures, chain of command and responsibilities of those involved with data/data ecosystem and data processes crystal clear. Makes ethical data policy and tools more accessible than perhaps, ever before.

Oxfam Responsible Program Data Policy

Published - 27 August 2015

Page Length: 7

How is it updated: Every 2 Years (5)

Inclusion: Not specified who wrote it but seems internal. Applies to "including but not limited to the people who provide data, those that collect it, and Oxfam..all external individuals or organizations it works with during the data lifecycle (partners, contractors, etc.) comply with the policy." (1-2) "The ultimate responsibility for this policy rests with the Executive Board...Policy implementation is the responsibility of Oxfam Country Directors and their designates. Support for policy implementation will be provided by relevant personnel within each affiliate." (5)

Scope: Mentions/outlines rights immediately- "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…. not just an issue of technical security and encryption but also of safeguarding the rights of people to be counted and heard; ensure their dignity, respect and privacy.." (1) Rights is meat of it. Social identity, crisis contexts and governance very lightly mentioned.

Applicability: Applies to "Data lifecycle from planning to collection through to disposal…..therefore, this policy includes definitions and requirements for managing high-, medium-, and low-risk data.Humanitarian, Advocacy and Campaigns, and Long Term." (1-2)

Colors of Law *mostly* appear in *glossary* section: Refers to UN rights of child: "If the data process involves minors, Oxfam will get both their, and their parents' or guardians', consent, except in circumstances when it is inappropriate to do so." (3) European Data Protection Directive 94/46/EC8: Anonymised data/Personal Data definitions (6) OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data: Data Controller, Data Subject, Transborder data flows of personal data definitions (6,7) Ireland Data Protection Commissioner Guidance on EU Directive 95/46/EC Data Processing definition (6)

Summary: Pithy and specific on who is responsible for what, emphasizes dignity through specified rights and inclusion of affected pops, emphasizes women.

Key Takeaways: High on positive language, Low on Specifics of tech/operationalization, chain of command/responsibility. Crude/elementary where law/rights correlation is concerned. No redress/accountability mechanisms. NO PIA. It defines rights of data subjects. Severely lacking in details to operationalize, law citations, citations core hum principles, etc. though some correlation can be inferred through outlined rights structure.

UNHCR

Policy Title: Policy on the Protection of Personal Data of Persons of Concern

Published - May 2015

Page Length: 48

How is it updated: "when necessary to maintain accuracy." (16)

Inclusion: No info on who wrote it, all UNHCR staff and implementing partners (8)

Scope: Covers and outlines these principles: "(i) Legitimate and fair processing (ii) Purpose specification (iii) Necessity and proportionality (iv) Accuracy (v) Respect for the rights of the data subject (vi) Confidentiality (vii) Security (viii) Accountability and supervision" (35). Centralizes accountability and responsibility to Data controller and in principle:"most senior UNHCR protection staff member in a country office/operation." (41). "(i) A Data Protection Officer within the Division of International Protection at UNHCR Headquarters, (ii) Data controllers in each country office/operation, and (iii) Data protection focal points in country offices/ operations." (37) "Processing of personal data may only be carried out on a legitimate basis and in a fair and transparent manner. UNHCR may only process personal data based on one or more of the following legitimate bases: (i) With the consent of the data subject (ii) In the vital or best interests of the data subject (iii) To enable UNHCR to carry out its mandate (iv) Beyond UNHCR's mandate, to ensure the safety and security of persons of concern or other individuals."

(15). Rights of data subjects (19-23) are outlined in categories Information (19), Access (20), Correction and Deletion (20), Objection (20), Modalities of Requests (21), Recording and Response by UNHCR (21), Restrictions (23). Outside of outline of data subject rights listed in comment to side, the rest of these "rights" are mostly UNHCR staff obligations ad are vetted by UNHCR staff/implementing partners.

Applicability: Applies to all UNHCR staff/implementing partners: "whether processing takes place within one UNHCR office, between different UNHCR offices in the same or more than one country, or whether personal data is transferred to Implementing Partners or third parties. The Policy continues to apply even after persons are no longer of concern to UNHCR." (8) and "implementing partners (33)"- implementing partners must "afford a level of data protection the same or comparable to this Policy..(35)." Discusses at length when (Substantial risk to safety/security of individuals and public (38))/how data collected can be transferred to national law enforcement/national court. "Prior to transfer- Data Protection Officer, in consultation with the Protection and National Security Unit within the Division of International Protection, LAS and the concerned Bureau(s), needs to be sought." (37-38) "The transfer of personal data is without prejudice to the UNHCR's privileges and immunities under the 1946 Convention on the Privileges and Immunities of the United Nations and should not be construed as doing so. Privileges and immunities of UNHCR and its staff members exist regardless of any cooperation agreement with the Government of a country (39). Any queries on privileges and immunities are to be addressed to UNHCR's LAS." (39)"Requests and objections from parents or guardians for children should be evaluated against the best interests of the child." (21) Grounds for refusal of data and updating of data by data subjects (19) are outlined. "When elaborating new systems, projects or policies or before entering into data transfer arrangements with Implementing Partners or third parties which may negatively impact on the protection of personal data of persons of concern, UNHCR needs to carry out a Data Protection Impact Assessment (DPIA). A DPIA is required where the collection and processing or transfer of personal data is likely to be large, repeated or structural (i.e. where data is shared with an Implementing Partner or third party over a certain period of time)." (28) DPIA guidance goes into detail about when/how it should be conducted/who should be involved. (28-29).

Key Takeaways: Tonality- This policy is not filled with pretty words and fluff, but it's a tedious read that will likely lose certain staff along way with specificity or too broad of a scope for certain levels of employees as its intended audience is broad-all staff (8). However, it is clearly written and explicit about who it applies to, when/why/how...DPIA highlighted. Absence of laws listed. There's no glossary or citations. Accomplishes goals set forth in table of contents but not through color of law or outside human rights definitions.

WFP

Policy Title: Conducting Mobile Surveys Responsibly

Published - May 2017

Page Length: 26

How is it updated: "will be regularly updated."

Inclusion (Responsibility-)**:** Written by WFP for field staff… *"*main risks for staff?" (5) Acknowledgements: contributions from Jos Berens (Leiden University), JM Bauer, Michela Bonsignore, Perena Sekhri and Angie Lee (WFP).

Scope: Covers very specifically entirety of data cycle from PIA, selecting 3rd party partners, collection process, post-collection process. (12-17, Summary on 17) Specifically outlines rights to redress and rectification procedures to the point of who/where/when (21), updating of data for data beneficiaries (18), Selecting 3rd party and local partners- with special regard to data protection/local law enforcement (3, 14, 15).

Applicability: Outlines specific data collection roles in field/all involved with data collection (11, 14, 15) as well as right to refuse from local pops (14), who is responsible for what actions/protections, methods/locations for complaints (18). Tools and methods of mitigating risk (20-22). Does not state procedures for refusal or how to address fears of possible aid loss/consequences from refusal to participate, Redress "In the event of a data breach, WFP must take adequate containment and recovery measures, such as notifying management (Country Director or the appropriate Chief/Director), reporting the incident and redressing the data breach as part of a comprehensive after-action report process involving all relevant actors. As part of a comprehensive after-action report process involving all relevant actors. Note that a data breach is grounds to end a contract with a third party provider." (21). Recommends Manager *"*should be accountable for managing the risks of DII analysis. Should conduct randomized data security audits (e.g. pull out PII logs and check)." (11) Also recommends "a provision requiring the third party providers to remove this information from the data they eventually send to WFP may be included in the agreement governing collaborations between WFP and third party providers, particularly in highly sensitive contexts. Adherence to this should be verified by WFP through random audits as well as checks by an external party." (21) Rights: "It means respect for human rights and do no harm: people should not be exposed to rights violations, harm, or undignified or discriminatory treatment as a consequence of personal data collection and processing." (7). Special attention is given to socio-economic factors that may impact "free participation" in surveys. (7) GDPR: **"**The position of data controllers is also outlined in the forthcoming European General Data Protection Regulation (GDPR), which although not applicable to all of

WFP's operations, can provide direction for resolving particular data responsibility issues." (7, 25)

Emphasizes review of domestic legislation in affected areas (19, 12). PIA outlined with emphasis on engagement with local orgs/communities to check mobile phone ownership landscape-usage rate, need/applicability for data solutions, etc. (12)

Classifications of data outlined and explained from low to severe. This seems a useful institutionalization/norm creating guideline: from low or no (public), moderate (restricted), high (confidential), severe (strictly confidential). (9)

Recommended private sector tools for each step in data process/classification are mentioned: IM Toolbox (24), Trello, Atlassian (26), Google Docs, One Drive (26, 27, 29), Wetransfer, sdcMicro, KoBoToolbox, Open Data Kit (27), iCloud (29), Google Sheets, sdcmicro, Spririon, Stealthbits, Tableau Prep (31).

Summary: Mentions and explains PII and DII (7) explains who is involved with/responsible for each (11, 14), mentions considering how long third parties should retain both after completion of purpose (15), scope of vulnerable pops very encompassing (7). Very specific guidance on who is responsible for what and when (11, 14, 15). Risk/Harm Analysis Chart (8). Special emphasis on consent as "lawfulness and fairness." (14) Minimization of data collection (12), purpose driven data collection. (7, 11, 12) "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." (11)

Key Takeaways: Understandable read for all staff involved (user-friendly and with consideration to those with time constraints) with concise summaries making policies highly, quickly operational/quickly routinized. Besides GDPR mentioned and domestic law review encouraged, no other laws mentioned. Doesn't root key principles and definitions in color of law or rights.

ENDS