Responsible Data Maturity Model
for Development and Humanitarian Organizations

Introduction

The Responsible Data Maturity Model (RDMM) is a tool to help organizations plot their Responsible Data journey. It was developed for CARE US. Contact Kelly.Church@careusa.org or lindaraftree@gmail.com for more information.

How to use the RDMM

- **As a diagnostic or baseline and planning tool** for organizations to see where they are now, where they would like to be in 3 or 5 years and where they need to put more support/resources.
- **As audit framework** for Responsible Data.
- **As a retro-active, after-action assessment tool or case study tool** for looking at a particular program and seeing which Responsible Data elements were in place and contributed to good data practices, and then developing a case study to highlight good practices and gaps.
- **As a tool for evaluation** if looking at a baseline/end-line for organizational approaches to responsible data.
- **In workshops as a participatory self-assessment tool** to 1) help people see that moving towards a more responsible data approach is incremental and 2) to identify what a possible ideal state might look like. The tool can be adapted to what an organization sees as its ideal future state.
- **To help management understand and budget** for a more Responsible Data Approach.
- **With an adapted context, "persona" or workstream approach** that helps identify what Responsible Data maturity might look like for a particular project or program or for a particular role within a team or organization. For example, for headquarters versus for a country office, for the board versus for frontline implementers. It could also help organizations to identify what parts of Responsible Data are the concern of different positions or teams.
- **As an investment roadmap** for headquarters, leadership or donors to get a sense of what is the necessary investment to reach Responsible Data maturity.
- **As an iterative pathway to action,** and a way to establish indicators or markers to mainstream Responsible Data throughout an organization,
- **In any other way you might think of!** The RDMM is published with a Creative Commons License that allows you to modify and adapt it to suit your needs.

What do the different levels mean?

The RDMM identifies five levels of maturity:

- **Unaware:** when the organization has not thought about Responsible Data much at all.
- **Ad-Hoc:** when some staff or teams are raising the issue or doing something on their own, but there is no institutionalization of Responsible Data.
- **Developing:** when there is some awareness, but the organization is only beginning to put policy, guidelines, procedures and governance in place.
- **Mastering:** when the organization has its own house in order and is supporting its partners to do the same.
- **Leading:** when the organization is looked to as a Responsible Data leader amongst its peers, setting an example of good practice, and influencing the wider field. Ideally an organization would be close to 'mastering' before placing itself in the 'leading' stage.

Glossary:

See the glossary on page 12 for definitions of any terms that are unfamiliar or require additional background.

AREAS	UNAWARE	AD-HOC	DEVELOPING	MASTERING	LEADING
Awareness and capacity	Limited or no awareness of the need for a responsible and ethical approach to data and data-related efforts or partnerships	Some staff and/or leadership are aware and pushing the rest of the organization to do more about data ethics and data privacy/security	Leadership and staff across the organization are aware of the need for responsible and ethical approaches to data, some have been trained, some job descriptions specifically include this area	All staff are regularly trained on Responsible Data and ethics and well-versed in the organization's approach and policies Organization is supporting implementing partners, grantees and/or subcontractors to improve their privacy and security practices	Organization is a leader and 'go-to' authority on ethics and responsible data approaches
Policy, guidelines, practices, governance	No responsible data management policies, privacy promoting practices or data governance are in place	Some groups or teams are creating their own checklists, tools, and guidelines but there is no organizational level policy or consistent procedures or practices There is little clarity on who is responsible for ensuring responsible data	There is general buy-in at all levels of the organization for Responsible Data and ethics guidelines and these are being drafted with input from the wider organization and clear roles and accountability	Responsible data policy and practices and governance are in place and regularly monitored, updated, and improved, including with regard to new legislation, changing technology, or other context changes	Organizational policy, guidelines and practices are open source and shared with the wider sector for on-going learning and improving Local partner organizations are supported to develop their own data policies and guidelines as feasible

AREAS	UNAWARE	AD-HOC	DEVELOPING	MASTERING	LEADING
Accountability	No one is accountable for responsible data management	Some team members have been assigned responsibility for responsible data management, but this is ad-hoc and reactive	Organization-wide responsible data policy and procedures are being developed and tested, including the chain of accountability	All staff and leadership have been trained on responsible data policies and procedures, and are clear on their roles & responsibilities Budgets, technology, and staff are in place where needed to ensure compliance and accountability to the policy and procedures	Accountability for responsible data is clearly assigned (whether to leadership, the board or a Data Privacy Office) and embedded across the organization The organization regularly feeds back to the sector on its responsible data efforts, including failures and improvement
Data partnerships	Staff and leadership enter into partnerships that include data sharing but do not assess them in terms of their data approach and potential for harm No organizational policy or criteria for data partnerships; different units adopt inconsistent contractual arrangements	Staff and leadership are beginning to question how to approach data in partnerships and what due diligence aspects need to be raised Some partnerships are assessed in terms of responsible data before agreements are made, often because of an individual, team or partner's concerns	Responsible data approaches are emphasized as a key element of any partnership or initiative and due diligence guidelines on data and data ethics are being developed	Staff and leadership do not enter into any type of partnership without first conducting data-related due diligence and ensuring responsible and ethical data approaches	Organization is a vocal advocate for responsible and ethical data partnerships and regularly raises this issue with its partners and the wider sector

AREAS	UNAWARE	AD-HOC	DEVELOPING	MASTERING	LEADING
Data inventory, identification, and classification	No understanding of what data the organization holds, where it is held, or who has access to it	Some teams or individual projects or programs keep track of the data sets they hold and restrict access to personal, sensitive or contextually risky data by role, but this is not an organization-wide practice	An organization-wide data inventory has been conducted and personal, sensitive, or contextually risky data is documented There is clarity on where data is held and role-based restrictions on who can access it There is clarity on how personal, sensitive or contextually risky data is used, by whom, and for what	A standardized data inventory process is in place across the organization in support of organization learning and knowledge management A regular process for reviewing and adjusting role-based access to data (for both staff, external consultants, and contractors) is in place and regularly implemented across the organization	Organization supports and encourages its staff and partners to conduct data inventories and better manage secure access to data

AREAS	UNAWARE	AD-HOC	DEVELOPING	MASTERING	LEADING
Data privacy rights	There is no awareness of or concern for privacy rights, data subject rights, or informed consent and no understanding of how to communicate them	Some staff are familiar with informed consent and data privacy rights/data subject rights, but are unsure of how to manage them, especially in situations where data is digital Consent processes are in place for certain activities, but they have not been updated or standardized, and/or they do not account for digital data and emerging digital approaches and legislation	Most staff are aware of data subject rights and working to ensure they are respected and communicated appropriately in any data initiative As part of organization-wide data policies, consent processes are being updated to ensure data subject rights are respected	There is consistent implementation of organization policy requiring that staff communicate with individuals, groups and communities about the personal, sensitive or potentially risky data being collected and why, with whom it is shared and for what purpose(s), any potential risks involved, how long data will be retained, their data subject rights, and who to contact with any complaints Information about data processing is consistently provided in clear and appropriate ways, considering aspects such as age, culture, literacy, data literacy, gender and context Front- and back-end systems are capable of complying promptly with data subject requests and complaints	Data subject rights, informed consent and other privacy protective measures are consistently improved and vocally supported by the organization and its staff, and good practices are regularly shared with the wider sector The back-end system for responding to data subject requests and/or complaints is functioning well and seen as a model for other organizations wishing to successfully and responsibly manage data

AREAS	UNAWARE	AD-HOC	DEVELOPING	MASTERING	LEADING
Legal Frameworks	There is no awareness of privacy laws that exist in different countries There is no understanding of lawful bases for personal or sensitive data collection, use, and retention/ destruction	Some staff and leadership are aware that there are different legal regulations in place for different types of data collection and use There is no consistent guidance or access to legal support when designing data collection/use plans and methods	Staff and leadership across the organization are aware that there are different legal frameworks to consider and different lawful bases for data collection according to county There are emerging processes to support teams to make sense of different legal frameworks and lawful bases for data collection during any data collection and use exercise	Legal review and lawful data capture and use is a part of any effort that includes data collection or use, and staff have sufficient expertise and/or support to ensure that data collection and use is legally compliant (or guidance is provided for cases where legal compliance could place data subjects and/or local organizations at extreme risk or where legal regulations are in conflict with one another) Organization privacy policies are documented, comprehensive, aligned with local legal regulations, and widely communicated in plain language to data subjects	Organization is often consulted or lauded by others for its understanding and/or application of global legal frameworks related to data

AREAS	UNAWARE	AD-HOC	DEVELOPING	MASTERING	LEADING
Risk assessment and mitigation	No context analysis or benefits-risks-threats assessment (or privacy impact assessment/ PDIA) of data collection and use plans and practices	Some teams are doing assessments to determine potential for risks, threats and harms related to data, but this is ad hoc	Processes are being developed to support teams to assess the potential benefits, risks, harms and thrates resulting from collection and use of personal, sensitive, and contextually risky data from vulnerable individuals or groups Benefits-risks-threats assessment processes are participatory when possible, and always informed by local context and wider technology and data trends	There is a standard process for assessing potential benefits, risks, harms and threats resulting any projects or programs that include sensitive, personal data, or contextually risky data that could put individuals, groups or organizations into harm Every project or data-initiative is assessed for privacy- and data-related risks or harms during the design phase and at certain other trigger points such as context change or technology change	Privacy and data-related risks, harm and threats assessments are consistently conducted and taken seriously in terms of go-no-go decisions on projects and partnerships These assessments are shared and discussed with potential partners who are encouraged to also adopt similar practices
Data minimization	Data is collected with no thought as to whether it is needed (or *should* be collected), what it will be used for, who will use it, and whether there is capacity to use and manage it	Teams are beginning to question whether they should be collecting certain data and whether they need it or will be able to use it	Teams are only collecting data when they have a clear and legitimate purpose for the data, and they have a plan, capacities, and budget in place for using it	Every data collection effort is required to have a clear plan for collecting a minimum amount of data with a specific and legitimate purpose Organization has systems in place to manage and ensure data minimization is practiced	Organization advocates for data minimization externally and requires it when joining in external partnerships

AREAS	UNAWARE	AD-HOC	DEVELOPING	MASTERING	LEADING
Data transmission	No awareness of the potential risks to individuals or groups when transmitting personal or sensitive data	Some teams are using encryption or secure file transfer tools and processes but there are no common tools or consistent practices Officially recommended tools and protocols are not being adopted by staff in all cases	Official file-sharing / data-sharing tools, protocols and processes are being developed to protect data privacy and security, including for cross-border data transmission Staff are aware of why these tools and processes are a better choice and are adopting them	Official file-sharing / data-sharing tools, protocols, and processes are mandatory for staff and partners There is widespread organizational adoption of these tools, protocols and processes among staff Partners are beginning to adopt these tools, protocols and processes	Data transmission policies, protocols, and processes are consistently monitored and improved upon
Data security	No organizational data security measures in place Staff have little or no awareness of data security, or what (if anything) is in place to protect data, or why it matters	Staff and leadership are aware of recommended data security policies and measures but do not regularly follow them Data security measures are not adapted to local contexts, low bandwidth operating environments, or new types of digital data	Data security policies and procedures are being updated to respond to/adapt to changes in context, laws and technology Staff are being trained and made more aware of the need for these policies Where weaknesses have been detected, improved security measures have been put in place	All staff are trained on updated data security policy and procedures There is consistent compliance with data security policies and procedures	Data security policies are monitored and improved regularly; security tests are regularly conducted to test for weaknesses Organization is widely known as an expert in data security in the sector

AREAS	UNAWARE	AD-HOC	DEVELOPING	MASTERING	LEADING
Data sharing and open data	No understanding or record of current data sharing or open data practices and no written data sharing agreements in place	Some staff are assessing potential risks that come with data sharing and open data Some staff are including data sharing language in contracts and other agreements Some staff are reviewing third-party data handling to ensure it is privacy protective Some staff are using de-identification techniques but this and all of the above are ad hoc, and learning is not widely shared Some staff are aware that laws exist related to cross-border data transfers but do not have any support to better understand and follow them	Staff and leadership understand assess data sharing and open data contractual requirements for risk or ethical issues, and an organization-wide process for assessing benefits, risks and harms of sharing or opening data is being developed A due diligence process for assessing third party data handlers (contractors, consultants, data processors, etc.) and any other type of data sharing arrangements is being developed Legal counsel is developing a standard data sharing clause for use in partnership agreements Legal counsel is available to support staff on complex partnerships or cross-border data transfer legalities Tactics for de-identification of data are being explored to reduce risks of harm if data are shared or opened	Benefits-risks-harms assessments are consistently conducted, and their results respected and implemented with regard to any data sharing or open data Due diligence is conducted on any third-party data handlers (including contractors, consultants, on-line data processors, etc.) or other type of data sharing arrangement before any data is shared Data sharing agreements are in place and enforced for all consultants, contracts and agreements and consistently monitored for compliance All data that is to be shared or opened is de-identified (where possible) and a risk assessment conducted to weigh benefits versus harms of sharing and opening data Mechanisms are in place to easily manage cross-border data transfers	Good practices are shared with the wider sector and have influenced greater care with data sharing and open data

AREAS	UNAWARE	AD-HOC	DEVELOPING	MASTERING	LEADING
Data combining (mosaic effect), big data analytics, and machine learning	No awareness of the potential risks of re-identification or other harms when data sets are combined, or big data and machine learning are used	Some staff and leadership are aware of potential risks due to new data analytics approaches, but there is nothing in place to assess or mitigate potential risks	An initial framework and guidelines are being developed or adopted and piloted to assess potential risks of combining data sets, big data analytics, machine learning, and other emerging approaches Privacy enhancing practices and techniques are being tested for applicability to the types of data sets in question	Before data sets are combined or big data or other emerging approaches are considered, a thorough assessment is conducted to weigh potential benefits, risks and harms to vulnerable individuals or groups Privacy enhancing techniques and practices are in place to reduce to the degree possible any re-identification of data or harm to data subjects	Organization advocates for greater care when combining data sets and using big data and other emerging approaches and has examples to share with the wider sector of good practices related to them Organization is on the cutting edge of identifying new ways to safely use and analyze data while considering and mitigating potential harms
Data retention and destruction	No data retention or destruction plan and no awareness of why it matters	Some staff are beginning to think about and establish time periods for data retention and destruction	An initial data retention and policy is drafted and in process of testing and application New initiatives are beginning to incorporate data retention and destruction plans with clear processes in place	Data retention and data management policies and procedures are established, and staff and leadership trained on them and are consistently following them Data is consistently managed in ways that ease data discovery, retention and destruction Systems are in place to automate these processes where possible	Data retention policy is regularly updated to reflect applicable legal frameworks Organization shares its data policies openly for others to learn from and adapt/apply

AREAS	UNAWARE	AD-HOC	DEVELOPING	MASTERING	LEADING
Incident response and data breach management	No awareness around potential risks of a data breach or the need for a data breach policy/plan	Some staff are concerned about the possibility of a data breach and seeking support to design preventive and reactive actions in case of one	A data breach policy has been drafted and is being tested Roles and responsibilities for a data breach have been established	The organization has successfully identified and prevented attempted data breaches, and/or responded to them smoothly and successfully	Data breach policy is tested annually for effectiveness and adapted to improve Data breaches are openly shared with the wider sector in order to support learning and improved security overall

Glossary:

Data minimization: Data minimization is the principle of not collecting more personal data than you need for your purposes and not collecting irrelevant details "just in case" they might be useful in the future

Data partnership: In this document, we use the term to refer to any type of partnership or collaboration that involves data sharing or processing of personal, sensitive or contextually risky data.

Data subject rights: These include a number of rights as outlined in the European Union's General Data Protection Regulation (GDPR), including the right to be informed, one's right to access personal data held by an entity, right to rectification of data held by an entity, right to be forgotten, right to restrict data processing, right to data portability, right to object to personal data processing, and right not to be evaluated on the basis of automated data processing.

Lawful basis for data collection: The EU's GDPR outlines 6 lawful bases for data collection, including:

a) **Consent:** the individual has given clear consent for you to process their personal data for a specific purpose.
b) **Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
c) **Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).
d) **Vital interests:** the processing is necessary to protect someone's life.
e) **Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
f) **Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

See the UK Information Commissioner's explanation for more detail https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

Mosaic effect: The mosaic effect happens when previously unlinked data about someone are combined and these then produce a profile that wasn't seen when the individual bits of data were isolated.

Responsible Data: Responsible Data (RD) is a concept outlining the collective duty to prioritize and respond to the ethical, legal, social and privacy-related challenges that come from using data in new and different ways. RD encompasses a variety of issues which are sometimes thought about separately, like data privacy and data protection, or ethical challenges. For any of these to be truly addressed, they need to be considered together. See the Responsible Data Forum https://responsibledata.io/what-is-responsible-data/

Risks: Here we consider risk to be the potential severity and likelihood that harm could come to an individual or community due to data being collected or used. We also consider harms that could result from mismanagement (purposeful or unintentional) of data.

Threats: Here we consider the potential likelihood that someone (usually an external actor) may want to get ahold of the data that we are collecting or storing to alter it or use it for unauthorized purposes.