Minutes - Information Management Network Meeting, 06th November 2019

Responsible Data Management and Data Protection

Chair: Shon Campbell, MIMU Manager.
Participants: UNHCR, Phandeeyar, UNFPA, WVI, ICRC, Jhpiego, UNICEF, WVI, FSWG, UNRCO, WHO, JPF, WWF, MIMU

	This meeting focused on the subject of **Responsible Data Management and Data Protection** with a short orientation/workshop provided by Matthew Richard of UNHCR and exchange of information by participating agencies on their current practices.
1	**Agencies' current practices in Data Protection** Prior to the meeting, a short questionnaire was circulated to persons planning to attend this meeting. Among the 15 respondents, 87% noted that their agency had some form of Data Protection Policy, and 80% noted that there was a known Data Protection Focal Point. Agencies present in the meeting shared the systems they currently have in place for data protection. Current activities included: - Attitudes – don't collect more than you need – then don't need to protect as much later on, regular updates on how to protect self in use of social media, discussions within the team on data protection - Processes – password protected data, avoiding use of some platforms for data sharing such as whatsapp, aggregate data before it is analyzed- less protection needed, tagged filing systems, designing a data flow which prevents individual data being shared with those who don't need to use it, storing hard copies and soft copies, protection of data on arrival, data sharing on a need-to-know basis, individual confidentiality agreements, - Infrastructure – updated antivirus programmes and networked firewalls, updated software, use of cloud storage backups, individual log-in passwords, data storage in home managed servers, access restrictions allowing only relevant staff to access the servers/folders, weekly backup, use of One drive synchronized to cloud storage, homegrown system to support monitoring system involving partners and donors, use valid certificate server, staff vs guest wifi codes, using internal SLACK channel for internal exchange.
2	**Responsible Data Management and Data Protection *(Matthew Richard, UNHCR Information Management Officer)*** **The global context**: Good practice in data management means ensuring data protection by design with workflows which apply data protection principles at every step. We also need to recognize that changes in technology have changed not only how we manage and capture data, but also how we consider data protection. Globally, the digital revolution has decreased the cost of hardware and increased the performance of systems – however it has also led to increased demands for personal data - from Governments (to identify individuals and to provide them access to public services), from companies (to provide targeted products and services to users), and from humanitarian and development organizations (to better coordinate, respond and assist persons of concern). **Why is data protection needed?** "Protecting individuals' Personal Data is an integral part of protecting their life and dignity. This is why Personal Data protection is of fundamental importance for humanitarian organizations." ICRC Handbook on data protection in humanitarian action:

Data protection is the systematic application of a set of institutional, technical and physical safeguards that preserve the right to privacy with respect to the collection, storage, use and disclosure of personal data. **အချက်အလက်ကာကွယ်ထိန်းသိမ်းခြင်း** ကိုယ်ရေးကိုယ်တာ အချက်အလက်များအား ကောက်ယူခြင်း၊ သိမ်းဆည်းခြင်း၊ အသုံးပြုခြင်းနှင့် ထုတ်ဖော်ခြင်းတို့အား လေးစားစွာဖြင့် လျှို့ဝှက်ထားရန် အခွင့်အလမ်းကို မူလအခြေအနေတိုင်း ထိန်းသိမ်း ထားနိုင်သည့် အဖွဲ့အစည်းဆိုင်ရာ၊ နည်းပညာဆိုင်ရာနှင့် ရုပ်ပိုင်းဆိုင်ရာ အကာအကွယ်များအား စုစည်းထားသည့် စနစ်ကျသော နည်းလမ်း ဖြစ်ပါသည်။

Privacy International, a leading agency promoting the protection of people's right to privacy globally, has some useful insights for our work: It notes that legal protections on data differ enormously around the world, and because information travels around the world on various networks, it may end up in areas with limited protection. It is important that the specifications and the data use are defined at the time of collection, and that the data is not used for other purposes than what it was collected for. Data should not be passed on for other uses or to other parties without the agreement of the provider. https://privacyinternational.org/video/1623/video-what-data-protection

Different types of data need protection. In our work in development and humanitarian sectors, we collect different types of data. This includes data about the context (eg admin boundaries, locations of services, development data, political and socio-economic data), data about the people affected by the crisis and their needs (needs assessment data, population figures, displacement data, locations of affected people), and data about the response (3W/4W data, Post-distribution monitoring, monitoring reports, information on cash and aid distributions, funding and financial tracking). Developments in technology have also opened up new ways of collecting and storing data – for example through tablets and mobile phone apps, drones, biometrics, kobo and ODK platforms.

Specific protections are needed for personal data - data that directly or indirectly identifies, or can be used to identify, an individual (eg name, address, sex etc), and sensitive data – personal data that warrants stricter security and confidentiality. This data can cause harm in the wrong hands. (eg religion, ethnicity, medical history, political affiliations, biometric data, refugee status, ex-combatant status…). Some information may be considered personal in one context, and sensitive in another.

Important principles in Data Protection - Populations can be helped as well as harmed by data we collect.

- Who owns the data? – Collecting data about someone creates an imbalance with the data collector effectively owning a commodity (the data_ from the subject. This can for example be linked to assistance so there is a strong incentive for those requested to provide data to give it when requested.
- Do no harm - The Do no harm principle means not exposing people to additional risks through our action. Everyone has the right under International Humanitarian Law to be protected against arbitrary or unlawful interference with his or her privacy. This needs to be considered next to the need for specific information to enable effective and efficient humanitarian and development.
- Collective responsibility - Protecting vulnerable populations from the harms posed by data use is our collective responsibility.
- Collect what you need, and use what you collect - It is important not to collect more than is absolutely needed.
- Protection risks in managing data include Discrimination, Stigmatization, Racism, Intimidation or xenophobic practices to groups or individuals. In humanitarian action, some of the risks of poor data management include misuse by hostile actors, identify theft, fraud and interception of assistance, reputation loss and loss of funding.
- Causes of data protection breaches - Data protection breaches can be caused in different ways, through negligence (loss and theft of devices and records; non-restricted access; not encrypting sensitive files; not anonymizing or aggregating sensitive files; e-mailing personal data), and malicious approaches (hacking; coercion; malware; phishing)

- Big data approaches – this new area of data gathering and data management needs new and even more advanced solutions to ensure data protection

The Responsible Data Life Cycle

Data protection needs to be considered at each step of the project and data management cycle – the Responsible Data Life Cycle is a useful way to consider these steps. it focuses on concepts of **privacy, security, and the protection of personal data**. They do not explicitly call for 'data responsibility', but inform policy and thinking on how we can practice responsible data management. Responsible data management recognises the rights of the data subject: The data subject should be able to access and verify their information, to correct their information, to remove their information (right to erasure), and to choose not to be included (right to object).

The steps in the Responsible Data Life Cycle:

1. Think about all the steps - determine how data will be protected before you start.
2. Designate data protection focal points
3. Make a plan.
4. Do a risk assessment - consider why we need the data and whether it will be used. UNHCR's Policy on the Protection of Personal Data of Persons of Concern (2015) is a useful resource for this – focus on bringing the focus back to the data subject and ensuring their rights are protected.
5. Responsibly train data collectors.
6. Collect data – ensuring informed consent. Don't collect data that will not be used - ***Collect what you need & use what you collect!***
7. Manage the data – consider transfer, access, storage, data sharing. This includes it security protection, internal tools, encrypt, anonymize, aggregate, data-sharing agreements.
8. Use the data responsibly - do something with it that can support improvements in the lives of those providing the data.
9. Feedback to respondents.
10. Retain, dispose, archive data – make sure it is deleted from own systems as well as online systems.
11. Data afterlife – ensure the data is really deleted from the systems and can't be restored.

Some practical resources that may be useful for Myanmar

- Define a dedicated Data protection focal point – or more than one if there are also field offices – UNHCR has a suggested ToR for this responsibility
- Data Protection Impact Assessment (UNHCR Data Protection Toolkit) - aims to determine potential risks related to personal data processing; to determine approaches to mitigate such risks; to improve the decision making of data controllers (managers); to demonstrate good practice in data management and contribute to trust and confidence in the organization.
- Self-assessment checklist for Data Protection Focal Points (UNHCR Data Protection Toolkit) – a guide for reviewing compliance. For UNHCR this is used every 2 years.
- Data Sensitivity Decision Tree (OCHA Guidelines) – is another tool that may be helpful however the categories of sensitivity can be subjective and challenging to implement
- Information Sharing Protocol template (OCHA Guidelines)
- Classifying data sensitivity (example from MIMU) – based on who can have access to the data.
- OCHA Draft Data Responsibility Guidelines – May 2019

In summary…

- It is critical to treat the people whose data we manage with respect and dignity, and ensuring that we always act in their best interests.
- Data protection involves a constantly evolving process about deciding when and how to collect data and how to manage risks. Technology is also changing which introduced new opportunities but also new risks not only in data gathering but also in data protection.
- A policy is not enough alone, we need to practice responsible data management and integrate it across the organization, its systems and processes.
- Data protection is more than just about following rules and complying with the law - it's also about our culture and individual attitudes towards managing and handling data.
- We must also consider our organisation's internal policies as well as the growing body of legislation around data management.

Suggested next steps

- Assign data protection focal points
- Review data collection methodologies – aim for data protection by design – meaning it has been thought through and planned.
- Review data security measures
- Data Protection Impact Assessments
- Procedures for requests for access, correction and deletion of personal data by persons of concern. – include tiered access which considers who can access the data within the organisation as well as allows the data subject access
- Share the Data Protection Toolkit as a resource

MIMU Classification of Data Sensitivity *(Shon Campbell, MIMU Manager)*

MIMU manages data from many different sources and has tried different ways of classifying protected data. The models put forward by OCHA and UNHCR have reinforced the need to apply data protection measures at every step of the data life cycle. The OCHA model for classifying data sensitivity based on level of risk (a scale from no/low risk to severe risk) was found however to be too subjective for MIMU purposes as some information could be at different places on the scale at different times.

The system used by MIMU:

1) Classify data protection levels based on who can access the information, using 5 categories which are translated to labels on all files, folders and correspondence for the data and any derived products.
    - Blank (no tag) - can be shared publicly
    - LEVEL_0 tag - likely restrictions. Requires a decision on final classification within 24 hours
    - LEVEL_1 tag – restricted to the MIMU team and limited external parties (for example, customized maps)
    - LEVEL_2 tag – restricted to use within the MIMU team only
    - LEVEL_3 tag – restricted within the MIMU team to limited users. This information is then kept in files with restricted access permission.
2) A Data Protection Protocol documents the rules at each step of the data life cycle process. noting where and how specific information is kept and labelled.
3) Restricted access folders have been established for specific restricted data.
4) Implementing the new data protection system – involved several steps
    - a team orientation on data protection and sensitivity with clear management leadership,
    - a brief inventory of the types of sensitive data each person was holding/managing and how it was labelled and stored
    - classification and labelling of sensitive files, folders and data by each staff member – including all desktop, shared drives etc

3. Further Reading and Resources

Presentations from this meeting

- The PPTs used for these presentations are available on request – contact MIMU (manager.mimu@undp.org)

Further reading and resources

- OCHA Data Responsibility Guidelines – Working Draft, May 2019
- WFP Guide to Personal Data Protection and Privacy (June 2016)
- Oxfam: resource on Responsible Data Management
- ICRC: Professional Standards for Protection Work (Chapter 6)
- ICRC: Handbook on Data Protection in Humanitarian Action
- IOM Data Protection Manual
- Responsible Data Forum: *Shooting Our Hard Drive into Space and Other Ways to Promote Responsible Data Management*
- PIM: Protection Information Management (A website hosting resources to enable the coordination, design and delivery of protection responses)
- UNHCR ODMLP, Modules 2 and 21 (UNHCR staff only)
- Information Security Foundation Course (UNHCR staff only)
- Doing No Harm in the Digital Era (Privacy International and ICRC)

Further guidance

- Security in-a-box: Digital Security Tools and Tactics
- Me and my shadow: Take control of your data
- The 8 day digital detox
- Oxfam: Taking Photos in a Humanitarian Crisis
- The Cash Learning Partnership: *Protecting Beneficiary Privacy*
- Information Commissioners Office (ICO)
- Gender, Privacy and Digital Security, Tactical Tech

Relevant links

- Trackography: an interactive map exploring how the global tracking industry is recording your online behaviour.
- What is Metadata?: Privacy international video explaining what metadata is and why we should care about it.
- Do not track: is a personalized documentary series about privacy and the web economy.
- In Limbo: is a documentary about internet privacy, digital identity, and online communications in which you can enter your own data enabling to see your digital self being peppered throughout the film.
- Why privacy matters: Glenn Greenwald, TED Talk. **(particularly recommended).**

5. Next Meeting – Date to be confirmed. Interested speakers are invited for December 4th.

	Participants	Designation	Agency/ Organization
1	Shon Campbell	MIMU Manager	MIMU
2	Ei Ei Thein	Data Manager	MIMU
3	Zin Min Tun	Database Analyst	MIMU
4	Zaw Win	GIS Analyst	MIMU
5	Khin Thandar Tun	GIS Associate	MIMU
6	Mee Mee Thaw	Information Management	UNICEF
7	Thi Thi Lwin	IM	UNHCR
8	Christoph Trost	Data Analyst	ICRC
9	Tin Cho Aye	Knowledgement and Innovative Coordinator	World Vision
10	Khaing Thazin Aye	IT Specialist	World Vision
11	May Ya Mone Tun	Sub National Network Coordinator	FSWG
12	Aye Yupar	Data and Management monitoring and Report	UNRCO
13	Dr.Thura Kyaw	Sr. Knowledge Management, Learning & Documentation Manager	Jhpiego
14	Dr.Zayar Phyo Aung	M&E Manager	Jhpiego
15	Pyae Phyo Kyaw	Information Management Officer	WHO
16	Dragos Salageanu	Technical Advisor	Joint Peace Fund
17	Thin Eaindra Oo	Sr. Application Support Officer	Joint Peace Fund
18	Yu Myat Mun	programme analyst (Population and Development)	UNFPA
19	Cing Don Nuam	Data Community Coordinator	Phandeeyar
20	Thadoe Wai	Conservation Planning and Evaluation Officer	WWF-Myanmar