TOOL N°2

HR PACK – PROGRAM DATA MANAGEMENT FOR HUMANITARIAN AID AND INTERNATIONAL DEVELOPMENT CSOs

THE PROFESSIONAL FRAME OF REFERENCE PUT INTO PRACTICE

SKILL BLOCK 5: ORGANISE AND IMPLEMENT APPROACHES ENSURING RESPONSIBLE DATA MANAGEMENT

cartong

AUGUST 2022

CARTONG

Created in 2006, CartONG is a French H2H/support NGO specialized in Information Management. Our goal is to put data at the service of humanitarian, development and social action projects. We are dedicated to improving the quality and accountability of field activities, in particular through better needs assessments and monitoring and evaluation. We act as a multidisciplinary resources and expertise centre, accompanying our partners' strategies and operations. Our staff and volunteers also support the community as a whole by producing documentation, building capacities and raising awareness on the technical, strategic and ethical challenges of digital technologies.

ACKNOWLEDGMENT

This publication is supported by the French Ministry of Europe and Foreign Affairs (MEAE-CDCS), the French Development Agency (AFD). Nevertheless, the ideas and opinions presented in this toolbox do not necessarily represent those of MEAE-CDCS and AFD.

1. SKILLS WITHIN THE BLOCK

S5.1: Be familiar with and implement data protection procedures and practices that ensure compliance with national and international law.

S5.2: Be familiar with and apply the ethical principles of responsible data management taking into account industry best practices and contextual specificities.

S5.3: Define and implement data security best practices.

2. THE COMMON AIM OF THESE SKILLS

All of these skills are designed to ensure **responsible data management** through the implementation of **good practices, compliance with standards, principles** in force in the humanitarian and international development sector and respect for the **national and international legal framework** on personal data.

The skills forming Skill block n°5 are required when the program [and M&E] teams collect any conceivable item of data on vulnerable populations. Such skills are required to determine whether the collected data is personal and/or sensitive so that measures can be implemented to ensure ethical data management, including appropriate data security and compliance with legal, industry-standard frameworks. However, depending on the context, these skills can be divided between people who are not directly connected to program data such as DPO posts, local DPO relay, field coordinators, IT, etc.

3. ASSOCIATED KNOW-HOW AND THEIR APPLICATION

S5.1: BE FAMILIAR WITH AND IMPLEMENT DATA PROTECTION PROCEDURES AND PRACTICES THAT ENSURE COMPLIANCE WITH NATIONAL AND INTERNATIONAL LAW

Skill 5.1

Level of proficiency	Technical know-how	Methodological know-how
	Distinguish personal from sensitive data. Execute clear instructions for data protection (configuration of tools, obtaining consent, execution of archive protocols, or de-identification, anonymisation, pseudonymisation, aggregation, etc.).	N/A
	Be familiar with and enforce the key elements of international data protection regulations (GDPR, etc.). Be familiar with and enforce the key elements of the data protection regulation of the country or countries of intervention, such as the principles of processing limitation, limited conservation, proportionality, the rights of the data subject, etc. Implement data protection measures, from the time of default data design and protection, for instance via the choice and configuration of data management tools, the design of collection forms, etc.	Briefly analyse legislation. Design and implement awareness-raising and training actions. Identify action points to improve program data protection. Adapt the recommended measures to the intervention contexts. Establish practices, procedures and methodologies allowing the implementation of key data protection principles, for example: • Choice of a legal basis, • Obtainment of informed consent, • Choice of a retention period, • Implementation of archiving protocols, de-identification, anonymisation, pseudonymisation, aggregation, etc.

	Have specific knowledge of the international and national data protection legislation. Establish practices, procedures and methodologies ensuring data protection of all components, for instance: • Draft of data-sharing agreements, Evaluation of a sub-contractor. Drafting or reviewing DTA/DSA type agreements or contracts. Conduct and draft a Data Protection Impact Assessment (DPIA) on a data processing or simple project, involving few players or few technical solutions. Ensure contractual monitoring of partners and donors on the data protection-related dimension.	Make a diagnosis and implement an action plan to ensure compliance with national and international legislation. Analyse whether a processing is compliant and highlight non-conformities. Develop a data protection strategy for a mission or organisation. Design and disseminate practices, procedures and methodologies allowing the implementation of key data protection principles.
	Conduct and draft a Data Protection Impact Assessment (DPIA) on a complex data processing at mission or organisational level, involving a great deal of solutions and players.	N/A

In which situation is skill S5.1 applied?	
In general, skill S5.1 is used	From the moment data on vulnerable populations is collected…
And more specifically for level A 	…and when it is only necessary to identify whether said data is sensitive or personal in order to apply the appropriate measures. Or when clear guidelines for specific organisational collections exist and all one has to do is apply them. A dedicated data protection relay exists at the local level to support this level.
And more specifically for level B 	…and where general guidelines exist within the organisation and need to be adapted to specific collection activities. …and/or when a dedicated data protection relay exists at the international level.

And more specifically for level C 	…and when a diagnosis of compliance with current legislation needs to be conducted. …and/or when the organisation's guidelines are to be drafted or updated.
And more specifically for level D 	…and when it is necessary to conduct an impact analysis on data protection in a complex environment.

S5.2: BE FAMILIAR WITH AND APPLY THE ETHICAL PRINCIPLES OF RESPONSIBLE DATA MANAGEMENT TAKING INTO ACCOUNT INDUSTRY BEST PRACTICES AND CONTEXTUAL SPECIFICITIES

Skill 5.2

Level of proficiency	Technical know-how	Methodological know-how
	Adopt the data protection standards applied to humanitarian aid and international development (Signal type Code of Ethics, Principles for Digital Development, etc.) and context (non-state armed groups, medical data, etc.). Implement donor guidelines for data protection.	Identify the key ethical issues of a data processing or project and alert if there is any doubt or identification of a risk (for instance, block a data transfer in the absence of a risk analysis). Ensure ownership by program teams of ethical issues (awareness raising techniques and training).
	N/A	Identify the issues at stake in the debate related to the application of data protection concepts and laws in the field of humanitarian aid and international development: • Concept of responsible management vs. protection, • Application of informed consent, inadequacy of the GDPR for the intervention context. Conduct an in-depth assessment of the ethical issues of a data processing or project (be able to argue independently to refuse data transfer to a partner, assess the level of risk of data collection, etc.). Make a diagnosis and implement an action plan to comply with national and international legislation.

In which situation is skill S5.2 applied?	
In general, skill S5.2 is used	From the moment data on vulnerable populations (personal and sensitive) is collected…

And more specifically for level B 	...and when it is necessary to adapt specific collection activities to the general guidelines that exist within the organisation (for compliance with standards defined by donors and the sector).
And more specifically for level C 	...and when it is necessary to conduct a diagnosis of compliance with donor guidelines and industry standards. ...and the organisation's guidelines are to be drafted or updated.

S5.3: Define and implement data security best practices

Skill 5.3

Level of proficiency	Technical know-how	Methodological know-how
	Pre-identify the types of data that need to be protected (sensitive, personal, community data). Have simple reflexes for securing paper based and digital data: locked cupboard, choice of a secured password, encrypting a file, sharing data internally and externally, etc. Be familiar with the best practices for securing the various tools used.	N/A
	Implement project-wide securing of paper based and digital data (shared cloud encryption, password sharing modality, choice of authentication method, user access management, traceability measures, password strength assessment, back-up modality, anonymisation and pseudonymisation method, etc.). Be familiar with the entire range of data security components (including methods for securing the various tools used).	Adapt the organisation's guidelines to specific contexts and develop standard practice guides. Disseminate and know how to ensure implementation of procedures.
	Perform "basic" data security audits. Gain a thorough understanding of the various components of technical and organisational data security and the degrees associated with each: • Difference between encryption during transfer vs. during storage, • Server certification, PGP key concept or AES standard, etc.	Design and align data security practices across the organisation. Assess the level of data security implemented in a project or organisation or with a partner (assess practices, assess relevance and appropriateness of the chosen measures). Be able to communicate easily with IT teams with regards to cybersecurity.

	Be thoroughly familiar with the organisation's IT environment and the appropriate cybersecurity measures associated with it. Apply advanced data security measures in a complex environment (players, tools, and multiple location). Perform complete data security audits.	N/A

In which situation is skill S5.3 applied?	
In general, skill S5.3 is used	From the moment the organisation uses computer and digital tools for data collection, management and storage...
And more specifically for level A 	...and when it is necessary to perform data security manipulations on said tools.
And more specifically for level B 	...and when it is necessary to coordinate data security practices, to ensure their implementation across a mission.
And more specifically for level C 	...and when it is necessary to establish strategic directions in terms of data security, to verify their proper application and to ensure coordination with the associated services.
And more specifically for level D 	...and when it is necessary to establish a complex system (multiple actors, locations, and IT and digital tools) to secure data.

4. WHAT TO KEEP IN MIND WHEN RECRUITING

Training

Dedicated data protection training: dual courses in information technology (so as to easily interact with IT staff) and law/legal.

Experience

Data Protection, implementation of an GDPR compliance framework.

Mastery of key concepts and tools

Basic	Intermediate	Advanced
• Sensitive data • Personal data • Community data • Passwords / Access Management • Do No Harm • Consent • Responsible Data Management vs. Data Protection	• General GDPR concepts (legal basis for the application of data protection) • Encryption (in transit and during storage) • Practice of de-identification, anonymisation, pseudonymisation, aggregation, management of data retention periods • Default data protection from design ("by design and by default")	• Detailed knowledge of the GDPR • Detailed knowledge of the donor rules • Data sharing agreement • DPIA • Cybersecurity • Server certification (PGP key concept or AES standard...)

Attitudes

- Being proactive, identifying deficiencies
- Able to challenge collection needs
- Spearhead proposals (solutions)
- Independence, confidentiality, discretion
- Communication and pedagogy
- Objectivity, impartiality

cartong

23 Boulevard du Musée
73000 Chambéry (France)
+33 (0)4 79 26 28 82

INFO@CARTONG.ORG
WWW.CARTONG.ORG