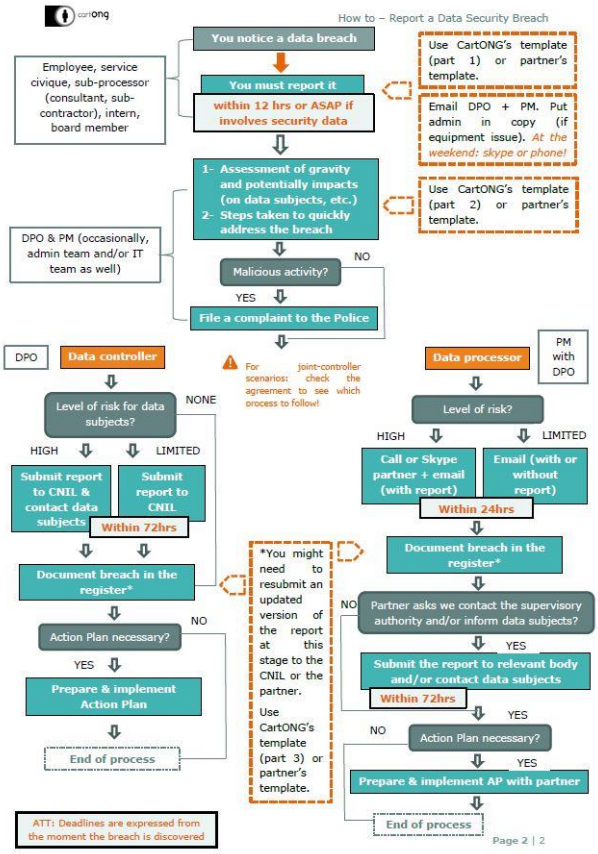
TOWARDS A RESPONSIBLE DATA APPROACH IN NGOS: 6 KEY LEARNINGS FROM CARTONG'S EXPERIENCE

How do you convince your colleagues, the management of your organization, your partners, other actors in the sector that yes, in fact, responsible data management is not only necessary but also possible within humanitarian and development organizations? That it is not only in the medical, banking or security sectors that data can become an actual weapon and that we have a significant responsibility as NGOs? That behind the "here's what we've been doing for your data protection" emails that we have all been receiving in the last 18 months, there are – or should be – profound changes in practices and processes within organizations, and that any change that creates constraints also creates opportunities? That even if the graphs summarizing data protection issues generally look rather like this (Warning-this might hurt your eyes!), this topic is accessible for everyone if the right formats are chosen? That one should not worry about the consequent amount of changes to be implemented and that, like any complex change management process, the first thing is to know how to prioritize? A long list of questions that CartONG has been consistently confronted with in the last two years.

Implementing encryption on mobile data collection tools, designing databases containing sensitive information, mapping stigmatizing diseases, developing web applications containing personal data: data protection has long been a concern at CartONG! With the enforcement of the GDPR in 2018, however, our structure decided that it was time to move to the next level and embarked upon a vast institutionalization process of responsible data management in-house. We invite you to discover the main steps of this journey – still in progress – by reading the article that we published on our website and the lessons we have learned from it in this blog post below.

The work undertaken for the last 18 months in CartONG has indeed allowed us to gather a few key learnings from what we have already undertaken. They are not necessarily revolutionary in themselves, but they complement and reinforce the first lessons learned on the subject shared by other actors in the sector.

I. The strength of the collective



CartONG deliberately chose to delay somewhat the appointment of a DPO in favor of operating with a "task force" for a year and a half. Indeed, the change in practices and culture brought about by the integration of a responsible data approach are such that it is illusory to want or have them led by a single person. While a leader or "orchestra conductor" is absolutely necessary, it is also vital that the latter be able to rely on a network of people both to reach all the departments of an organization and to increase awareness levels and the capacity to raise concerns about an activity (whenever applicable), but also to provide the teams with a first level of response and guidance capable of supporting them on the spot if necessary. In the case of CartONG, these "focal points" have also made it possible to share the workload related to the drafting of new documents (procedures, policies, etc. – an example on the left you can find the PDF format in the zip folder) and to adapt them as closely as possible to the needs of the various technical teams.

Our advice? Spend as much time as necessary in order to have focal points properly convinced by the subject, attentive to the concerns of their colleagues and able to answer the questions linked to everyday work. This will be one of the keys to ensuring that team training sessions – traditionally carried out as part of a change management process – have a lasting impact!

II. The added value of an external support

Working with an external consultant was really important for CartONG, not only because it is very difficult to sufficiently master internally – especially for a small organization like ours – all aspects of data protection (which requires both legal skills and cyber-security skills for example, and this in many areas: human resources, partner relations, web development, etc.) but also because the use of an experienced external third party is a factor of success in a change management strategy. It is certain for us that without relying on a consultant, we would not have made such rapid progress nor would we have been able to deploy the first elements of compliance in such an effective and efficient manner.

Our advice? Find one (or more) service providers close to your core activities and capable of being in a "support" position, i.e. able to answer your various questions and queries that arise on a daily basis and able to accompany you in the process of internalizing the necessary skills.

III. The importance of the diagnostic phase

Because the subject of data protection is so vast, it is common to feel overwhelmed and not know where to start. In this context, being able to identify one's strengths and weaknesses may seem obvious, but without a thorough assessment, it is in fact difficult to clearly identify and prioritize the actions yet to be taken. In fact, if we had anticipated the necessity – within the framework of the consultancy mission – of undertaking a quick inventory of CartONG's

practices, we had completely underestimated its importance and its impact. The latter has allowed us to identify many elements that we had clearly underestimated (data transfers outside of the EU for example, rare but happening from time to time at CartONG), to prioritize elements that originally seemed less urgent in our contexts of intervention (such as the redesign of our IT charter) or on the contrary to put into perspective the "importance" of certain actions (such as the adaptation of some HR aspects that turned out to be less critical than initially planned).

Our advice? Don't neglect the assessment – if you are not yet convinced.

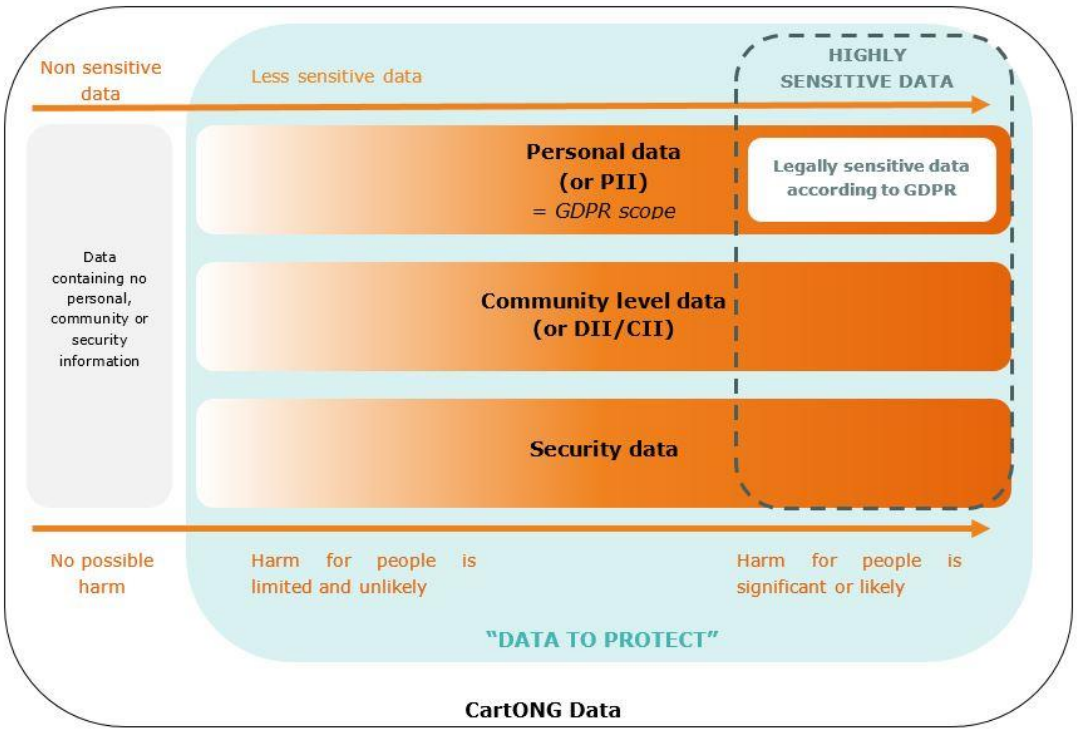
IV. A very long term undertaking

Compliance and full integration of the principles of responsible data management remains a long-term task, especially for a small association of the size of CartONG. The work initiated in 2019 is just only the beginning and efforts will naturally have to continue over the next few years.

Our advice? Don't look for full, let alone immediate compliance! It is better to prioritize the actions that have the greatest impact for the people concerned and to go step by step, without neglecting practical implementation rather than simply achieving compliance from the outside.

V. Responsible data management is not just a matter of GDPR

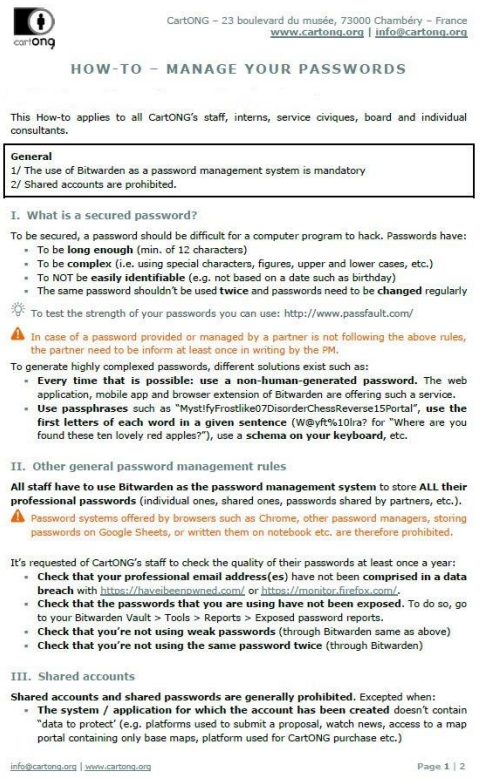
In our sector, it is vital to remember that the scope of the data protection issue is not limited to legal issues of compliance with the GDPR. Not only is it a key issue from an ethical point of view for humanitarian and development operations in order to "do no harm" in the digital age (integration of the "do no harm" principle into data management – cf. commitment n° 3 of the fundamental humanitarian standard https://corehumanitarianstandard.org/resources/chs-guidance-notes-and-indicators), but also and above all, a question of respect for the rights and dignity of the people we seek to help. To this end, it is important not to restrict the scope of the approach to the legal definitions contained in the GDPR, but to include, like most of the key actors on this subject, all data that could be harmful to individuals or organizations. This therefore includes, among others, aggregated community data. CartONG has deliberately made such a choice by conceptualizing a broad "data to protect" approach to our activities (see illustration, you can find the visual in the zip folder).



Responsible data management vs. data protection

Responsible data management is a concept that is becoming more and more widespread in the aid sector. According to OCHA, it goes beyond the concepts of "data privacy" and/or "data protection" and involves a set of principles, processes and tools that support the safe, ethical and effective management of data in humanitarian responses. See also: https://responsibledata.io/what-is-responsible-data/

VI. Data protection can also make life easier!



CartONG – 23 boulevard du musée, 73000 Chambéry – France
www.cartong.org | info@cartong.org

HOW-TO – MANAGE YOUR PASSWORDS

This How-to applies to all CartONG's staff, interns, service civiques, board and individual consultants.

General
1/ The use of Bitwarden as a password management system is mandatory
2/ Shared accounts are prohibited.

I. What is a secured password?

To be secured, a password should be difficult for a computer program to hack. Passwords have:
- To be **long enough** (min. of 12 characters)
- To be **complex** (i.e. using special characters, figures, upper and lower cases, etc.)
- To NOT be **easily identifiable** (e.g. not based on a date such as birthday)
- The same password shouldn't be used **twice** and passwords need to be **changed** regularly

To test the strength of your passwords you can use: http://www.passfault.com/

In case of a password provided or managed by a partner is not following the above rules, the partner need to be inform at least once in writing by the PM.

To generate highly complexed passwords, different solutions exist such as:
- **Every time that is possible: use a non-human-generated password.** The web application, mobile app and browser extension of Bitwarden are offering such a service.
- **Use passphrases** such as "MystIfyFrostlike07DisorderChessReverse15Portal", **use the first letters of each word in a given sentence** (W@yft%10lra? for "Where are you found these ten lovely red apples?"), use a **schema on your keyboard**, etc.

II. Other general password management rules

All staff have to use Bitwarden as the password management system to store **ALL their professional passwords** (individual ones, shared ones, passwords shared by partners, etc.).

Password systems offered by browsers such as Chrome, other password managers, storing passwords on Google Sheets, or written them on notebook etc. are therefore prohibited.

It's requested of CartONG's staff to check the quality of their passwords at least once a year:
- **Check that your professional email address(es)** have not been **comprised in a data breach** with https://haveibeenpwned.com/ or https://monitor.firefox.com/.
- **Check that the passwords that you are using have not been exposed.** To do so, go to your Bitwarden Vault > Tools > Reports > Exposed password reports.
- **Check that you're not using weak passwords** (through Bitwarden same as above)
- **Check that you're not using the same password twice** (through Bitwarden)

III. Shared accounts

Shared accounts and shared passwords are generally prohibited. Excepted when:
- **The system / application for which the account has been created** doesn't contain "data to protect' (e.g. platforms used to submit a proposal, watch news, access to a map portal containing only base maps, platform used for CartONG purchase etc.)

info@cartong.org | www.cartong.org Page 1 | 2

Finally, data protection is not only synonymous with new constraints or new procedures for teams. It can also be an opportunity to simplify or clarify certain processes (such as archiving) or even to make real improvements in daily work life. At CartONG, the deployment of a secure but also very practical and intuitive tool for password management – such as Bitwarden – has been a key element of support and no one wishes go back to the way of working (you can find the PDF document in the zip folder).

Our advice? Do not neglect the investments that can simplify the life of the teams. It is good to tone down the complexity surrounding the subject as much as possible by providing tools that meet their constraints.

Some key resources & readings that we recommend to sector actors:

The Handbook on Data Protection in Humanitarian Action (ICRC): https://www.icrc.org/en/handbook-data-protection-humanitarian-action.

The "Responsible Data" community (including its mailing list) coordinated by The Engine Room.

The work carried out by HumData (OCHA) through the design of guides and technical notes: https://centre.humdata.org/data-policy/

The study on the compliance of civil society organizations (CSOs) with the GDPR recently published by the Open Society Foundations. This report presents the opportunities and challenges faced by CSOs and also offers a good practice guide to mitigate risks.