Privacy by Design,
Data and Technology Checklist

SUMMARY

Processing data in a responsible way is a core activity at IFRC. This is a basic worksheet on technology and data processing in software projects to develop an efficient and legitimate data workflow.

Groups who contributed to this worksheet are: Information Management, Health, Legal (IFRC and Norwegian Red Cross), PMER, IT, and Knowledge and Learning.

Responsible data is:
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.
Responsible Data Forum, working definition, September 2014

INSTRUCTIONS

Fill out as best you can in the amount of time you have. Please continue to answer all the questions until you feel you can assure 'privacy by design'. Note that items with an asterisk (*) have further details in the 'Things to Consider' section at the end.

THE CHECKLIST

Project Management

ITEM	QUESTION	NOTES
1.	What is the total cost of the project? This should include software development, training, and other costs connected to the projects lifecycle.	
2.	Will a risk assessment be conducted as part of the Project Management review?	
3.	Which stakeholders need to be consulted for signoff?	
4.	Who are the main stakeholders for this project? Who will use the technology, who will be affected by the technology?	

5.	Within the IFRC Secretariat, what is the process to follow? Who do we need to go to first?	

General Technical Management

ITEM	QUESTION/COMMENT	NOTES
6.*	What is the software licence?	
6.a	If the licence is proprietary, will IFRC and/or NS have the right to request customization and/or regular maintenance?	
6.b	Will there be a service contract for this?	
7.	Who is governing the use of the software?	
8.	Who owns the source code for the software?	
9.	Who maintains the software?	
10	How will the hardware be managed?	
11	Is there a service level agreement for resolving issues? (e.g. security upgrades)	
12	Are there data and software backups? Is the system redundant?	
13*	Will it be a cloud service?	
13. a	Does the service meet the requirements identified in the risk assessment?	
13. b	What is the legal jurisdiction for the server?	
13. c	How does backup copying/mirroring work?	

13. d	When is data held by the service provider deleted?	
13. e	Is access management in accordance with statutory requirements and the service provider's own internal control systems?	
13.f	How does the service provider ensure that personal data from one data controller is not mixed with those of another?	
13.g	Can the service provider can use the enterprise's data for its own purposes?	
13.h	Ensure that the service provider's privacy terms (or other terms) do not exceed the provisions of the data processor agreement.	
13.i	Can you regulate the service provider's use of subcontractors, and that the enterprise has an overview of and control over such subcontractors.	
13.j	Is the use of cloud computing services audited on a regular basis? In other words, you yourself or an independent third party must perform a security audit to ensure that the data processor agreement is being complied with.	
13.k	If the agreement states that a third party is to perform the audits – will you be provided with the final audit report?	
13. l	Can the data be transferred to a new service provider if this is deemed desirable?	

13. m	Is the solution adequately documented, so that public authorities can perform an audit?	
14.	Have provisions for security and encryption been made?	
14.a	Is the data encrypted before it is stored in the cloud?	
14.b	Is communication between the data controller and the data processor encrypted?	
14.c	Is communication between the data processor and any subcontractors/data centres encrypted?	
14.d	Who holds the encryption keys?	

"Selecting enterprise software requires balancing a lot of considerations: software features, viability and support model of the vendor, total cost of ownership, capabilities in your company and your business strategy and growth expectations. Success takes investment. You will pay for your software whether you use open-source or commercial applications."

Source: https://techcrunch.com/2016/06/13/the-new-world-order-for-open-source-and-commercial-software/

Data Management

ITEM	QUESTIONS	NOTES
15.	Who are the controllers of the data?	
15.a	What does "processing of data" mean?	
15.b	Who will be the "processor of the data"?	
15.c	What is the Terms of service - standard EU agreement?	

16	How have you determined your security measures/mitigation?	
16.a	How will "The right to privacy- and family life" impact processing data within the Movement?	
16.b	What are the legal jurisdictions for the data management: storage, use and sharing of the data?	
17	If there are data backups, who is accountable to keep these up to date?	
17.a	Are the backups in the same or different legal jurisdiction?	
17.b	How many copies of the data will be kept and where? (cloud server? remote server? local server?)	
18	Will the data workflow/ system keep an audit trail and if yes to what level of detail? (who accessed it, when, where and what did the user do)	
19	What is the data workflow process?	
20*	Is it secure and does it include data minimization whenever feasible? Data minimization is the practice of collecting and keeping only the data you need.	
20.a	What are the responsible data risks and mitigation steps during each step of the data workflow?	
21	What are the guidelines for protection of the data?	
21.a	What are the training and accountability needs?	

Data Sharing

ITEM	QUESTIONS	NOTES
22	Who owns the data?	
22.a	Who has access to the data?	
22.b	Is it possible to open the data?	
23	Who can share the data?	
23.a	Is there a terms of service agreement with the party that the data was shared with?	
23.b	Is there a record of data sharing in the system and/or for the organization?	
23.c	Is there a Terms of Service and license for the data?	
24	What capabilities for import, export and exchange of data are required? And in which format?	

Things to consider

On item 6:
It will be helpful to review open source licensing - **https://opensource.org/licenses.** Keep in mind that if a university is in charge of the system, they often have a department and a regular student pipeline of people who can upgrade and maintain the system. Note that they would need to abide by the strict guidelines and not have access to the data. Use a processing agreement with strict regulation on confidentiality and privacy. And/or there would need to be a sign off process.

On item 13:
As per the upcoming ICRC Data Protection Handbook, cloud services can include risks such as the following in the context of Humanitarian Action:

- The use of services from unprotected locations;
- Interception of sensitive information;
- Weak authentication;
- Data can be stolen from the cloud service provider, such as by hackers; and
- Possible access by government and law enforcement authorities

> In addition, those Humanitarian Organisations that enjoy privileges and immunities under international law should be aware that outsourcing to a Third Party cloud service provider the Processing of Personal Data may put their data at risk of loss of such privileges and immunities.
> *Source: Upcoming ICRC Data Protection Handbook*

If you use cloud service remember there are three different models:

1. Public cloud, where the vendor makes cloud computing services available to all customers.
2. Private cloud, where cloud computing services are made available only to those businesses to which they apply. This arrangement enables a greater level of customisation than is possible in the public cloud model.
3. Hybrid cloud, which can be a combination of the models described above.

If use of cloud remember:

- To sign a data processing agreement
- Emphasis the principle of Confidentiality
- Ask for routine reporting of those who have access to the cloud
- Identify all the enterprise's systems containing personal data. Then grade the data from sensitive to non-sensitive.
- Evaluate what could go wrong.
- Assess the consequences if anything were to go wrong, e.g. that personal data falls into the wrong hands.
- Create a list of security measures that have been implemented to deal with any incidents.
- Assess the security measures in the agreement with the cloud computing service provider.

Item 20

Other common denominators that will impact your workflow:

- The principle of confidentiality
- Consent
- Data controller: a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed
- Personal data and sensitive personal data
- Processing
- Must be of general interest – the interest of the state and the population
- Red Cross as an auxiliary to the public authorities