Privacy, Data Protection and Responsible Data

Introduction

The objective of this module is to introduce champions to the key concepts they need to be familiar with in other to safely manage privacy issues and ensure the sensitive data they hold on individuals meets basic legal requirements and ethical requirements.

Learning Goals

- Understand privacy and data protection policies - including country, industry and best practice
- Look at how third part and/or cloud provider policies can effect their security

Assessment Goals

- Know which policies effect the work of the organisation
- Highlight areas the organisation must address to be able to meet privacy and data protection standards

Recommend Preparations

Print off privacy and/or relevant data protection policies for a variety of organistions, so that participants can investigate them during the training. Where possible this should also include the any that are used by the organisations that the participants represent, so that any missing features can be easily identified.

Suggested Time

45 Minutes

Notes

Data protection regualation varies greatly from country to country. Where possible, you should customise this module based on the laws that champions operate in. We have chosen to base the legal aspects of this module primarily on EU law, as it is one of the strongest global frameworks and it's likely to be mirrored in many jurisdications.

Activity

Break the participants into groups and ask them to examine and critically analyse the privacy and data

protection policies from a variety of groups, for example Google, Facebook, the UN, their own organistions etc. Ask them to feedback on:

- How easy it is or isn't to read the policies
- What each policy allows the organisation to do or not to do with it
- What they think needs to be added to make them feel more comfortable using the service or organisation

Discussion

- What does privacy mean to the participants?
- What data do they collect in their organisations?
- What expectations do they have of people who manage their data? (Give examples such as a their doctor, their bank, the government Google, Facebook etc.)
- Do they or their organisations meet these expectations for others?
- What relevant laws on data protection and privacy do they have in their country?
- Do they know of any examples of their organisation or similar organisations breaching data protection?
- What are the privacy and data protection policies of the providers they work with?

Inputs

Who's has your back?
The Electronic Frontier Foundation has developed a simple scorecard of how many (primarily US based) companies are deals with the legal aspects of user privacy.

Who Has Your Back? Government Data Requests 2017

BY RAINEY REITMAN | JULY 10, 2017

	Follows industry-wide **best practices**	Tells users about government **data requests**	Promises **not to sell out users**	Stands up to **NSL gag orders**	Pro-user public policy: **Reform 702**
Adobe	★	★	★	★	★
airbnb	★	☆	☆	★	★
amazon.com	★	☆	☆	☆	★
Apple	★	★	★	★	☆
at&t	★	☆	☆	☆	☆
COMCAST	★	☆	☆	☆	☆
CREDO mobile	★	★	★	★	★
Dropbox	★	★	★	★	★
Facebook	★	★	★	☆	★
Google	★	★	★	☆	★
LinkedIn	★	★	★	☆	★

Source: EFF "Who has your back?"

General Data Protection Regulation

There are many different privacy and data protection rules that apply to the data that you store and hold.

Because it is one of the most impacting and comprehensive, we are going to use the framework on the European Union General Data Protection Regulation.

It create's two disctinct roles and sets of responsibilities.

Data Controller: is the is the individual or entity who controls and is responsible for the for the collection and
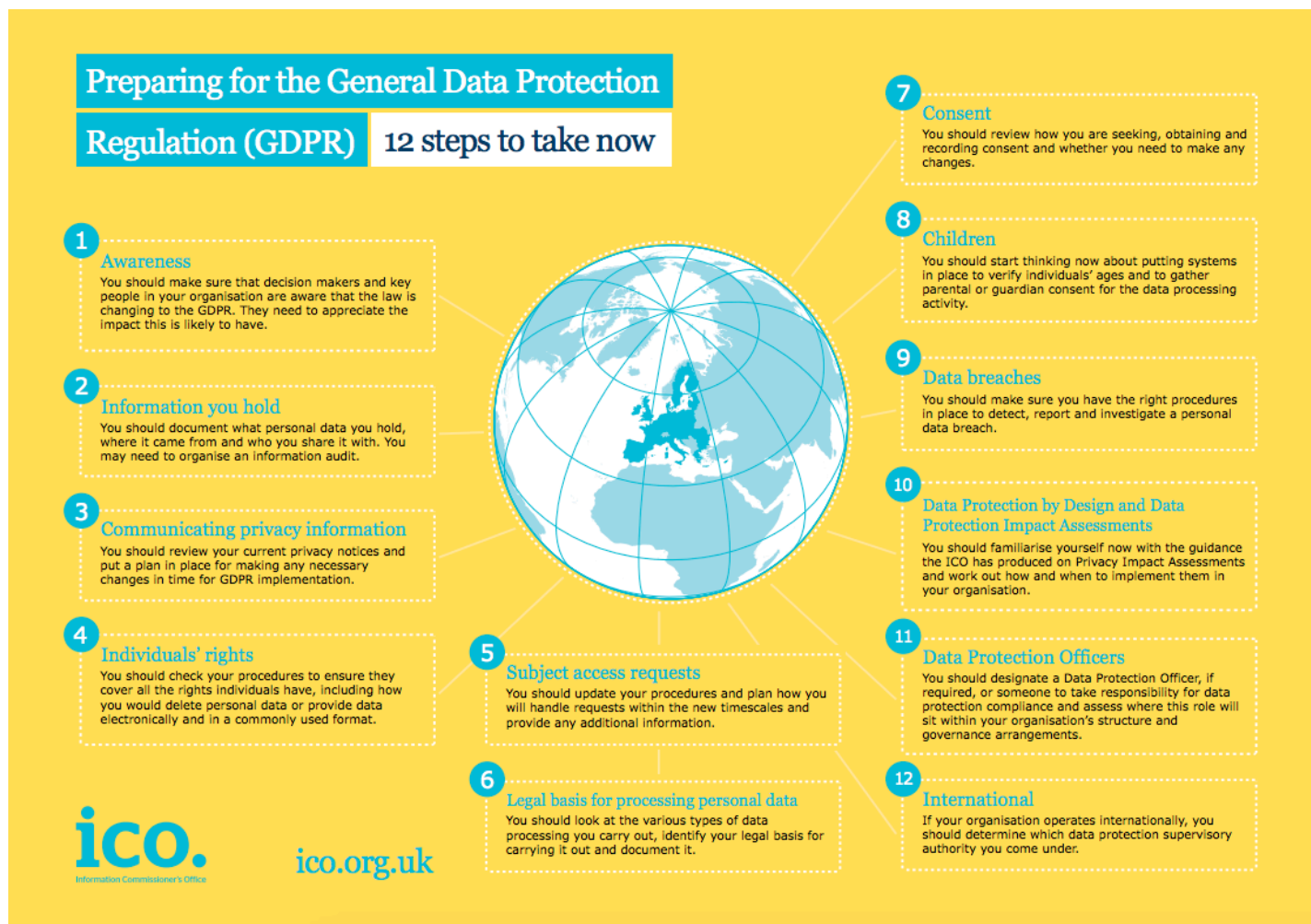
keeping of personal data. (For example, your organisation is they collect information on donors or individuals at risk.)

Data Processor: is the individual or entity who holds or processes the data but does not exercise responsibility or control over the personal data.

Many nonprofits are likely to be effected by it. Large fines for data protection failures have already been given out in the past and these are due to get bigger.

It has strong features such as:

- It's scope is very wide and includes all EU citizen data and data held by companies in the EU and/or with special arrangement outside of it
- Individuals or "data subjects" have a lot of rights including the right to be forgotten, portability, correction and to not be subject to adverse decisions caused by automated processing.
- Data protection fines can now be up to €20 million Euro or 4% of turn-over, whichever is higher
- Organisations must be clearer about why, how, where they store data and for how long
- Organisations must clearly explain their data protection policies when seeking consent. It cannot be hidden in legal jargon as part of terms and conditions.
- If collecting "sensitive" data that can identify or adversly affect an individual, they must take makes to ensure it's protection.
- Examples of protection include encryption or making the data pseudonymous or anonymous
- Data cannot be used for purposes other than the reasons that an individual agreed it to be collected for. With the exception of statistics, legal or public health purposes.

Preparing for the General Data Protection Regulation (GDPR) — 12 steps to take now

1 Awareness
You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have.

2 Information you hold
You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit.

3 Communicating privacy information
You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.

4 Individuals' rights
You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.

5 Subject access requests
You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.

6 Legal basis for processing personal data
You should look at the various types of data processing you carry out, identify your legal basis for carrying it out and document it.

7 Consent
You should review how you are seeking, obtaining and recording consent and whether you need to make any changes.

8 Children
You should start thinking now about putting systems in place to verify individuals' ages and to gather parental or guardian consent for the data processing activity.

9 Data breaches
You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.

10 Data Protection by Design and Data Protection Impact Assessments
You should familiarise yourself now with the guidance the ICO has produced on Privacy Impact Assessments and work out how and when to implement them in your organisation.

11 Data Protection Officers
You should designate a Data Protection Officer, if required, or someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements.

12 International
If your organisation operates internationally, you should determine which data protection supervisory authority you come under.

ico.
Information Commissioner's Office

ico.org.uk

Source: UK Information Commissioner Office

Responsible Data

A number of civil society groups have been jointly working to share lessons and best practices for gathering and using data. This is known as the "Responsible Data" Project.

The group has defined that the responible use of 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."*

The project has created a handbook designed specifically for helping civil society groups develop, manage and close projects that hold sensitive information. It covers everything from survey choice to selecting hosting providers.
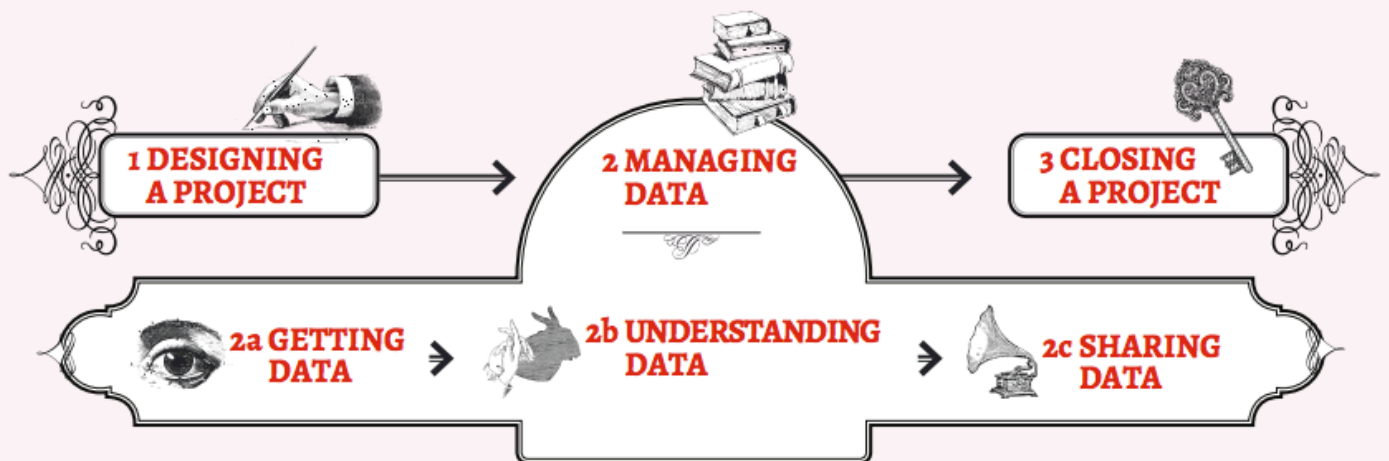
Source: [The Responsible Data Handbook](#)

Deepening

Based on the outline of the GDPR, or other relevant legislation, along with the principals of Responsible Data. Split the participants into groups and give them a task to design a project taking into consideration all of these aspects. Example projects might include topics such as:

- The setup of a new fundraising database which holds lots of information about potential new donors
- A hostedd database that aims to record testimony and incident reports from victims of topic likely to contain sensitive data about a topic such as domestic and sexual assault
- A new system in your organisation for managing recruitment, payroll, disciplinary action, social security information - all of which is stored with a third party in their cloud

Synthesis

Participants should turn to their assessment documentation and consider how their organisation deals with the subject matter covered in this module. Where necessary they should ask questions and work with other participants to identify any:

- Issues they have found that effect their organisations
- Possible solutions they have learned
- Possible difficulties they may face in implementation (ideally using the time ad experience of trainers and other participants)
- Things would need to overcome these difficulties
- Connections to other organisations or individuals that would help them
- Timeline, resources and costs for implementation

This should be noted in their assessment, for future use.

In line with keeping this curriculum as an updated community tool, we would also ask that participants provide comments, feedback and new ideas for this module on the project website and/or Github!

Resources

- [Responsible Data Handbook](#)
- [Facebook Privacy Policy](#)
- [Google Privacy Policy](#)
- [Twitter Privacy Policy](#)
- [United Nations Privacy Policy](#)
- [The Guardian Privacy Policy](#)
- [Open Whisper Systems Privacy Policy](#)
- [Tor Project Privacy Policy](#)
- [Comparing the privacy policy of internet giants side-by-side](#)
- [DLA Piper - Data Protection Laws of the World](#)
- [European Union - General Data Protection Regulation](#)
- [Privacy Policy Generators](#)
- [Guide for System Administrators in At-Risk Organizations: Ensuring User Data Protection and Privacy](#)