

GDPR: Briefing for foundations

Emma Hutchins

Senior Policy and Communications Officer, ACF

emma@acf.org.uk

Webinar overview

Introduction to the GDPR

Answering common questions

Other support available

Questions from participants

Introduction to the GDPR (I)



About the GDPR

- 25 May 2018
- EU citizens' data (regardless of your organisation's size or location)
- Enforced in the UK by the Information Commissioner's Office

Introduction to the GDPR (II)



Key features

- A set of principles, not rules
- More rights for individuals
- Accountability:
 - “the controller shall be responsible for, **and be able to demonstrate**, compliance with the principles.”
- Greater fines for non-compliance

Key definitions

Q. What constitutes personal data?

A. Any information which can be used to identify an individual directly or indirectly.

- Special categories of data include genetic and biometric data plus political opinions, religious belief, etc.
- Individual acting as the primary contact? TBC...

Key definitions

Q. What constitutes marketing materials?

A. Newsletter, event invitations, publicity for a new grants programme – if they could be seen to promote your aims and ideals.

- To send direct marketing:
 - By electronic means – refer to PECR
 - By post – consent or legitimate interests

Q. How does it apply retrospectively?

A. Foundations will have to look at what the lawful basis is for processing pieces of data and whether it still applies. E.g. If relying on consent, it would need to be up to standard.

Principles

The principles

- Lawful, fair, transparent
- Adequate, relevant, limited to what is necessary
- Accurate and up to date
- Time-restricted
- Secure

Largely the same as under the Data Protection Act

Principles (II)

Q. Is it sufficient to put our privacy notice on our website?

A. Not generally. You'll need to draw attention to it. There is potentially scope for a layered approach (e.g. full notice on the website and signposting/excerpts on forms)

Q. What should our privacy notice include?

- Details of the data controller
- Purpose and lawful basis for processing
- Right to withdraw consent (if applicable)
- Legitimate interests (if applicable)
- Retention period
- Individuals' rights (and how to exercise them)
- [And more](#)

Lawful bases for processing

Q. Which lawful basis best covers our grant-making?

A. For you to decide in your circumstances.

The lawful bases are:

- Consent
- To perform or enter into a contract
- To comply with a legal obligation
- To protect the vital interests of a data subject
- To perform a task in the public interest
- Legitimate interests

Lawful bases for processing (II)



Consent

- Clear and specific statement
- Granular
- Clear and concise language
- Make it easy to withdraw consent
- Keep evidence
- Keep under review
- Avoid making it a pre-condition of a service

Lawful bases for processing (III)



Legitimate interests assessment

3 parts:

1. Identify the legitimate interest
2. Show that the processing is necessary to achieve it
3. Balance it against the individual's rights, interests, and freedoms

Checklists

- We have checked that legitimate interests is the most appropriate basis.
- We understand our responsibility to protect the individual's interests.
- We have conducted a legitimate interests assessment (LIA) and kept a record of it, to ensure that we can justify our decision.
- We have identified the relevant legitimate interests.
- We have checked that the processing is necessary and there is no less intrusive way to achieve the same result.
- We have done a balancing test, and are confident that the individual's interests do not override those legitimate interests.
- We only use individuals' data in ways they would reasonably expect, unless we have a very good reason.
- We are not using people's data in ways they would find intrusive or which could cause them harm, unless we have a very good reason.
- If we process children's data, we take extra care to make sure we protect their interests.
- We have considered safeguards to reduce the impact where possible.
- We have considered whether we can offer an opt out.
- If our LIA identifies a significant privacy impact, we have considered whether we also need to conduct a DPIA.
- We keep our LIA under review, and repeat it if circumstances change.
- We include information about our legitimate interests in our privacy notice.

Individuals rights

Individuals have the following rights under the GDPR:

- The right to be informed
- The right of access
- The right to rectification
- The right to erase
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

Q. What do we do in response to a subject access request?

A. Provide data you hold on them in a relevant filing system for free within one month. Embarrassment is not an exemption!

Accountability and governance



Q. Do we need to appoint a Data Protection Officer?

A. Public authorities, those undertaking large scale systematic monitoring, or those processing sensitive data on a large scale as a core activity need to appoint a DPO. Otherwise avoid using the term.

Q. What is a reasonable timeframe to hold data?

A. For you to assess and document in a data retention schedule. Ask ‘what would the individual think is reasonable?’

Application: Foundation practice



Q. Will this restrict our ability to collaborate with other foundations?

A. No, but it is vital to consider how data is processed and who is responsible.

Q. Can we continue to hold data for archives/historical purposes?

A. GDPR applies to the data of living people only. Data held for archiving purposes only should be fine if it is *not* being actively processed.

Further support

Q. What support is available from the ICO?

- [Guide to the GDPR](#)
- [FAQs for charities](#)
- [Support for small organisations](#)
- [12 steps to take now](#)
- [Myth busting blogs](#)
- [Data audit template](#)
- [Helpline](#): 0303 123 1113 and select option 4

Further support (II)

Q. What support is available from ACF?

- [Briefing](#)
- [Area on our website](#)
- [Events](#) – Monitoring and evaluation network, Smaller funders' network
- [LinkedIn group](#)

Further support (III)

Q. Where else can we find support?

- Fundraising Regulator
- NCVO
- Institute of Fundraising
- Paul Ticher (independent consultant)

Your questions



Thank you for joining us



The recording and presentation will be made available shortly

Please fill in the evaluation forms which Leah will send after the webinar