# The General Data Protection Regulation

Briefing Note
September 2017

## What is it and what can you do to prepare for it?

**The General Data Protection Regulation (GDPR) will replace the UK Data Protection Act 1998 (DPA) from 25 May 2018. The GDPR will apply across Europe, regardless of the UK's decision to leave the EU.**

**The new regulation strengthens the rights of individuals to access and amend their personal data; places greater emphasis on an organisation's accountability; and introduces more serious consequences for non-compliance, including fines.**

### Key definitions

**Personal data** means any data which relates to a living individual who can be identified from the data, or from the data and other information that is in, or likely to come into the, possession of the data controller.

The GDPR covers personal data kept on employees, volunteers, service users, members, supporters and donors.

**Sensitive data** means personal data consisting of information about the racial/ethnic origin of the subject; political opinions; religious or similar beliefs; whether they are member of a trade union; physical or mental health; sexual life; commission (including alleged) of any offence committed; proceedings for any offence committed (including alleged).

The **Data controller** is the company, organisation or individual who holds personal data and determines the purposes and manner in which it will be processed.

For example an organisation, a GP or pharmicist.

The **Data processor** is any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

For example a market research company or payroll company.

For more information on key definitions visit the **Information Commissioner's Office (ICO) website.**

### Key Principles

The GDPR requires organisations to comply with eight principles relating to the rights of individuals:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- The right not to be subject to automated decision-making, including profiling

The GDPR states that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specific, explicit and legitimate purposes and not used in a manner incompatible to the original purpose



Continued overleaf

- Adequate, relevant and limited to what is necessary
- Accurate, up to date and amended in a timely manner if necessary
- Kept in a form which allows identification for no longer than is necessary
- Kept secure

And that requests from individuals for access to their data must be responded to within one month and for free unless the requests are 'excessive' or 'unfounded'.

## Lawful Basis

In order to use personal data you need to identify a lawful basis, also called 'condition for processing', and document it. There are six lawful bases for processing data including 'consent' and 'legitimate interests'.

For more information on lawful bases visit the **ICO website.**

## Consent and privacy statements

Consent must be informed and freely and explicitly given. **Pre ticked boxes or 'opting out' will not be good enough.** Evidence of consent must be kept and should be easy for people to withdraw at any time, for example by unsubscribing from emails.

Privacy statements must be written in plain English, be easily accessible and include:

- What information is being collected?
- Who is collecting it?
- How is it collected?
- Why is it being collected?
- How will it be used?
- Who will it be shared with?
- What will be the effect of this on the individuals concerned?
- Is the intended use likely to cause individuals to object or complain?

For more guidance on privacy statements visit the **ICO website.**

## Legitimate Interests

Personal data can be processed (without consent) if there are 'legitimate interests' for doing so, and if the interests of the processor are balanced against those of the individual. For example, email marketing may be regarded as being under 'legitimate interest'.

## Getting ready for the GDPR - what should I do now?

(From knowhownonprofit.org)

- Make sure trustees and senior management know the GDPR is coming
- Identify what data you currently hold and where it came from. Document and keep your findings
- Make sure your privacy notices are written clearly and easily accessible
- Put systems in place to respond to requests for access or updates to personal data or for the data to be deleted (called 'subject access requests')
- Understand and document what your 'lawful basis' is for storing and using personal data
- Review and update how you seek and manage consent
- Think about extra protections for under 16s
- Put procedures in place to report a data breach to the ICO within 72 hours if necessary, and make sure all staff understand what constitutes a data breach
- Build 'privacy by design' into new projects and undertake data protection impact assessments where relevant
- Have a named person responsible for data protection
- If you're a fundraiser, make sure you follow the latest guidance from the Fundraising Regulator
- Take the ICO self assessment online

## Useful information

- Information Commissioner's Office website ico.org.uk
- Third Sector GDPR Hub www.thirdsector.co.uk/gdpr
- NCVO Guidance knowhownonprofit.org/
- Institute of Fundraising www.institute-of-fundraising.org.uk

**Contact**
**Anne Fry**
**Communications Manager, VONNE**
- **Email:** anne.fry@vonne.org.uk
- www.vonne.org.uk
- **Tel:** 0191 233 2000