RUSSELL-COOKE | SOLICITORS

# Data protection for fundraisers

3 July 2018

Carla Whalen, Associate

@RCcharityteam

# Overview

- **Legislation**
  - What's in force and what's in the pipeline?
- **Guidance**
  - ICO, Fundraising Regulator, Institute of Fundraising
- **ICO investigations** into charity fundraising
- **Lessons learned**
- **What now?**

# Data protection – the legislation

- **General Data Protection Regulation** (GDPR) – replaced the Data Protection Act 1998
- **Data Protection Act 2018** (DPA) – implements EU Law Enforcement Directive, supplements GDPR, extends data protection laws to areas not covered by GDPR
- **Privacy and Electronic Communications Regulations 2003** (PECR) additional restrictions on direct marketing by electronic means (email, text, internet messaging, telephone)
- **European Union (Withdrawal) Bill** – will transpose the GDPR into UK law when we leave the EU

# Data protection – fundraising guidance

- Information Commissioner's Office (**ICO**)
  - Supervisory authority for data protection in UK
  - Investigations, information and enforcement notices, monetary penalties, prosecutions
- Fundraising Regulator
  - 'GDPR library'
- Institute of Fundraising (**IoF**)
  - Connecting People to Causes: a practical guide to fundraising research

# Fundamentals

- **Personal data –** information relating to a living person who is identified (or can be identified) from that information
- **Special categories of personal data** race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation
- **Controller –** person or body that determines the purposes and means of processing personal data
  - Joint controllers
  - Controllers ‘in common’
- **Processor –** person or body which processes data on behalf of a data controller

# Fundamentals – lawful processing

- Controllers must have a valid **lawful basis** to process personal data:
  - consent, performance of a contract, compliance with a legal obligation, vital interests, public task, legitimate interests
- Must identify an additional specific condition if processing **special category personal data**:
  - explicit consent, obligations under employment/social security/social protection law, substantial public interest etc.
- **Criminal offence data** – DPA 2018 (similar to lawful basis for processing special category personal data)

# ICO charity fundraising enforcement action

- ICO investigated charity fundraising practices between 2015 - 2017 and 13 charities fined
- What did they do?
  - **Wealth profiling –** carried out by external companies *without the donor knowing*
  - **Data matching** – the donor has a right to choose what personal information they give to the charity
  - **Data sharing –** sharing supporter records with other charities *without knowing* which charities received the information and *without the donor knowing*

# Data protection in 2018 – a new approach

- **Transparency** and **accountability**
  - Data controller will be **responsible for**, and must be able to **demonstrate compliance** with, the principles relating to processing of personal data
- **Record keeping** – some exceptions for organisations with <250 employees
- **Privacy by design and default** (e.g. data minimisation, pseudonymisation, anonymisation, creating and improving security features)
- **Data Protection Officers** and **Data Protection Impact Assessments** (DPIAs)

# Individuals' right to be informed

- Data controller must provide privacy information at the time personal data are obtained (free of charge)
- Privacy notice – must include:
  - **Identity** and contact details of **data controller**
  - Contact details of data protection officer (where applicable)
  - **Purposes** of intended processing and legal basis (if legitimate interest, provide information)
  - **Recipient(s)** of personal data
  - Transfer to third country or international organisation (where applicable)

# Third-Party Data Processors

- Art. 28 – only use processors providing "**sufficient guarantees**" that processing will meet GDPR requirements and ensure protection of individual rights
- Processing by data processor must be governed by a contract with the data controller, to include:
  - subject-matter and duration of processing
  - nature and purpose of processing
  - type of personal data and categories of data subjects
  - obligations and rights of the controller

# Lessons learned

- **Transparency is key –** charity fundraisers need to:
  - Know what lawful basis is being used to process people's personal data
  - Understand the difference between consent and legitimate interests
  - Understand how PECR impact on fundraising communications
  - Understand how and when to issue privacy notices
  - Only do what the privacy notice says you'll do with people's personal data
  - Keep privacy notices under review

# What now?

- **Increased public awareness**
  - Giving control to the individual
  - Supporters asking questions about use of personal data and reading privacy notices?
  - Increase in supporters asking to exercise individual rights (e.g. right to object, right to access)?
- **ICO enforcement action**
  - Expectation that charities will have learned from 2015-2017 investigations and outcomes
  - Stronger enforcement action? Higher fines?

# GDPR – rights of individuals

- Right of **access** – subject access requests
- Right to **rectification** – if data is inaccurate or incomplete
- Right to **erasure** – 'right to be forgotten'
- Right to **restrict processing** – storage only
- Right to **data portability** – moving data from one IT environment to another
- Right to **object** – includes right to object to direct marketing and other legitimate interest processing
- Rights re: **automated decision making** and **profiling**

# ICO – notification of breach

- GDPR requires controllers to **notify the ICO of a personal data breach**
  - If it is likely to result in risk to rights and freedoms of individuals
  - Without undue delay and, where feasible, not later than 72 hours after becoming aware of it
- If data breach **likely to result in high risk to rights and freedoms** of an individual, controller must also **communicate the breach to the individual** without undue delay

# Checklist

- Staff training and awareness
- Policies and procedures (including breach reporting)
- Contracts with processors
- Seek feedback from supporters
- Keep privacy notices under review
- Spot-checks and mini-audits
- Ask for help if there’s something you don’t understand

# Contact

Carla Whalen
Associate Qualified in Scotland
T: +44 (0)20 8394 6419
carla.whalen@russell-cooke.co.uk

Russell-Cooke is a top 100 firm with around 200 highly regarded specialist solicitors and lawyers. We advise a mix of commercial and not-for-profit clients.