MeLearning
Learning made easy

# GDPR – what the Accountability principle means for charities

Open Forum Event

Piers Clayden

1 November 2017

Clayden | Law

# General Data Protection Regulation – some context and background

- GDPR is a challenge for charities
  - Lack of clear guidance is the biggest challenge (*IOF Survey Sept 2017*)
- GDPR and Brexit?
- No significant exemptions for charities
- GDPR – evolution not revolution

Clayden | Law

# Accountability Principle – an introduction

- A new addition to the current DPA regime
- Controllers must be able to ***demonstrate*** compliance with all of the 6 data processing principles
- Compliance is no longer a tick box/form filling exercise
- Not just complying but ***showing*** you comply
- New operational requirements will result in increased bureaucracy and costs
- Will require continual review and updating
- Enshrines good “data governance” concepts

# Training

- Staff (employees as well as volunteers) training is an organisational measure that can demonstrate compliance
- Auditable and verifiable
- Added benefit of increasing awareness of staff about responsibilities and mitigating risk of fines, decline in donations and reputational damage

# The e-learning suite

| COURSE | Core (all employees) | Foundation (executing the policies) | Practitioner (leading the project) | Board |
|---|---|---|---|---|
| 1. GDPR – Introduction and Background | ✓ | ✓ | ✓ | ✓ |
| 2. GDPR – Definitions and Principles | ✓ | ✓ | ✓ | |
| 3. GDPR – Individual Rights | ✓ | ✓ | ✓ | |
| 4. GDPR – Consent and Conditions for Processing | | ✓ | ✓ | |
| 5. GDPR – Steps to Compliance | | ✓ | ✓ | ✓ |
| 6. GDPR – The Accountability Principle | | | ✓ | |
| 7. GDPR – Sanctions, Remedies and Liabilities | | | ✓ | ✓ |
| 8. GDPR – Information (Privacy) Notices | | ✓ | ✓ | |
| 9. GDPR – Breach Management and Notifications | | ✓ | ✓ | |
| 10. GDPR – Supply Chain Management | | | ✓ | |
| 11. GDPR – Data Sharing | | | ✓ | |
| DURATION | 1h 30m | 3h 30m | 5h 30m | 1h 30m |

# Privacy by Design & Default

- Appropriate safeguards must be integral to data processing activities, not just an afterthought
- Some proportionality allowed in light of costs and risks
- Must aim for data minimisation – ie. only process the minimum amount of personal data needed for the purpose
- Also minimise storage (retention) periods as well as data accessibility
- Be proactive – “bake in” data protection into practices, systems and policies

# Privacy Impact Assessments

- A PIA is required prior to data processing which is likely to result in high risk for individuals' rights and freedoms
  - Eg – automated processing for profiling; large scale processing
- PIA to contain:
  - Description and purpose of the processing
  - Assessment of necessity and proportionality
  - Assessment of the risks to rights and freedoms
  - Risk mitigation measures

# Data Protection Officer

- Mandatory for certain organisations (unlikely to cover charities)
- But voluntary DPO appointment is a good way to demonstrate compliance
- Where appointed, DPO must:
  - Have sufficient seniority and expertise to perform the role
  - Be properly resourced to do the role and allowed to do so independently
  - Report into the highest executive level
  - In essence, be a “privacy guardian” and monitor GDPR compliance
- DPO is protected from dismissal for performing his/her tasks

# Service Providers

- High duty of care in selection of external service providers who handle personal data on behalf of charity (data processors)
- Includes cloud IT providers, external fundraisers, wealth screening BUT also volunteers
- Charities will be liable for damage caused by data processors unless can show that charity was “not in any way responsible” for the event
- So incumbent on charities to do due diligence on service providers to check they offer “sufficient guarantees” (resources and expertise) on GDPR compliance
- Contracts have to be in writing and include prescribed obligations

# Record keeping

- In addition to the records needed to demonstrate previous compliance obligations, charities required to keep a record of processing activities:
  - Purposes of processing
  - Categories of data processed
  - Categories of third party recipients
  - Retention periods
  - Description of technical and organisation security measures
- Exemption if employ less than 250 BUT only if not processing sensitive or high risk data

# Thank you!

Any questions?

Contact details:
Piers@claydenlaw.co.uk
www.claydenlaw.co.uk