

Preparing for GDPR

What is it and how will it affect you?

Fiona Brookes (presenting), with:

Craig Humphries, Iain Pritchard, and Paul Sypko (on Q&A panel)

13 July 2017

Purpose of the session

- Provide an overview of the EU General Data Protection Regulation (GDPR) and how it extends beyond the Data Protection Act
- Explore the practical implications for not-for-profit organisations
- Understand what preparation is needed
- Share experiences and put questions to Adapta's panel of data protection experts

Adapta Consulting

- A specialist information systems consultancy
- We only work with membership organisations, charities, associations, trusts and others in the NfP sector
- We are completely supplier-independent
- Our consultants have held senior positions in a broad range of different organisations
- Our advice and guidance is based on practical experience gained over many years

Data Protection – a potted history

DPA
1984

DPA
1998

PECR
2003

GDPR
25 May 2018

Will be replaced by GDPR

Will be updated in time for GDPR

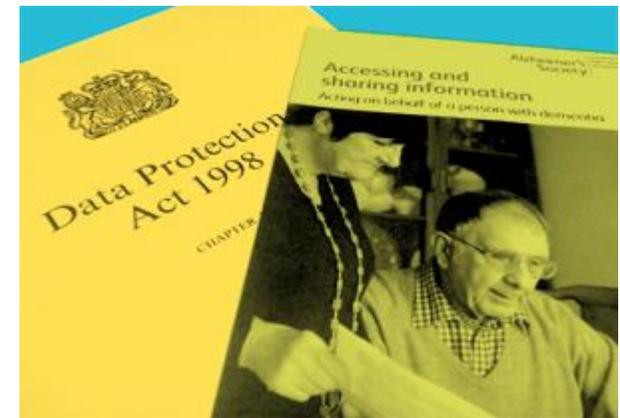
Will apply regardless of Brexit

ePR
2018

Complying with the Data Protection Act

When processing personal and sensitive personal data we have to comply with the 8 principles which are

1. Data must be collected lawfully and fairly
2. It must be used only for specified purposes
3. The quantity of data collected should be appropriate
4. The data should be accurate and up to date
5. It should be kept only as long as necessary
6. It should be processed in accordance with the rights of those it concerns
7. It should be kept securely
8. It should not be transferred out of the EEA unless it is to an area which has similar standards



Summary of relevant changes GDPR brings

Breaches

- Increased fines
- Civil and criminal liability
- Reported within 72 hours

Consent

- Valid
- Recorded
- Freely given freely
- Parental
- Retrospective
- Recent

Governance & accountability

- Data Protection officer
- Show how you comply
- Keep records of processing activities
- Privacy by design
- Know your personal information
- Data processors

Users rights

- To be informed
- Subject access
- Erasure
- Data portability
- Rectification

Increased right to be informed

- Identity and contact details of the controller and the data protection officer
 - Purpose of the processing and the legal basis for the processing
 - The legitimate interests of the controller
 - Categories of personal data
 - Any recipient or categories of recipients of the personal data
 - Details of transfers to third country and safeguards
 - Retention period
 - The existence of each of data subject's rights
 - The right to withdraw consent at any time
 - The right to lodge a complaint
 - The source the personal data originates from
 - Whether the provision of personal data is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data
 - The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences
- Concise, transparent, intelligible and easily accessible
 - Written in clear and plain language, particularly if addressed to a child
 - Free of charge

Get ready for GDPR

1. Raise awareness

4. Document your data handling processes

7. Issue & collect revised data processor agreements

10. Develop a personal information register

2. Appoint a DPO

5. Determine lawfulness & legal basis for processing

8. Move to full channel specific opt-ins for DM communications

11. Provide GDPR compliance training

3. Undertake a compliance review

6. Determine consent strategy

9. Revise your data protection documents

12. Implement a plan for ongoing compliance

Panel Discussion



Questions & Answers



Thank you

This presentation is available to download from the Adapta website
www.adaptaconsulting.co.uk

