m~hance
with you all the way

GDPR

(what difference will it make….?)

11 May 2017

adapta

Purpose of the session

- To summarise and explain the changes in data protection obligations that have followed the introduction of the General Data Protection Regulation (GDPR)

- To explore and discuss some of the implications for organisations in the sector

adapta

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

adapta

Data Protection – a potted history

DPA
1998

Will be replaced by GDPR

PECR
2003

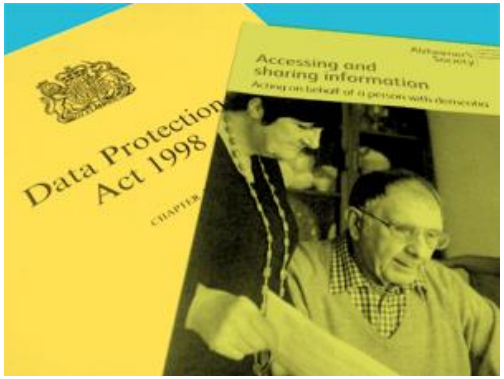
Will be updated in time for GDPR

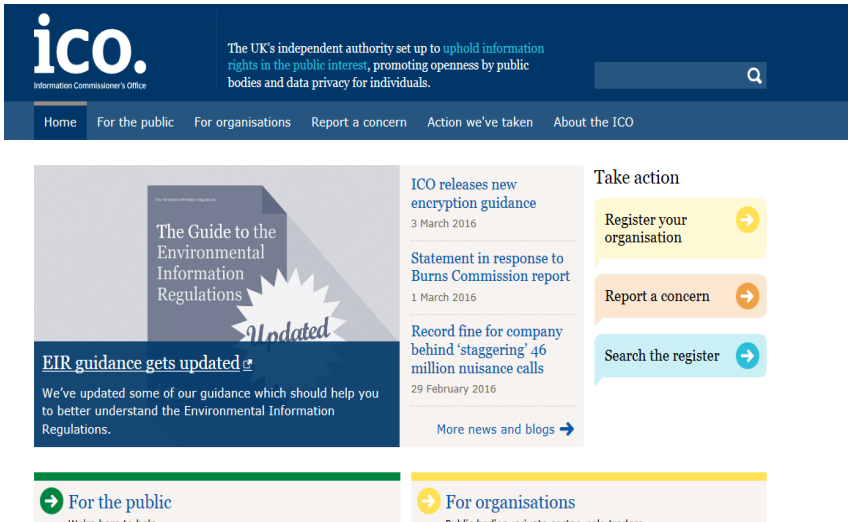
GDPR
25 May 2018

Will apply regardless of Brexit

Data protection

- Data Protection Act 1984 and 1998 – in place for 30+ years
- Provides rules for organisations that collect and use personal information – applies to manual and electronic records
- EU General Data Protection Regulation (GDPR) comes into force in May 2018 …. regardless of Brexit
- GDPR builds on DPA but there are significant changes too





adapta

When things go wrong … some recent sector examples

- The British Heart Foundation - secretly screened millions of their donors so they could target them for more money - £18,000 fine
- The RSPCA - secretly screened millions of their donors so they could target them for more money - £25,000 fine
- The Alzheimer's Society - volunteers used personal email addresses to receive and share information about people who use the charity, stored unencrypted data on their home computers and failed to keep paper records locked away. They were not trained in data protection, the charity's policies and procedures were not explained to them and they had little supervision from staff – enforcement
- The British Pregnancy Advice Service – exposed thousands of personal details to a malicious hacker - £200,000 fine

The ICO issued fines of £6K- £18k to 11 charities earlier this year for a combinations of breaches which included sharing data with other charities, finding out information about people that they didn't provide, and ranking people according to their wealth.

This included the **NSPCC**, **GOSHCC**, **Oxfam**, **Macmillan Cancer Support**, **WWF-UK**, the **Royal British Legion**, **Guide Dogs for the Blind Association**, **Cancer Support UK**, **Cancer Research UK**, **Battersea Dogs and Cats' Home**, **The International Fund for Animal Welfare**

When things go wrong … more examples, common mistakes

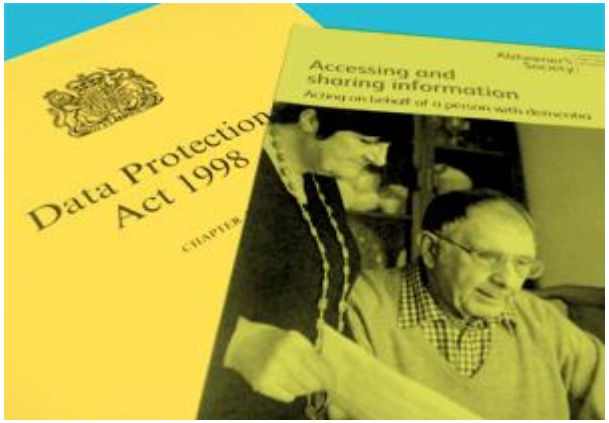
- The Nursing and Midwifery Council … lost dvds … unencrypted.. £150k fine
- North East Lincolnshire Council … missing unencrypted memory stick …£80k fine
- Greater Manchester Police … stolen USB stick … unencrypted, no password protection … £150k fine
- Royal Veterinary College … loss of a memory card … signed undertaking
- Surrey County Council … misdirected emails

  with attached files … not encrypted or password protected … £120k fine
- North Somerset Council … sent unencrypted

  emails with personal data to wrong NHS employee … £60k fine

adapta

Complying with the 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

adapta

What changes with GDPR

Right to be informed

Faster subject access

Faster reporting of data breaches

Right to erasure

Data protection impact assessments

Active consent

Right to rectification

€20 million fines

Portability

Demonstrate consent

Recent consent

Accountability & governance

Privacy by design

adapta

Changes – breaches

DPA

- Fines of up to £500k
- Comparatively low-profile penalties (historically)

GDPR:

- Penalties likely to be higher profile (consequent reputational risk)
- Fines of up to 4% of annual global turnover or 20 million euros (whichever is greater)
- Civil and criminal liability for officers and key employees
- High risk data breaches must be reported to the supervisory authority within 72 hours

Changes – governance & accountability

- New **accountability** requirement - GDPR requires you to show **how** you comply with the principles
- Appropriate technical and organisational measures are needed to ensure and demonstrate that you comply e.g. internal data protection policies such as staff training, internal audits of processing activities, impact assessments
- Records of processing activities must be kept where processing personal data that could result in a risk to the rights and freedoms of individuals

Changes – consent

- **Valid consent** to process personal data will be needed instead of implicit consent - a person has actually done something actively to provide their consent
- **Pre-ticked opt in** boxes and empty opt-out boxes (which have to be ticked by the person in order to opt out) will no longer be sufficient
- **Demonstrate** that consent has been given
- **Consent must be given freely** - performance of a contract must not depend upon consent being given when the processing is not actually required to perform the contract
- **Parental consent** will be required to process the personal data of children under the age of 16 (or possibly 13)

DPA definition: "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed"

GDPR definition: "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her"

adapta

Changes – the right to be informed

Subjects have the right to be informed about …..

• Identity and contact details of the controller and where applicable, the controller's representative, and the data protection officer • Purpose of the processing and the legal basis for the processing • The legitimate interests of the controller or third party, where applicable • Categories of personal data • Any recipient or categories of recipients of the personal data • Details of transfers to third country and safeguards • Retention period or criteria used to determine the retention period • The existence of each of data subject's rights • The right to withdraw consent at any time, where relevant • The right to lodge a complaint with a supervisory authority • The source the personal data originates from and whether it came from publicly accessible sources • Whether the provision of personal data 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 •

Information about the processing of personal data must be:

- Concise, transparent, intelligible and easily accessible
- Written in clear and plain language, particularly if addressed to a child
- Free of charge

adapta

Changes – users' rights

- **Subject access** – usually within a month and for no fee
- **Right to erasure** - right to be forgotten … a data subject has the right to request personal data is erased when it is no longer being processed
- **Data portability** - personal data must be in a format where it can be easily and electronically transferred to another processing system
- **Right to rectification** – if personal data is inaccurate or incomplete

Changes – data processors

- Data processors will have direct and increased responsibilities - they can be held responsible for data breaches

- There is still a responsibility on your organisation to ensure that:
  - Contracts with data processors comply with GDPR
  - You choose appropriate data processors
  - Data processors comply with data protection and the GDPR

Changes – privacy by design

- Compliance must be considered in the design and implementation of all processes, from start to finish
- Data protection can no longer be an afterthought
- Data Protection Impact Assessments (DPIA) must be undertaken when appropriate (e.g. when using new technologies and the processing is likely to result in a high risk to the rights and freedoms of individuals)

Get ready for GDPR compliance

- Develop a strategy for obtaining consent – and a practical as well as legal level of granularity
- Consider and document the legal basis for holding personal data
- Be able to evidence consent
- Plan for subjects' increased right to be informed – know your data and data handling processes
- Update existing and develop new data protection policies and procedures for GDPR compliance …. and implement
- Train staff on GDPR requirements, revised policies and procedures
- Design and integrate a 'privacy by design' approach (e.g. for procurement of products and services, and data and digital development projects)

adapta

m~hance
with you all the way

Questions, comments and a bit of discussion..?

adapta
adapta