Preparing for GDPR

What is it and how will it affect you?

Iain Pritchard

Craig Humphries

20 June 2017

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)
- Explore some of the practical implications of the changes and the choices that organisations need to consider
- To share tips on how to identify areas for change
- To share experiences, ask questions

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
1998

Will be replaced by GDPR

PECR
2003

Will be updated in time for GDPR

GDPR
25 May 2018

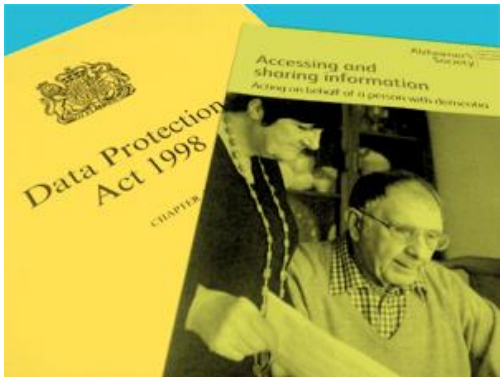
Will apply regardless of Brexit

adapta

iAm

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



When things go wrong … some recent sector examples

- The British Heart Foundation - screened millions of their donors so they could target them for more money - £18,000 fine
- The RSPCA - 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**

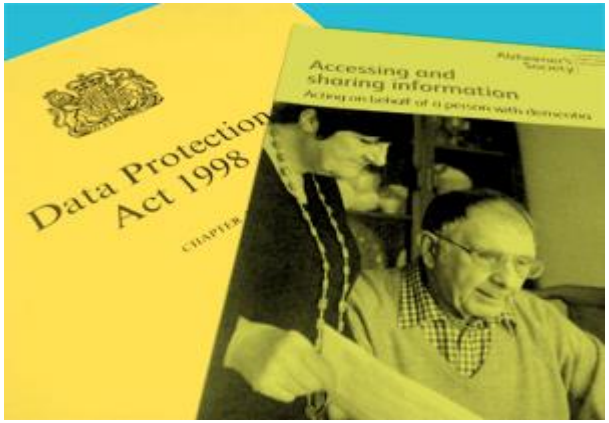
When things go wrong … more examples, common mistakes

- 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

iAm

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

iAm

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

Privacy by design

Accountability & governance

adapta

iAm

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 to have 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"

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

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)

Areas to consider for change

- Awareness
- Accountability
- Information to hold
- Data protection by design
- Data protection officers
- Lawful basis
- Consent
- Children
- Communication policy
- Individuals' rights
- Subject access
- Data breaches
- International transfer of data

Awareness

- Designate a person to take responsibility for GDPR compliance within your organisation
- Raise awareness of GDPR within your organisation
- Provide regular staff, volunteers and Board training on GDPR requirements
- Review employee and volunteer policies, Board induction pack, guidance and procedures for GDPR compliance coverage

Accountability

- Consider your existing data protection governance arrangements (e.g. risk and assurance)

- Implement any new measures that can demonstrate you comply, such as:
  - internal data protection policies,
  - internal audits,
  - new reports to support demonstration of assurance,
  - staff training,
  - reviews of internal HR policies.

Information you hold

You must maintain internal records of processing activities.

- Consider undertaking a data audit
- Document the data you hold, record the source of the data, and record the details when personal data is shared (e.g. 3rd party marketing agency, mailing houses and data cleaning agencies)
- Consider creating process maps of all data related activities
- Create or review your existing data retention schedules – check they adhere to your data protection policy

Please note: there are differing requirements related to the information to be maintained for organisations with above and below 250 employees

adapta

iAm

Data Protection by design

- Raise staff awareness and implement training to support the organisation in taking a Data Protection by Design approach (e.g. how to prepare a data protection impact assessment - DPIA)

- Review and update your existing policies and procedures to support Data Protection by Design (e.g. data protection impact assessments being part of procurement and project initiation activity)

- Consider how you will demonstrate that Data Protection by Design has been considered

Please note: The ICO provide a DPIA template on their website: https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

Data Protection Officers

Formally appoint a designated DPO if your organisation:

- is a public authority (except for courts acting in their judicial capacity)

- carries out large scale systematic monitoring of individuals (for example, online behaviour tracking) **or**

- carries out large scale processing of special categories of data or data relating to criminal convictions and offences.

The ICO perspective:
"someone in your organisation, (or an external data protection advisor), takes proper responsibility for your data protection compliance and has the knowledge, support and authority to do so effectively"

adapta

iAm

Lawful basis for processing personal data

- Review all your data processing activities and consider the lawful basis for carrying out the activity

- Document, for future accountability purposes, the legal basis for each personal data processing activity

Consent

- Consider your organisation's strategy to consent
- review your consent processes and marketing collateral to ensure they are specific, granular, clear, prominent, actively opted-in, documented and can be easily withdrawn
- Review your systems (e.g. CRM and HR) to ensure they will meet GDPR consent requirements
- Review your online forms used to gather consent for compliance with GDPR (e.g. website, online fundraising forms, online consent platforms and email marketing)
- Create a document store to contain copies of all consent wording used on online and offline marketing collateral – this helps to support accountability

Children

- Check whether your existing policies and procedures are inline with GDPR requirements
- Identify and document any of your existing data processing activities related to children's personal data
- Record the lawful basis for processing

Communication privacy information

- Review your existing privacy notices for adherence with GDPR (ensure the review includes all online presence)
- If required, update and publish revised privacy notices
- Review your privacy policies and outsourced service provider contracts (e.g. web shop, fundraising and marketing agencies and online fundraising platforms) - ensure they will be appropriate and inline with your own policies.

Individuals' rights

- Review your processes and systems (e.g. CRM, website, HR) to ensure they support individuals' rights under GDPR

- Review whether the organisation will be required to adhere to the new 'right to data portability' under GDPR - *This allows individuals to obtain and reuse their personal data for their own purposes across different services*

Subject access

- Review your existing policies and processes relating to subject access requests
- Update your policies and processes as required to meet GDPR requirements
- Undertake staff training inline with the new policies and processes
- Consider whether your existing staff resourcing levels have sufficient capacity to adhere to the new GDPR Subject Access Request timelines

Data breaches

- Review policies and procedures to ensure they meet the GDPR requirements
- Review your existing processes to notify the ICO and individuals where a breach will result in a high risk to rights and freedoms
- Update your existing policies and processes as required

International transfer of data

- Review whether your organisation operates in more than one EU member state
- If it does, decide and document which is the lead supervisory authority

Thank you

This presentation is available to download from the Adapta website

www.adaptaconsulting.co.uk

adapta

iAm