A presentation by

HILL DICKINSON

HILL DICKINSON

GDPR overview

Insurance Institute of Manchester

Joe Orme
Associate
Hill Dickinson LLP

Objectives (1)

- The General Data Protection Regulation (GDPR) – what is the rationale behind the change.
- Understand key terms in Data Protection Law.
- Key changes under the GDPR and how to apply them to your business.

Objectives (2)

- Apply your mind to any risk areas in your organisation ahead of the implementation date (25 May 2018).

- What can you do now to prepare?

The General Data Protection Regulation (GDPR) – rationale

- General message – more onerous obligations than Data Protection Act 1998
- Great disparity between UK and other EU member states as to how personal data safeguarded
- Harmonisation of data subjects' rights, security and sanctions
- UK to implement changes post-Brexit through a new Data Protection Bill

Jargon Buster (1)

- Personal Data
  - any information relating to an identified or identifiable natural person ('data subject');
  - an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

Jargon Buster (2)

- Special categories of personal data (formerly sensitive)
  - Racial or ethnic origin
  - Political opinion
  - Religious or philosophical beliefs
  - Trade union membership
  - Genetic and biometric data used to uniquely identify a natural person
  - Health data
  - Sex life or sexual orientation
- Criminal conviction data treated the same way

Jargon Buster (3)

- Controller
  - alone or jointly with others, determines the purposes and means of the processing of personal data
- Processor
  - processes personal data on behalf of the controller (need Article 28 written agreement)
- Processing
  - any activity that involves the use of Personal Data. It includes obtaining, recording, holding, organising, amending, retrieving, using, disclosing, erasing, and transmitting to third parties.

What are the principles

- Lawful, fair and transparent
- Limited and specific purpose
- Adequate, relevant and not excessive
- Accurate and kept up to date
- Not kept longer than is needed for the purpose the data has been collected
- Security
  - Transferring personal data outside the EU

Lawful conditions for processing

- Consent
- Performance of a contract or in order to take steps at the request of an individual to enter into one
- Legal obligation
- Vital interests of the individual
- Necessary for the performance of a task carried out in the public interest or the exercise of official authority vested a public body
- Legitimate interests.

Conditions for Special Categories

- Article 9 GDPR – limited
- Data Protection Bill – much more
- Key message – processed under narrow circumstances and with tighter controls
- Consider how you use this type of data and why

Changes – right to be informed (1)

- Essentially through privacy notices that are already required.
  - Concise, transparent, intelligible and easily accessible
  - Written in clear and plain language
  - Free of charge
- Code of practice sets out a layered approach

Changes – right to be informed (2)

- What you need to tell individuals depends on if you obtain information directly from them or not.
- Key points to cover:
  - Controller's and DPO's contact details
  - Purpose of and legal basis for processing
  - Details of transfers to third countries and the safeguards in place
  - Retention periods
  - Data subject's rights – including right to withdraw consent
  - Any automated decision making, any profiling and how they will be used to make decisions

Changes – right of access (1)

- Subject access request
  - The reason?
    - So that individuals are aware of and can verify the lawfulness of processing
  - Goodbye fee – cannot charge £10 as is the case under DPA
  - Provide requested data in 1 month (currently 40 calendar days)
  - Can extend time for providing information up to 2 months when requests are complex or numerous.
  - Individuals must be informed within one month that an extension is being applied and why

Changes – right of access (2)

- Request is manifestly unfounded or excessive:
  - May charge a fee
  - May not have to comply
  - Must tell the individual within one month why organisation is not complying and the right to complain to the ICO

Changes – data portability (1)

- New right
- Allows individuals to obtain and reuse their personal data
- Some organisations already have this agreed within sectors
- Applies to:
  - Personal data provided by the individual to the controller
  - Processing is based on the individual's consent or for the performance of a contract; and
  - Processing is carried out by automated means

Changes – data portability (2)

- Controllers must provide personal data:
  - In a structured;
  - Commonly used; and
  - Machine readable form.
- Free of charge
- Can be required to directly transmit the data to another organisation
- Must respond without undue delay
- If not responding, explain why within one month

Other rights

- Right to object to processing
  - Need compelling grounds to continue if legitimate interests
- Right to restrict processing
  - Used whilst addressing inaccurate data and alongside rectification
- Right to rectification
  - Address inaccuracies in data stored
- Right to erasure
  - Not absolute right, only when there is no compelling reason to still process the data

Changes – breach notifications (1)

- New obligation
- Must report a breach to ICO that is likely to risk the rights and freedoms of individuals
  - Report to ICO within 72 hours of breach
- Must report to individual concerned if there is a high risk

Changes – breach notifications (2)

- What do you need to include in your report?

  - ✓ The nature of the personal data breach including categories of individuals and personal data concerned
  - ✓ Details of point of contact at the controller (DPO?)
  - ✓ Description of likely consequences of the breach
  - ✓ What measures have been taken or proposed to be taken

Changes – accountability and transparency

- Data protection is no longer a tick box exercise
- Must be able to demonstrate compliance with the data protection principles. How?
  - Implement technical and organisation measures to meet compliance
  - Maintain documentation on processing so that it can be mapped
  - Use data protection impact assessments:
    - When using new technologies; and
    - Processing is likely to result in a high risk to rights and freedoms of individuals
  - Record of processing activities

Changes – mandatory Data Protection Officer (DPO)

- Good practice to have somebody in the organisation who "owns" data protection
- It is a mandatory requirement to appoint a DPO if:
  - Controller is a public authority
  - Organisation carries out large scale systematic monitoring of individuals or
  - Carries out large scale processing of special categories of data or data relating to criminal convictions

Changes - Consent

- Updated definition which requires a higher threshold.
  - must be a freely given, specific, informed and unambiguous indication of the individual's wishes through clear affirmative action or statement
- Not the only condition for processing.
- Must have the requisite consent for direct marketing to an individual.
- Must evidence what consent was given, when and how it was obtained.
- Must allow the right to withdraw consent and advise individuals about this.

What can you do now? (1)

- Be aware of GDPR / reform developments
  - Your organisations should be already taking steps to comply
  - Know your policies, procedures and contacts within the organisation responsible for compliance
  - ICO website and legal news – abundance of current awareness, newsletters and guidance at your fingertips
- Be compliant with current legislation and ICO Guidance
  - ICO website – key for resources

What can you do now? (2)

- Know your data and how you use it
- Audit consent
  - When do you seek it?
  - When do you rely on other conditions for processing?
  - Is it deficient?
  - High-risk areas e.g. direct marketing

What can you do now? (3)

- Risk areas:
  - Security
  - Your status – data controller or data processor?
  - International (including EU) transfers
  - Direct marketing
  - CCTV

What can you do now? (4)

- Designate a DPO
  - Do you need a mandatory DPO? If not, consider implementing the position in some form
- Compliance training
  - Currently one of biggest failings yet one of easiest ways of raising awareness and reducing risk of breaches

HILL DICKINSON

Joe Orme
Associate

T: 0151 600 8974
E: joe.orme@hilldickinson.com

HILL DICKINSON

HILL DICKINSON

The information and any commentary contained in this presentation are for general information purposes only and do not constitute legal or any other type of professional advice. We do not accept and, to the extent permitted by law, exclude liability to any person for any loss which may arise from relying upon or otherwise using the information contained in this presentation. Whilst every effort has been made when preparing this presentation, no liability is accepted for any error or omission. If you have any particular query or issue, we would strongly recommend you contact a member of the team who would be happy to provide specific advice.

A presentation by

HILL DICKINSON