

Understanding the impact that GDPR will have

Andrew Wright

Managing Partner

Clarkson Wright & Jakes Ltd

Amy Bell

Amy Bell Compliance Ltd

Contents

- A review of the GDPR
- How GDPR fits in with the new Data Protection Act?
- What is Privacy by design?
- What can you do with the data you already hold?

Background

- “Biggest change to Data Protection Legislation in a generation”
- Evolution, not revolution
- World has moved on
- Seeking alignment across member states
- 25th May 2018
- Brexit – Data Protection Bill

GDPR Headlines

- Core Principles – Article 5
 - Lawful, fair and transparent
 - Expected by the person whose data it is
 - Just enough data to be able to do what you need to
 - Accurate
 - Only keep as long as necessary
 - Protect the data subjects
 - Data Controller is accountable

GDPR Headlines

- Data Subject Rights
 - Know what will happen with their data
 - Obtain copies of the data
 - Have inaccurate data corrected
 - Have data erased
 - Restrict processing
 - Data Portability
 - Right to object to processing
 - No Automatic processing

GDPR Headlines

- Data Controller (or Processor) Accountability
 - Be accountable/Demonstrate compliance
 - Adopt privacy by design
 - Take care with third parties (due diligence)
 - Adopt security measures
 - Inform ICO within 72 hours of breach
 - If high risk inform Data Subject within 72 hours of breach
 - Carry out privacy impact assessment
 - Decide whether to appoint a DPO

What to do first?

- Engage
 - Board/Management
 - People who manage data
 - Third parties
 - Staff
- Why bother
 - Heavy penalties – had 2 years!
 - Potentially a lot of work
 - Potentially huge business impact

What data do you have?

Audit

- What data do we have?
 - Customer
 - Employee
- Where is it?
 - Outlook
 - CRM system
 - Paper
- Data Security applied
 - Encryption
 - Password protection
 - None
- What is the source?
 - Customer
 - Employee
 - Third party
- How was consent obtained?
 - Online
 - Paper
- Is the data shared?

Conditions for processing

- Contract
- Legal Obligation
- Protect vital interests
- Public Interest
- Legitimate Interest
- Consent

Consent

- Explicit Consent
- Conditions for valid consent
 - Transparency
 - Distinguishable
 - Not conditional, except for performance of the contract
- Rules out pre-ticked boxes
- Demonstrate consent – double opt in?
- Not hidden in terms and conditions
- If you are currently relying on consent which will not be valid – think again

Security

- Identify the data
- Risk assessment – risk to the data subject, not the organisation!
- Measures to mitigate
- Training
- Testing

Privacy by design

- Established processes
- Inflight projects
- Future work
 - Technology and risk evolving
 - Privacy Impact Assessments

Data Protection Bill

- Draft Bill - September
- Many aspects simply reflect GDPR
- Lowering of age of consent to processing for children to 13
- National Security
- Allow processing of data relating to criminal convictions (to allow background checks)
- Separate DP regime for Law Enforcement



The End!

These course notes, slides and other materials that are provided for use on the course have been prepared solely for the benefit of delegates. They are designed to be part of the presentation and not to stand on their own. The materials will provide an outline of the provisions of various matters including legislation and case law. They will not be exhaustive and in particular will contain many points of law that will have been reduced to broad statements for the purposes of brevity and to aid explanation and understanding. It is important that delegates refer to original sources or one of the standard works on the relevant subject area for further guidance. In particular, in no circumstances should the materials be used for giving advice.



Clarkson Wright & Jakes Ltd
Solicitors and Notaries

GDPR Breakfast Seminar

19 September 2017