ashfords

CESW – GDPR UPDATE

8 February 2018

Why Data Protection?

- All elements of your business will touch personal data
  - Staff
  - Enquiries
  - Suppliers
  - Contractors
  - Marketing
- All Change - Complete Overhaul of Data Protection
  - General Data Protection Regulation (“GDPR”)
  - Police & Criminal Justice Directive
  - ePrivacy Regulation
- Data Protection Bill
- Brexit position papers

Elizabeth Denham – Information Commissioner

"The biggest change to data protection law for a generation"

"The new legislation creates an onus on companies to understand the risks that they create for others, and to mitigate those risks. It's about moving away from seeing the law as a box ticking exercise, and instead to work on a framework that can be used to build a culture of privacy that pervades an entire organisation"

"If a business can't show that good data protection is a cornerstone of their practices, they're leaving themselves open to a fine or other enforcement action that could damage bank balance or business reputation"

"When it comes to data protection, small businesses tend to be less well prepared. They have less to invest in getting it right. They don't have compliance teams or data protection officers. But small organisations often process a lot of personal data, and the reputation and liability risks are just as real"

"Last year we issued more than one million pounds in fines for breaches of the Data Protection Act, so it's not a power we're afraid to use"

"The ICO's commitment to guiding, advising and educating organisations about how to comply with the law will not change under the GDPR. We have always preferred the carrot to the stick"

Data protection principles in the GDPR

- Lawfulness, fairness and transparency
- Purpose limitation
  - archiving, scientific, historical or statistical purposes
- Data minimisation
  - “not excessive” v “what is necessary”
- Accuracy
- Storage limitation
- Integrity and confidentiality
  - Technical and organisational
- Accountability

Personal Data

- Definition of Personal Data
  - Living individual – Identified – Identifiable from
  - 20 years since the Directive
  - Online identifiers
    - Device IDs
    - Cookie IDs
    - IP addresses
- Sensitive Personal Data – Special Category Data
  - Special categories of personal data
    - Genetic Data
    - Biometric Data

Data Processor Obligations

- Controller - Processor Contract
  - Appropriate obligation of confidentiality
- Sub-Processors
  - Prior written consent
- Record of Processing Activity
  - Controller/Processor
  - Representatives/DPO
  - Information requiring cross border transfer
  - Categories of activities
  - Security measures
- Security of Processing
  - Appropriate technical and organisational
- Co-operation and consultation

Wider Territorial Scope

- Establishment Test
  - Controller or processor established in EEA
  - Processing inside or outside EEA
- Goods and Services Test
  - Offer to residents of EEA
- Monitoring Test
  - Behaviour within EEA
- Relevant Factors
  - Language – Currency
  - Ability to Order

Data Protection Officer

- Obligatory appointment
  - public authority or body
  - regular and systematic monitoring of data subjects on a large scale
  - Special categories of data and personal data relating to criminal convictions and offences
- Voluntary appointment?
- Expert knowledge
- First point of contact

Conditions for Processing - Consent

- ***Employers Should not rely on Employee consent!***
- ***Consent***
  - *"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 or personal data related to him or her".*
    - Unbundled
    - Active opt-in (Pre-ticked boxes & Inactivity)
    - Granular
    - Documented
  - Can we carry over existing Consents?

Other Conditions for Processing

- Performance of a Contract
- Compliance with a Legal Obligation
- Vital Interests
  - Data Subject
  - Others
- Public interest
- Legitimate interests

Breach notification

- Processor
  - Without undue delay
- Controller
  - Regulator - 72 hours
  - Individual – risk to their rights and freedoms
- Withholding notification
  - Unlikely to result in risk
  - Appropriate protection
  - Trigger disproportionate effort

Harsher Penalties

- ICO range of powers
  - investigate
  - authorise
  - correct
  - advise
- Two Tiers
  - Greater of 4% global turnover/€20 million
  - Greater of 2% global turnover/€10 million
- Judicial remedies
- Compensation

Right to be Forgotten

- Google Spain
- Individuals can request deletion
  - Problem with legality
  - Consent withdrawn
- Right of rectification
- Restriction on processing
  - Complaints being investigated
- If successful
  - Obligation on controller
  - Down the chain

Impact of Brexit on GDPR

- **The Rt Hon Karen Bradley MP – Secretary of State for DCMS**
  "We will be members of the EU in 2018 and therefore it would be expected and quite normal for us to opt into the GDPR and then look later at how best we might be able to help British business with data protection while maintaining high levels of protection for members of the public"
- **Elizabeth Denham – Information Commissioner**
  "I acknowledge that there may still be questions about how the GDPR would work on the UK leaving the EU but this should not distract from the important task of compliance with GDPR by 2018. We'll be working with government to stay at the centre of these conversations about the long term future of UK data protection law and to provide our advice and counsel where appropriate"
- **Queen's Speech**
  Data Protection Bill – removes any doubt about the UK's commitment to data protection and the GDPR.
- **DCMS Statement of Intent** - 7 August 2017
- **Data Protection Bill** – 14 September 2017

International Transfers

- Safe Harbor
  - Max Schrems - CJEU
  - Commission Decision invalid
- Privacy Shield
  - Stronger obligations?
  - Safeguards and transparency?
  - Undertaking from US Director of National Intelligence?
  - Annual review?
- Model Clauses
  - New clauses under GDPR?
  - Data Protection Commissioner v. Facebook Ireland Ltd and Maximilian Schrems

Preparing for GDPR

- Awareness
  - Resource
  - Capacity
- Information held
  - What?
  - Where?
  - Why?
- Procedures
  - Individuals rights
  - Data breaches
- Privacy Notices
  - How communicated?
- Legal basis for processing
  - Consent
  - Legitimate interests
- Privacy Impact Assessments
- Subject Access Requests
  - Data Portability
  - 40 days v 1 month

Speaker

Chris Coughlan

Senior Associate

Head of Data Protection & Privacy

+44 (0)117 321 8060

c.coughlan@ashfords.co.uk

Questions?