GDPR UPDATE

4 July 2018

Ashfords LLP
ashfords.co.uk

Why Data Protection?

- All Change - Complete Overhaul of Data Protection
- As well as GDPR - Data Protection Act 2018
- This is a Privacy Law not just a Marketing Law
- Information Commissioner
  - Elizabeth Denham

  “The biggest change to data protection law for a generation”

  “There is no deadline…25 May 2018 is the beginning not the end”

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

"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"

Personal Data

- Definition of Personal Data
  - Living individual – Identified – Identifiable From
  - 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
  - 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

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

Right to be Informed

- Name and contact details of your organisation
- Contact details of your DPO
- Purposes of the processing
- Lawful basis for the processing
- The legitimate interests for the processing
- The categories of personal data obtained*
- The recipients or categories of recipients of the personal data
- Details of international transfers
- Retention periods
- The rights available to individuals in respect of the processing
- The right to withdraw consent
- The right to lodge a complaint with the ICO
- The source of the personal data*
- The details of whether individuals are under a statutory or contractual obligation to provide the personal data**
- The details of the existence of automated decision-making, including profiling

* Article 14 only
** Article 13 only

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

Individuals' Rights

- Individuals can request deletion
  - Problem with legality
  - Consent withdrawn
- Right of access
  - Subject access requests
- Right of rectification
- Restriction on processing
  - Complaints being investigated
- Object to processing
  - Legitimate Interests
  - Direct Marketing

Fines Litigation & Increased Powers

- Up to 4% group global turnover or €20 million
- Controller v Processor Litigation
- Increased compensation claims
- Enforcement Powers
  - Information notices for individuals
  - Criminalise controllers for frustrating information/assessment notices
  - Urgent information/assessment notices
  - Modernise search and seizure powers

Ongoing compliance

- Awareness
  - Resource
  - Capacity
- Information held
  - What?
  - Where?
  - Why?
- Procedures
  - Individuals rights
  - Data breaches
- Privacy Notices
  - How communicated?
- Legal basis for processing
  - Consent
  - Legitimate interests
- Breach response
- Individuals' Rights
  - Right to be forgotten
  - Subject access

Speakers

Alex Aisthorpe

Solicitor

a.aisthorpe@ashfords.co.uk