Data Protection

Mark Gleeson

brownejacobson LLP

Today's focus

- Briefing on the new law
- Identify the practical impact on you
- Design your GDPR compliance programme

GDPR background

- What is it?
- Why is it coming in?
- What about Brexit?

What is it?

- Probably the most lobbied piece of EU law ever
- Replaces the Data Protection Directive 1995 (DPD)
- Will be enforced in Member States from 25 May 2018
- EU Member State laws implementing the DPD will no longer apply
- Creates a “level-ish” playing field across EU
- What is the Data Protection Bill?

Why is it coming in?

Developments since 1995

- Legal
  - Case law
  - Regulatory triple whammy
- Technological
- Societal

Who has to comply?

- Controller or processor established in one or more Member State
- Controller or processor established outside the EU and either
  - offering goods and services to individuals in the EU or
  - monitoring the behaviour of individuals taking place in the EU

What about Brexit?

- GDPR and the new Data Protection Act will apply from May 2018 After Brexit
  - New Data Protection Act will apply
  - GDPR will apply to many UK organisations due to extra-territorial scope
  - GDPR will be swept up by the EU (Withdrawal) Bill 2017
  - Government wishes to "*maintain the stability of data transfer between EU Member States and the UK*"

Key issues

- Scope
- Key players
  - Data subject
  - Controller
  - Processor
  - Supervisory authorities
- What are personal data?
- What are special categories of data?

Key issues

- Principles and accountability
- Lawful basis for processing
- Transparency
- Responsibilities of controller and processors
- International transfers
- Rights of data subjects
- Breach notification
- Enforcement and compensation

Accountability

- Compliant policies and procedures
- Records of processing
- DPO appointment
  - Mandatory/voluntary
- Privacy by design/by default
- Data privacy impact assessments

Principles

- Principles
  - Lawfulness, fairness and transparency
  - Purpose limitation
  - Data minimisation
  - Accuracy
  - Storage limitation
  - Integrity and confidentiality

Lawful basis for processing

- Consent
- Necessary for the performance of a contract
- Necessary for legal obligation
- Necessary to protect vital interests
- Task carried out in the public interest
- Legitimate interests

Lawful basis for processing special categories

- Explicit consent
- Obligations and rights in employment, social security and social protection
- Vital interests
- Manifestly made public
- Legal claims and courts
- Substantial public interest
- Medicine
- Public health
- Archiving

Consent and explicit 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 of personal data relating to him or her

- Explicit consent
- Re-papering consents - recital 171
- Article 29 WP guidance

Individual rights

- Information
- Subject access
- Rectification
- Erasure (Right to be forgotten)
- Portability
- Objecting
- Compensation
- Profiling
- Restriction

Right to information - transparency

- Where personal data collected from data subject
- Where personal data have not been obtained from data subject

Marketing

- Lawful basis
  - Consent
  - Legitimate interest
- Re-using lists
- Third party marketing
- Privacy and Electronic Communications Regulations 2003
- Draft e-Privacy Regulation

Breach notification

- Personal data breach
- Controller breach notification
  - Supervisory Authorities
  - Affected individuals
- Processor breach notification
  - Controller

Sanctions for non-compliance

- Supervisory Authorities
  - Investigative powers
  - Corrective powers
- Penalties
  - 2% global turnover or €10m
  - 4% global turnover or €20m
- Compensation

Turning the law into practice

- Map the law to your processing
- Identify key data processing
- Identify high-risk processing
- Identify gaps
- Mitigate the risks

The team

- Board oversight
- Legal
- Compliance
- IT
- HR
- Marketing
- Project management
- External advisers

The plan

- Initiation
  - Awareness
  - Buy-in
  - Budget
- Assessment
  - Mapping
  - Gap analysis
- Remedy

Data mapping

- Review and record in writing all processing activities
- Record international transfers and mechanism

Data mapping

- The 5 Ws
  - **Why** is personal data processed?
  - **Whose** personal data is processed?
  - **What** personal data is processed?
  - **When** is personal data processed?
  - **Where** is personal data processed?
- Questionnaire
- Produce a risk based report

Secure data and information

- Assess security risk
- Update information security and policy
- Maintain security measures

Third party relationships

- Assess third party relationships
  - Group
  - Customers
  - Partners
  - Processors
- Appropriate contracts and controls
- Undertake due diligence and audits

Compliance culture

- Board level issue
- Accountability
- Training and awareness

How Browne Jacobson is supporting clients?

- End to end GDPR reviews
- Scoped assistance
- Menu service
- Ad hoc adviser
- Steering group member

Thank you

Mark Gleeson
mark.gleeson@brownejacobson.com
020 7871 8534