DMH Stallard

Privacy matters

The General Data Protection Regulation

25 May 2018

Anthony Lee, Partner

Privacy laws

- Existing law – based on EU Directive 95/46/EC
  - UK Data Protection Act 1998
- May 2018 – the EU General Data Protection Regulation
- Other laws – eg confidentiality

Harmonisation

- "Direct effect"
- More consistency across EU member states
- But, "special rules" allowed in various areas

Scope

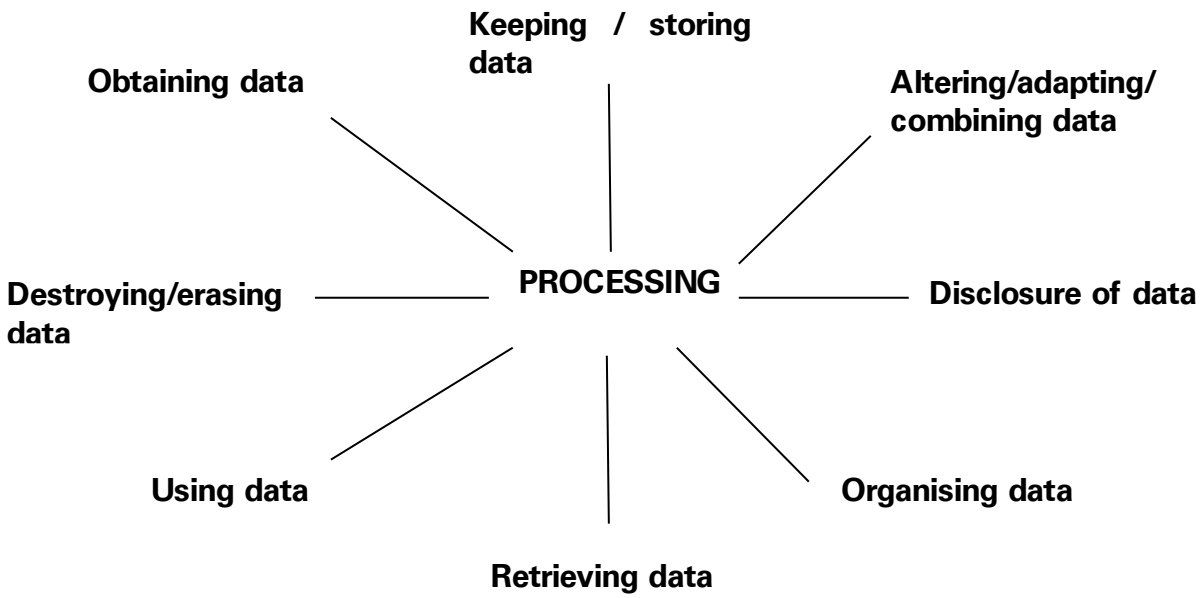
- EU based data controllers and processors are caught today
- Where no EU presence: applies if processing re goods/services or monitoring
- Certain activities excluded e.g. national security; personal/household activities

The 7 Principles

- Broadly similar to the Directive's principle
  - "lawfulness, fairness and transparency"
  - "purpose limitation"
  - "date minimisation"
  - "accuracy"
  - "storage limitation"
  - "integrity and confidentiality"

- "Accountability" – be able to demonstrate compliance with the principles

Processing includes:



Central requirements

- Appropriate technical and organisational measures
- Controller – to have and be seen to have
- Processor – to provide sufficient guarantees

Lawful basis for processing

- Must meet one or more of the "enhanced fair processing" conditions
- The bar is higher for special categories of personal data
- Broadly replicates the Directive's conditions
- But, legitimate interests condition cannot be relied on in relation to special categories of personal data or by public authorities

Key changes

- Risk-based approach to compliance
- Accountability and data protection by design
- Greater emphasis on transparency
- Rights of individuals
- Consent harder to obtain
- Strict data breach notification rules
- Increased enforcement powers/fines

Accountability

- Data protection polices and procedures
- Data protection by design and default
- Record keeping obligations
- Data protection impact assessments
- Co-operation with DPAs

Accountability continued

- Prior consultation with DPAs in high risk cases
- Mandatory DPOs for public sector (and Big Data)
- Security and notification of breaches
- Codes of conduct; certification, seals and marks

Consent

- Must be freely given, specific, informed and unambiguous
- Can be withdrawn at any time
- Cannot be bundled with T&Cs
- If “take it of leave it”, not freely given

Data Security

- Continued spotlight on security
- Combination of technical and organisational measures to guard against
  - external threats (such as hack attacks)
  - internal threats (such as accidental loss by employees)

- Importance of policies and procedures
- Personal data but should be borne in mind in respect of other data

Some culprits

Using a processor

- Data sharing – must have a lawful basis
- Processor must have appropriate technical and organisational measures in place
- Additional detailed requirements for contracts
- Keep the data subjects informed

Using a processor continued

- Additional detailed requirements for contracts, including:
  - following documented instructions
  - ensuring persons under confidentiality obligations
  - having adequate security measures in place
  - providing assistance to the controller
  - keep the data subjects informed
  - deleting/returning personal data at the end of provision of services
  - providing information to demonstrate compliance
  - audit rights
  - flowing down obligations on sub processors

Data Export

- Exports out of EEA will continue to be restricted
- Some changes (e.g. approved certification mechanism)
- Commission will continue to determine “safe” countries
- Standard contractual clauses (adopted/approved by the Commission)
- Binding corporate rules (BCRs)
- Privacy shield for US not addressed
- Breach subject to maximise fines (4% of turnover)

Goodbye Safe Harbor, Hello Privacy Shield

- Commission permitted export to companies in US if registered under the Safe Harbor scheme
- Snowden revelations
- Schrems' case
- Safe Harbor decision ruled invalid
- Exports to Safe Harbor companies no longer "adequate"
- Replaced by Privacy Shield
- Implications
- The Jury is OUT!

Will Brexit Make Any Difference?

- No
- The UK government has said GDPR will come into force
- The "Great Repeal Bill" is intended to bring all current EU legislation into UK law
- The UK outside Brexit will want to be seen as an "adequate" country
- The UK Data Protection Bill

10 steps to take

- Awareness
- Information held & data flows
- Technical measures
- Organisational measures
- Third parties
- International transfers
- Rights of individuals
- Consents
- Informing individuals
- Incident response plan

Summary

- Stricter laws
- New obligations
- Focus on policies and procedures
- Spotlight on weak practices/security
- Emphasis on safe data flows
- Increased enforcement powers/heftier fines

Contact Details

- **Anthony Lee, Partner**
  Tel: 07802 283990
  Email: Anthony.Lee@dmhstallard.com