

EU Data Protection Legislation Current and Future

Presenter: Hugh Jones

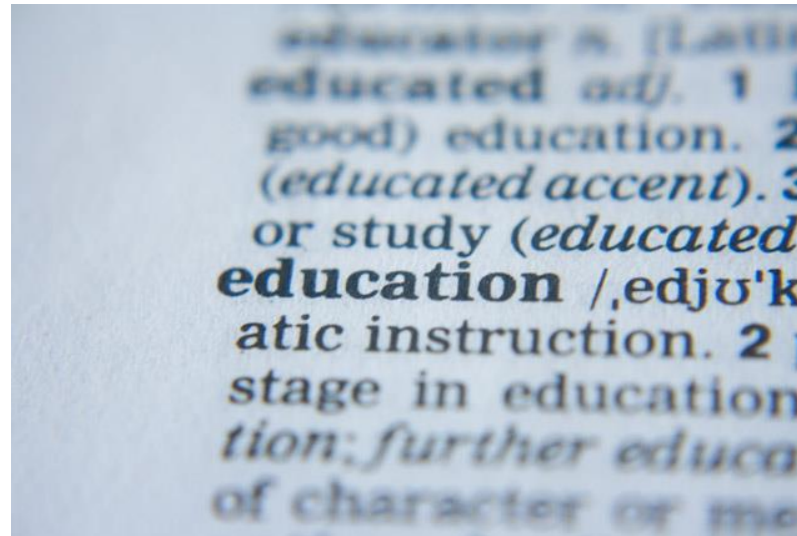


General Data Protection Regulations

- ▶ Proposed legislation
- ▶ Wording due to be finalised in early 2016
- ▶ Due to come into effect in early 2018
- ▶ Objective is to harmonise EU legislation
- ▶ 'Catch up' with new technologies
- ▶ Accommodate current business models
- ▶ Recognise the global business market

New Definitions

- ▶ Pseudonymised Data
- ▶ Profile
- ▶ Encryption
- ▶ Data Recipient
- ▶ Third Party
- ▶ Data Subject Consent
- ▶ Breach
- ▶ Genetic/Biometric Data
- ▶ Health Data
- ▶ Establishment
- ▶ Nominated Representative
- ▶ Child



Key Principles

- ▶ Selection (“One-stop Shop”)
- ▶ Accountability and Liability
- ▶ Data Processing must be:
 - ▶ Fair and Justifiable
 - ▶ Security
 - ▶ Portability and Accessibility
 - ▶ Specified and Lawful
 - ▶ Transparent and Explicit
 - ▶ Adequate and Relevant
- ▶ Specific Categories of Processing

Selection of Jurisdiction



- ▶ Referred-to as ‘The One-Stop Shop’
- ▶ Data Controller reports to the Statutory Authority where the Controller is established / operational
- ▶ Where Controller is active in several EU jurisdictions, they can indicate a preferred jurisdiction
- ▶ That authority will then be responsible for the Controller’s compliance

Accountability

- ▶ Role of Data Controller
 - ▶ Primary point of compliance
- ▶ Role of Data Processor
 - ▶ Mandatory contract in place
- ▶ Role of Data Protection Officer
 - ▶ Dedicated role within the organisation
 - ▶ Not necessarily an employee
- ▶ Individual accountability of Board members

Revision of Key Roles

- ▶ Must be able to demonstrate compliance processing
- ▶ Evidence of Privacy by Design or by Default
- ▶ Possibility of being a 'Joint Controller'
- ▶ Obligations for non-EU based Data Controller
- ▶ Required clauses for Data Processor Contract
- ▶ Control over sub-contracting



Individual Liability under the Acts

- ▶ “Where an offence under this Act has been committed....
- ▶ by a body corporate
- ▶ and is proven to have been committed with the consent or connivance of, or to be attributable to any neglect on the part of a person,
- ▶ being a director, manager, secretary or other officer of that body corporate,
- ▶ or a person who was purporting to act in any such capacity...
- ▶ that person, as well as the body corporate,
- ▶ shall be guilty of that offence and be liable to be proceeded against and punished accordingly”

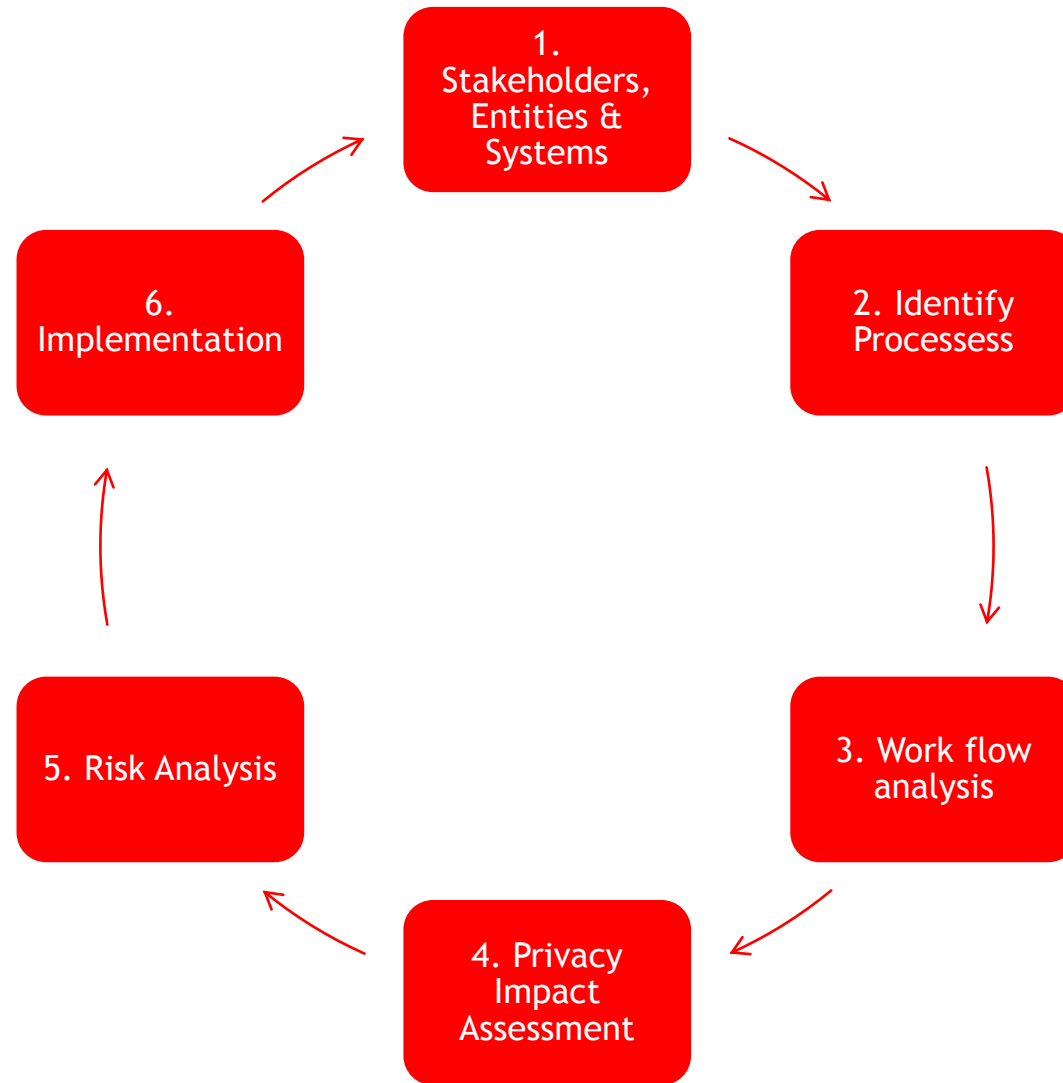
Data Protection Officer (DPO)

The Controller or Processor must designate a Data Protection Officer under certain criteria:

- ▶ to monitor internal compliance with the Regulations
- ▶ where the processing is carried out in the public sector or
- ▶ in the private sector by a large enterprise, or
- ▶ where the core activities of the controller require regular and systematic monitoring of Data Subjects, e.g. CCTV
- ▶ Governance of organisation's data management
- ▶ Drafting of compliant with data policies
- ▶ Influencing system and functional changes
- ▶ Currently an optional role
- ▶ May be mandatory in certain circumstances



Privacy Impact Assessment



Privacy Impact Assessment

- ▶ Where processing is likely to give rise to risk to the data
- ▶ Where relevant, involve the DPO
- ▶ Systematic evaluation of proposed processing
- ▶ Identification of risk
- ▶ Outline of the measures being taken to mitigate those risks
- ▶ Outline of structures and measures planned to achieve compliance
- ▶ Where substantial risk is identified, must check with Supervisor Authority



Offences under the GDPR

- Failure to meet time-line for response to Subject Access Request
- Provision of false or inadequate information to the Statutory Authority
- Fails to respect individual Rights - rectification, erasure, opt out, etc.
- Failure to comply with a formal Notice from the Statutory Authority
- Failure to notify the Statutory Authority of a Data Breach
- Failure to appoint a Data Protection Officer, if required
- Failure to carry out a Privacy Impact Assessment
- Failure to maintain appropriate logs and documentation (PIA, etc.)
- Inability to adequately demonstrate the compliance of data processing
- Disclosure of personal data which was obtained without authority
- Inappropriate engagement of a Data Processor (e.g. no contract in place)

Enforcement of legislation

- ▶ Formal notices
 - ▶ Information
 - ▶ Enforcement
 - ▶ Prohibition
- ▶ Mandatory breach notification
- ▶ Prosecution
- ▶ Reputational damage of a breach
- ▶ Cost of recovery of market share, good will, trust



Timeline for Deployment (anticipated)

- ▶ Mid-September to mid-October 2013: Orientation vote in LIBE Committee
- ▶ Autumn 2013 (depending on progress in the Council of Ministers)
- ▶ Negotiations between European Parliament, Council and Commission (the Trilogue)
- ▶ Finalisation of new wording - end-2015 (Luxembourg EU Presidency)
- ▶ Expected formal adoption by Trilogue in early 2016
- ▶ Deployment and enforcement end-2017 / early-2018.

So why comply with the GDPR?

- ▶ 'It's the law of the EEA'
- ▶ Protection of brand from negative publicity
- ▶ Avoid risk to reputation from prosecution
- ▶ Protection of trust
 - ▶ Employees
 - ▶ Suppliers
 - ▶ Customers
- ▶ Enables better decision-making
- ▶ Makes good business sense
- ▶ Delivers business value



Questions

