

EU Data Protection Regulation Preparing for the Future

Presenter: Hugh Jones



General Data Protection Regulations

- ▶ Proposed legislation
- ▶ Wording agreed in early January, 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
- ▶ Scope -
 - ▶ Where DC or DP are within the EU, regardless of where the processing takes place
 - ▶ Where Data Subject is an EU citizen, regardless of where DC or DP is based
 - ▶ Includes provision of goods and services, monitoring of behaviour within EU



IDMAie
Interactive Direct Marketing Association

SYTORUS
DATA PROTECTION SPECIALISTS



New Definitions

- ▶ Pseudonymised Data - individual cannot be identified
- ▶ Profiling - automated processing to evaluate personal aspects
- ▶ Data Recipient - Non-EU entity to which personal data are disclosed
- ▶ Third Party - any party authorised to process the personal data (not DP)
- ▶ Data Subject Consent - freely given, informed, specific indication of wishes
- ▶ Breach - breach of security leading to unlawful or accidental disclosure
- ▶ Genetic/Biometric Data - data relating to inherited genetic characteristics
- ▶ Health Data - data relating to mental or physical health, including admin
- ▶ Main Establishment - Place of key administration and decision-making
- ▶ Nominated Representative - Entity in EU which represents a non-EU entity
- ▶ Complaint - a relevant and reasoned objection to processing

Key Principles to replace ‘The 8 Rules’

- ▶ Data Processing must involve:
 - ▶ Lawful, Fair and Transparent processing
 - ▶ Purpose Limitation (specified purposes)
 - ▶ Data Minimisation (adequate, relevant and limited)
 - ▶ Accurate and Up-to-date processing
 - ▶ Limitation of storage in a form that permits identification
 - ▶ Confidential and Secure - protects integrity and privacy
 - ▶ Accountability and Liability - demonstration of compliance
- ▶ Specific Categories of Processing

Selection of Jurisdiction



- ▶ Referred-to as ‘The One-Stop Shop’
- ▶ Data Controller reports to the Supervisory Authority where the Controller is established / mainly 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

Data Controller Role

- ▶ Must be able to **demonstrate** compliant processing
- ▶ Implementation of appropriate technological and organisational safeguards
- ▶ **Documented** evidence of Privacy by Design or by Default
- ▶ Log of data management activities and breaches
- ▶ Possibility of being a 'Joint Controller'
- ▶ Obligations for non-EU based Data Controller
- ▶ Required clauses for Data Processor Contract
- ▶ Influence over sub-contracting



Data Processor Role

- ▶ Must be able to **provide** appropriate technical and organisational structures
- ▶ Must be able to **demonstrate** competence and compliance
- ▶ Can only engage sub-contractors with Controller's approval
- ▶ Controller has right to object to appointment of sub-contractors
- ▶ Data Processor contract must be in place, with prescribed clauses
- ▶ Same contract clauses and obligations will apply to sub-contractors
- ▶ Processor is primarily liable for failure of sub-contractors
- ▶ Where Processor has discretion, they will be treated as a Controller for that proportion of the processing
- ▶ Must maintain a written (electronic) log of processing activities
 - ▶ Categories of processing
 - ▶ Transfers to third countries
 - ▶ Details of Controller on whose behalf the processing is carried out

Data Processor Contract - Clauses

- ▶ Details on the subject matter of the processing
- ▶ Duration, nature and purpose of processing
- ▶ Type(s) of PID involved in the processing
- ▶ Categories of Data Subjects impacted
- ▶ Obligations and rights of the Data Controller
- ▶ Clear instructions on processing parameters from the Controller
- ▶ Obligation of confidentiality for Processor's staff
- ▶ Responsible for engagement and management of sub-contractors
- ▶ Fully support the Controller in meeting their obligations
- ▶ Return or destroy all data at the end of the engagement
- ▶ Make available data to demonstrate compliance - support audits

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”

Criteria for appointing a DPO

- ▶ Controller is a public body or authority (except courts)
 - ▶ Processing involves systematic monitoring of individuals
 - ▶ Large-scale processing of Sensitive or Semi-sensitive data
 - ▶ Processing of data relating to criminal activities or records
 - ▶ A group of organisations can have one DPO
-
- ▶ DPO does not have to be an employee (ahem!)
 - ▶ Should have expert knowledge of DP legislation
 - ▶ Should be sufficiently senior to implement obligations
 - ▶ Details must be provided to the Supervisory Authority

Data Protection Officer (DPO)

The Data Protection Officer must:

- ▶ monitor internal compliance with the Regulations
- ▶ Be involved in all aspects of processing of personal data
- ▶ Be available to answer Data Subject questions or complaints
- ▶ Ensure governance of organisation's data management activities
- ▶ Be point of contact for Supervisory Authority
- ▶ Draft compliant data management policies
- ▶ Influence system and functional changes
- ▶ Contribute to (or run) Privacy Impact Assessment
- ▶ Be bound by confidentiality and secrecy
- ▶ Cannot be instructed in performing their role
- ▶ Cannot be penalised for performing their role
- ▶ Reports to highest management level

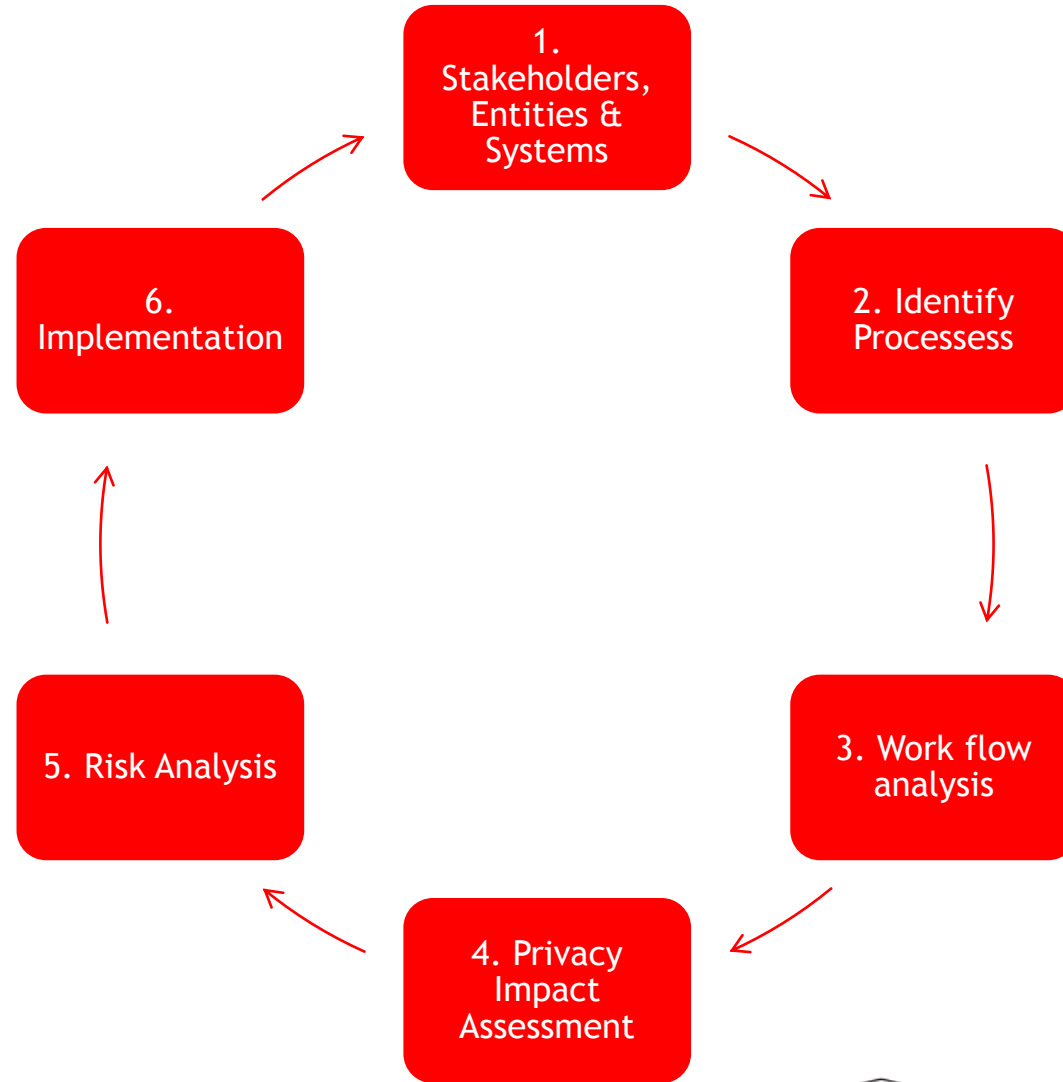


Privacy Impact Assessment

- ▶ Where processing is likely to give rise to risk to the data
 - ▶ Where relevant, involve the DPO
 - ▶ Systematic evaluation of proposed processing
 - ▶ Identification and evaluation of risk
 - ▶ Outline of the measures being taken to mitigate those risks
 - ▶ Outline of structures and measures planned to achieve compliance
 - ▶ Must be regularly reviewed and updated by the Controller
-
- ▶ Where substantial risk is identified, must check with Supervisory Authority
 - ▶ Supervisory Authority may define a list of circumstances where PIA mandatory



Privacy Impact Assessment



IDMAie
Interactive Direct Marketing Association

SYTORUS
DATA PROTECTION SPECIALISTS



Privacy Impact Assessment Report

At a minimum, should include:

- ▶ Description of the intended processing
- ▶ Purpose(s) of processing
- ▶ Explanation of the lawful processing justifications
- ▶ Risk Assessment of the proposed processing
- ▶ Description of measures being taken to mitigate risks
 - ▶ Safeguards
 - ▶ Security Mechanisms
 - ▶ Procedures for processing
- ▶ Related Codes of Conduct or processing standards
- ▶ Involvement of stakeholders (Data Subjects, Representatives, Processors)

Overseas Transfer Restrictions



- ▶ EEA countries (EU + EFTA) - 31
- ▶ 'Safe' Countries - 10
- ▶ Adequacy of Destination
 - ▶ Rule of Law
 - ▶ Respect for Human Rights and Fundamental Freedoms
 - ▶ Appropriate legislation and security measures
 - ▶ Specific DP legislation
 - ▶ Enforcement by a Supervisory Authority
- ▶ Model Contracts
- ▶ Code of Conduct with Enforceable Commitments
- ▶ Binding Corporate Rules



IDMAie
Interactive Direct Marketing Association

SYTORUS
DATA PROTECTION SPECIALISTS



Breach Notifications

- ▶ Ongoing logging and recording of incidents
- ▶ Breach Notification
 - ▶ Within 72 hours of becoming known
 - ▶ Describe implications of the breach, volumes, etc.
 - ▶ Outline measures taken to resolve the breach
 - ▶ Outline measures taken to prevent recurrence
 - ▶ Outline steps taken to minimise impact on Data Subjects
 - ▶ Details of any communications to Data Subjects
 - ▶ Name and details of DPO for reference
- ▶ Exemption if there is no risk to privacy of Subjects



‘Right to be Forgotten’

- ▶ NOT the ‘Right to Disappear’!
- ▶ Applies where the data is no longer necessary regarding the original purpose
- ▶ Where there is no legal basis for continued processing
- ▶ Where Subject objects to processing and no alternative justification
- ▶ Where the data is being unlawfully processed
- ▶ Controller must make other Controllers aware of preference
- ▶ Must make reasonable efforts to erase or remove the data from use
- ▶ Controller has the right to object
 - ▶ Right of Freedom of Expression
 - ▶ Other legal obligations may apply
 - ▶ Processing in the public interest

Adequate and Relevant

Adequacy Criteria include:

- ▶ State of the Art - appropriate, available technology
- ▶ Rule of Law - is the processing legitimate?
- ▶ Nature - is the processing necessary?
- ▶ Security - what security measures are in place?
- ▶ Scope - is the processing compatible with the purpose?
- ▶ Context - will the processing enable the stated objective?
- ▶ Adequacy - will the processing achieve the objective on its own?
- ▶ Alternatives - could the same objective be achieved by other means?



Enforcement of the Regulation

- ▶ Formal notices from Supervisory Authority
 - ▶ Information
 - ▶ Enforcement
 - ▶ Prohibition
- ▶ Prosecution
 - ▶ Penalties up to €10m or 2% of GAT
 - ▶ Penalties up to €20m or 4% of GAT
 - ▶ Penalties should be 'appropriate and dissuasive'
- ▶ EU Consistency Mechanism
- ▶ EU Data Protection Board - right of appeal
- ▶ Reputational damage of a breach
- ▶ Cost of recovery of market share, good will, trust



Specific Situations of Data Processing

- ▶ Reconciliation of conflict between GDPR and national legislation
- ▶ Publication of data in substantial public interest
- ▶ Re-Use of public sector information
- ▶ Use of PPSN / National Id Number
- ▶ Health and Genetic data
- ▶ Processing for Employment - Specific EU guidelines (Jan 2015)
- ▶ Processing for Social Protection and Employment
- ▶ Processing for Statistical & Historical Archives
- ▶ Processing for Church and Religious organisations
- ▶ Secrecy Obligations due to other legislative commitments

So why comply with the GDPR?

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



Questions



IDMAie
Interactive Direct Marketing Association

