Preparing for EU GDPR

Alan Calder
Founder & Executive Chair
IT Governance Ltd
2 June 2016

www.itgovernance.co.uk

Introduction

- Alan Calder
- Founder – IT Governance Ltd
- The single source for everything to do with IT governance, cyber risk management and IT compliance
- *IT Governance: An International Guide to Data Security and ISO 27001/ISO 27002, 6th Edition* (Open University textbook)
- *www.itgovernance.co.uk/shop/p-772-it-governance-an-international-guide-to-data-security-and-iso27001iso27002.aspx*
-

IT Governance Ltd: GRC One-Stop-Shop

All verticals, all sectors, all organizational sizes

Agenda

- An overview of the regulatory landscape and territorial scope
- Principles of the EU GDPR
- Breach notification rules
- Data subject rights
- Changes to consent
- Processor liabilities
- Role of the Data Protection Officer

History of the UK's privacy laws

- Post WWII – concerns about protection of human rights
- 1950 EU Convention on Human Rights (ECHR) – introduces privacy
- 1980 OECD guidelines on transborder data flows
- 1984 UK responds with first DPA 1984
- 1998 UK responds with EU-harmonised DPA 1998 (now covers manual files)
- 1998 Human Rights Act (HRA 1998) – Article 8 'Right to Privacy'
- Safe Harbor for EU/USA transfers – now struck down
- Varying DPA compliance requirements across EU
- Work starts on new EU law in 2013

The nature of European law

- Two main types of legislation:
  - Directives
    - Require individual implementation in each Member State
    - Implemented by the creation of national laws approved by the parliaments of each Member State
    - European Directive 95/46/EC is a Directive
    - UK Data Protection Act 1998
  - Regulations
    - Immediately applicable in each Member State
    - Require no local implementing legislation
    - EU GDPR is a Regulation

Article 99: Entry into force and application

This Regulation shall be binding in its entirety and directly applicable in all Member States.

KEY DATES

- On 8 April 2016 the Council adopted the Regulation.
- On 14 April 2016 the Regulation was adopted by the European Parliament.
- On 4 May 2016, the official text of the Regulation was published in the EU Official Journal in all the official languages.
- The **Regulation** entered into force on 24 May 2016, and applies from **25 May 2018**.
- http://ec.europa.eu/justice/data-protection/reform/index_en.htm

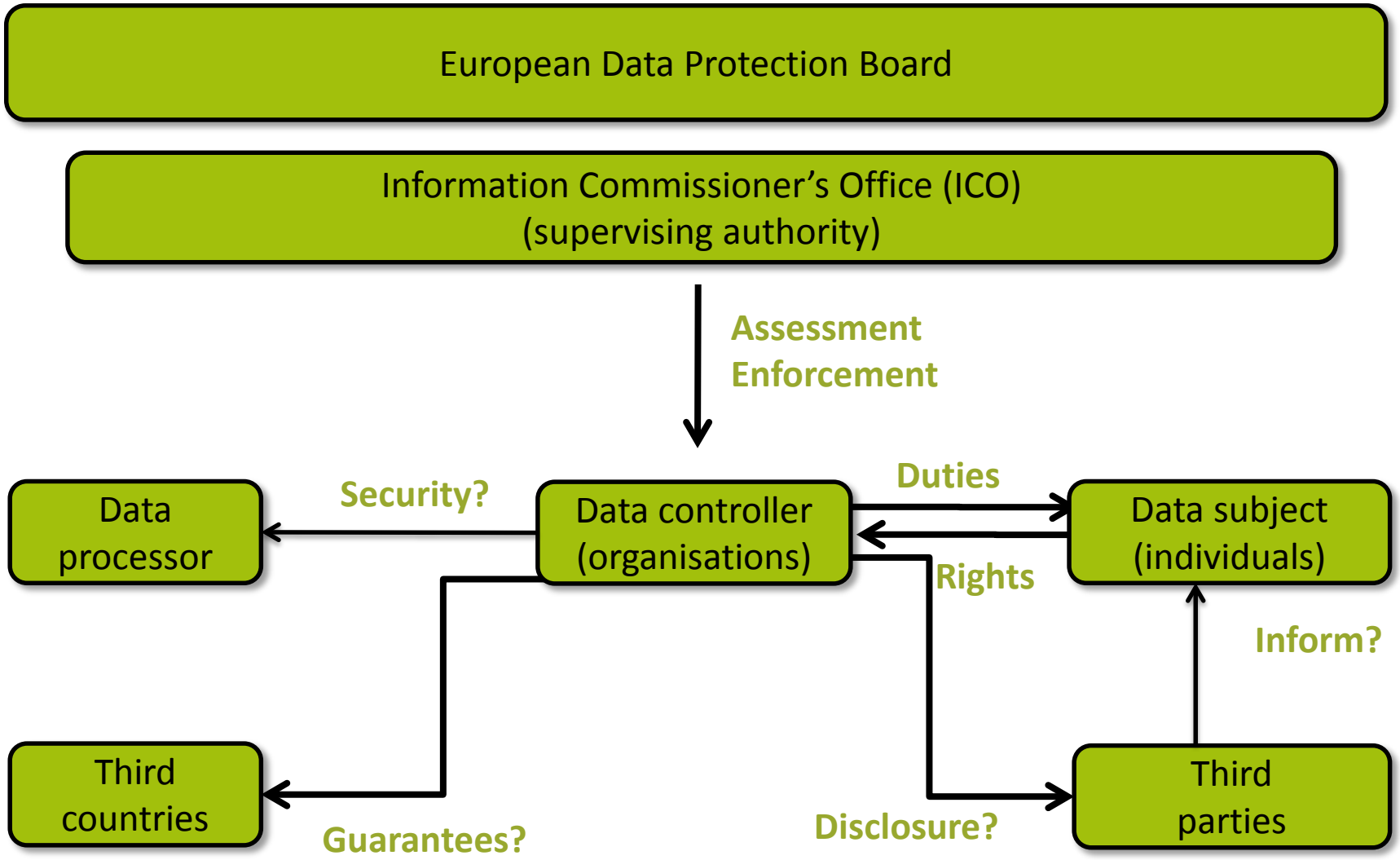
Final Text of the Directive: http://data.consilium.europa.eu/doc/document/ST-5419-2016-REV-1/en/pdf

GDPR

The GDPR has eleven chapters:

1. • Chapter I General Provisions: Articles 1 - 4
2. • Chapter II Principles: Articles 5 - 11
3. • Chapter III Rights of the Data Subject: Articles 12 - 23
4. • Chapter IV Controller and Processor: Articles 24 - 43
5. • Chapter V Transfer of Personal Data to Third Countries: Articles 44 - 50
6. • Chapter VI Independent Supervisory Authorities: Articles 51 - 59
7. • Chapter VII Cooperation and Consistency: Articles 60 - 76
8. • Chapter VIII Remedies Liabilities and Penalties: Articles 77 - 84
9. • Chapter IX Provisions Relating to Specific Processing Situations: Articles 85 - 91

Data protection model under GDPR



Articles 1 – 3: Who, and where?

- Natural person = a living individual
- Natural persons have rights associated with:
  - The protection of personal data
  - The protection of the processing personal data
  - The unrestricted movement of personal data within the EU
- In material scope:
  - Personal data that is processed wholly or partly by automated means;
  - Personal data that is part of a filing system, or intended to be.
- The Regulation applies to controllers and processors in the EU irrespective of where processing takes place.
- It applies to controllers not in the EU

Remedies, liability and penalties

- ***Article 79: Right to an effective judicial remedy against a controller or processor***
  - Judicial remedy where their rights have been infringed as a result of the processing of personal data.
    - In the courts of the Member State where the controller or processor has an establishment.
    - In the courts of the Member State where the data subject habitually resides.
- ***Article 82: Right to compensation and liability***
  - Any person who has suffered material, or non-material, damage shall have the right to receive compensation from the controller or processor.
  - Controller involved in processing shall be liable for damage caused by processing.
- ***Article 83: General conditions for imposing administrative fines***
  - Imposition of administrative fines will in each case be effective, proportionate, and dissuasive
    - taking into account technical and organisational measures implemented;
  - € 20,000,000 or, in case of an undertaking, 4% total worldwide annual turnover in the preceding financial year (whichever is higher)

Article 5: Principles - Personal data shall be:

1. Processed lawfully, fairly and in a transparent manner
2. Collected for specified, explicit and legitimate purposes
3. Adequate, relevant and limited to what is necessary
4. Accurate and, where necessary kept up to date
5. Retained only for as long as necessary
6. Processed in an appropriate manner to maintain security
7. Accountability

Article 5 & 6: Lawfulness

- Secure against accidental loss, destruction or damage
- Processing must be lawful – which means, inter alia:
  - Data subject must give consent for specific purposes
  - Other specific circumstances where consent is not required
    - So that controller can comply with legal obligations etc
- One month to respond to Subject Access Requests – & no charges
- Controllers and processors clearly distinguished
  - Clearly identified obligations
  - Controllers responsible for ensuring processors comply with contractual terms for processing information
  - Processors must operate under a legally binding contract
    - And note issues around extra-territoriality

Articles 7 - 9: Consent

- Consent must be clear and affirmative
  - Must be able to demonstrate that consent was given
  - Silence or inactivity does not constitute consent
  - Written consent must be clear, intelligible, easily accessible, else not binding;
  - Consent can be withdrawn any time, and as easy to withdraw consent as give it;

- Special conditions apply for child (under 16) to give consent
- Explicit consent must be given for processing sensitive personal data
  - Race, ethnic origin, gender, etc
  - Specific circumstances allow non-consensual processing eg to protect vital interests of the data subject
- Secure against accidental loss, destruction or damage (article 5)

Articles 12 - 18: Transparency

- Any communications with a data subject must be concise, transparent, intelligible
- Controller must be transparent in providing information about itself and the purposes of the processing
- Controller must provide data subject with information about their rights
- Specific provisions (Article 14) covering data not obtained directly from the data subject
- Rights to access, rectification, erasure (‘right to be forgotten’), to restriction of processing, and data portability

Article 25 et seq: Privacy by Design

- Privacy must now be designed into data processing by default
- Data controllers/processors not established in the EU must designate a representative
- Data Privacy Impact Assessments mandatory (article 35)
  - For technologies and processes that are likely to result in a high risk to rights of data subjects
- Data audits
  - GDPR applies to existing data, as well as future data
  - Privacy may have to be designed in retrospectively
  - Organizations need to identify what PII they hold, where, on what grounds, and how it is secured in a way that will meet requirements of GDPR

Article 32: Security of Personal Data

- A requirement for data controllers and data processors to implement a level of security appropriate to the risk, including:
  - pseudonymisation and encryption of personal data;
  - ensure the ongoing confidentiality, integrity and availability of systems;
  - a process for regularly testing, assessing and evaluating the effectiveness of security measures;
  - security measures taken need to comply with the concept of privacy by design;

Article 33: Data Breaches

- Mandatory data breach reporting – within 72 hours
  - Describe actions being taken to
    - Address the breach
    - Mitigate the consequences
  - Data subjects contacted ‘without undue delay’
    - Unnecessary if appropriate protection is already in place
    - Consider encryption for all mobile devices, for all databases, and for email
  - Penetration testing to identify potential attack vectors should be standard
- Failure to report within 72 hours must be explained

Article 37 et seq: Data Protection Officer (DPO)

- DPO mandatory in organizations processing substantial volumes of PII (article 37)
- A protected position, reporting directly to senior management
  - Appropriately qualified
  - Consulted in respect of all data processing activities
- Will be a ‘good practice’ appointment outside the mandatory appointments
- Most staff dealing with PII (eg HR, marketing, etc) will need at least basic training
- Staff awareness training also critical (accidental release of PII could have financially damaging consequences)

www.itgovernance.co.uk/shop/p-1833-certified-eu-general-data-protection-regulation-gdpr-foundation-and-practitioner-combination-online-course.aspx

Article 40 et seq: Certifications

- Requirement is to apply appropriate administrative organizational and administrative measures.
- How can you demonstrate this?
  - Codes of conduct and certifications may be used to demonstrate compliance with GDPR
  - Recognised international standards (eg ISO/IEC 27001)
  - Recognised national management standards (eg BS 10012 – for a PIMS or Personal Information Management System)
  - Recognised national technical standards (eg Cyber Essentials in the UK)
  - Emergence of new standards, privacy seals etc across EU
- Certification does not absolve controller of need to comply

Article 44: International Transfers

- Any transfer of personal data by controller or processor shall take place only if certain conditions are complied with:
  - Transfers on the basis of adequacy;
  - Transfers subject to the appropriate safeguards
  - Binding corporate rules apply.
- All provisions shall be applied to ensure the protection of natural persons is not undermined.
- To countries with similar data protection regulations
  - Cloud providers are a key risk area
  - Highest penalties apply to breaches of these provisions
- October 2015: Court of Justice declared Safe Harbor invalid
- April 2016: serious flaws in Privacy Shield:
  - fails to meet EU adequacy standards;
  - lack of a data retention principle;
  - indiscriminate collection of data for national security purposes;
  - insufficiency of legal remedies.
  - Privacy Shield discussions still ongoing

Independent Supervisory Authorities

- Member states must create independent supervisory authorities and resource them appropriately
  - Tasks:
  - Monitor and enforce
  - Communicate
  - Promote awareness
- Powers:
  - To investigate, correct, advise, enforce
- Leading Supervisory Authority for multi-state controllers

European Data Protection Board (EDPB)

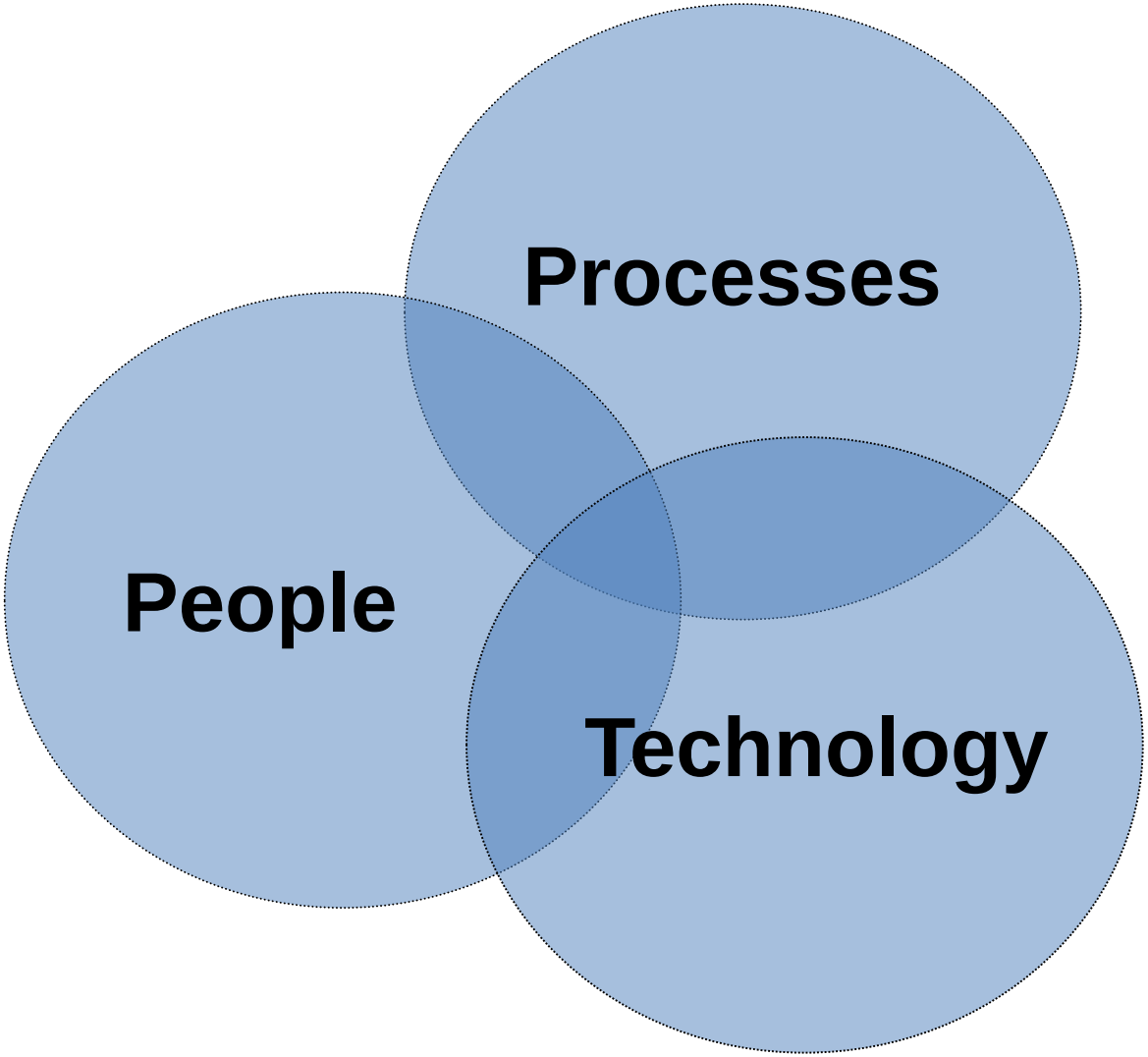
- Ensure cooperation, communication, consistency and mutual assistance between national supervisory authorities
- Monitor and ensure correct application of the Regulation
- Examine any question dealing with its application

- Ie: Ensure a level playing field

GDPR - Summary

- Complete overhaul of data protection framework
  - Covers all forms of PII, including biometric, genetic and location data
- Applies across all member states of the
- Applies to all organizations processing the data of EU citizens – wherever those organizations are geographically based
- Specific requirements around rights of data subjects, obligations on controllers and processors, including privacy by design
- Administrative penalties for breach up to 4% revenue or €20 million
  - Intended to be 'dissuasive'
- Data subjects have a right to bring actions (in their home state) and to receive damages if their human rights have been breached *('Right to an effective judicial remedy against a controller or processor')*
- Fines to take into account *'the technical and organizational measures implemented…'*

Information Security



Cyber Security Assurance

- GDPR requirement - data controllers must implement:
  - "appropriate technical and organizational measures to ensure and to be able to demonstrate that the processing is performed in accordance with the regulation."
  - Must include appropriate data protection policies
  - Organizations may use adherence to approved codes of conduct or management system certifications "as an element by which to demonstrate compliance with their obligations"
  - ICO and BSI are both developing new GDPR-focused standards
- ISO 27001 already meets the "appropriate technical and organizational measures" requirement
- It provides assurance to the board that data security is being managed in accordance with the regulation
- It helps manage ALL information assets and all information security within the organization – protecting against ALL threats

IT Governance: GDPR One-Stop-Shop

- Accredited Training – 1 Day Foundation Course
  - London OR Cambridge: http://www.itgovernance.co.uk/shop/p-1795-certified-eu-general-data-protection-regulation-foundation-gdpr-training-course.aspx
  - ONLINE http://www.itgovernance.co.uk/shop/p-1834-certified-eu-general-data-protection-regulation-foundation-gdpr-online-training-course.aspx
- Practitioner course, classroom or online
  - www.itgovernance.co.uk/shop/p-1824-certified-eu-general-data-protection-regulation-practitioner-gdpr-training-course.aspx
- Pocket Guide www.itgovernance.co.uk/shop/p-1830-eu-gdpr-a-pocket-guide.aspx
- Documentation Toolkit www.itgovernance.co.uk/shop/p-1796-eu-general-data-protection-regulation-gdpr-documentation-toolkit.aspx
- Consultancy support
  - Data audit
  - Transition/implementation consultancy
  - www.itgovernance.co.uk/dpa-compliance-consultancy.aspx

Questions?

acalder@itgovernance.co.uk

0845 070 1750

www.itgovernance.co.uk