The Role of the Data Protection Officer

Adrian Ross LLB (Hons), MBA
GRC Consultant
IT Governance Ltd
28 July 2016

Introduction

- Adrian Ross
- GRC consultant
  - Infrastructure services
  - Business process re-engineering
  - Business intelligence
  - Business architecture
  - Intellectual property
  - Legal compliance
  - Data protection and information security
  - Enterprise risk management

IT Governance Ltd: GRC One-stop shop

All verticals, all sectors, all organisational sizes

Agenda

- An overview of the regulatory landscape
- Territorial scope
- Remedies, liabilities and penalties
- Security of personal data
- Data protection officer

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

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, liabilities and penalties

- **Natural Persons have rights**
  - 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.
  - 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.
- **Administrative fines**
  - Imposition of administrative fines will in each case be effective, proportionate, and dissuasive
    - taking into account technical and organisational measures implemented;
  - € 10,000,000 or, in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year
  - € 20,000,000 or, in case of an undertaking, 4% total worldwide annual turnover in the preceding financial year

Data breaches in the UK

- January to March 2016 - 448 new cases
- Data breaches by sector
  - Health (184)
  - Local government (43)
  - Education (36)
  - General business (36)
  - Finance, insurance and credit (25)
  - Legal (25)
  - Charitable and voluntary (23)
  - Justice (18)
  - Land or property services (17)
  - Other (41)

Source: UK Information Commissioner's Office

Key facts about cyber breaches

Which organisations suffered data breaches in 2015?

- 69% of large organisations
- 38% of small organisation

What was the median number of breaches per company?

- Large organisations: 14
- Small organisations: 4

What was the average cost of the worst single breach?

- Large organisations: £1.46m - £3.14m
- Small organisations: £75k - £311k

What will happen next year?

- 59% of respondents expect more breaches this year than last

- *PwC and BIS: 2015 ISBS Survey*

60% of breached small organisations close down within 6 months – National Cyber Security Alliance

What sorts of breaches?

Of Large Organisations:

- External attack – 69%
- Malware or viruses – 84%
- Denial of service – 37%
- Network penetration (detected) – 37%
  - (if you don't think you've been breached, you're not looking hard enough)
- Know they've suffered IP theft – 19%
- Staff-related security breaches – 75%
- Breaches caused by inadvertent human error – 50%

PwC and BIS: 2015 ISBS Survey

Article 33: Personal data breaches

- The definition of a personal data breach in GDPR:
  - A 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Section 4: Data protection officers

Article 37: Designation of the data protection officer

- DPOs appointed in three situations:
  - Where the processing is carried out by a public body;
  - Where core activities require regular and systematic monitoring of personal data on a large scale;
  - Where core activities involve large-scale processing of sensitive personal data.

Section 4: Data protection officers

- ***Article 37: Designation of the data protection officer***

  - Group undertakings can appoint a single DPO
  - Where controller or processor is a public authority a single DPO may be appointed for several such authorities depending on structure and size
  - DPO can represent categories of controllers and processors
  - DPO designated on the basis of professional qualities and knowledge of data protection law, but not legally qualified
  - May fulfill the role as part of a service contract
  - Controller or processor must publish DPO and notify supervisory authority

Section 4: Data protection officers

Article 38: Position of the data protection officer

- Controller and processor must ensure proper and timely involvement of the DPO
- Controller and processor must provide support through necessary resources
- DPO has a large degree of independence
- Protected role within the organisation
- Direct access to highest management
- Data subject has clear access to DPO
- Bound by confidentiality in accordance with EU law
- No conflict of interest arising from additional tasks or duties

Section 4: Data protection officers

Article 39: Tasks of the data protection officer:

- to inform and advise of obligations;
- to monitor compliance;
- to provide advice with regard to data protection impact assessments;
- to monitor performance
- to cooperate with the supervisory authority;
- to liaise with the supervisory authority;
- to have due regard to risk associated with processing operations.

To advise on data protection impact assessments

Data protection impact assessment

- ***Article 35: Data protection impact assessment***
- The controller shall seek the advice of the DPO
  - where a process is using new technologies, and taking into account the nature, scope, context and purposes of the processing, there is a high risk to the rights and freedoms of natural persons
  - DPIA is particularly required where:
    - Taking into account automated processing including profiling there are legal effects concerning natural persons;
    - The processing is on a large scale of special categories of data or personal data related to criminal convictions;
    - A systematic monitoring of publicly accessible area on a large scale.

Data protection impact assessment

- ***Article 35: Data protection impact assessment***
- A data protection impact assessment shall contain the following:
  - a systematic description of the purposes and means of the processing:
  - any legitimate interest pursued by the controller;
  - an assessment of the necessity and proportionality of the processing operations;
  - an assessment of the risks to the rights and freedoms of data subjects;
  - the measures envisaged to address the risks;
  - adherence to approved codes of conduct;
  - any consultation with data subjects on intended processing;
  - any processing in relation to a law to which the controller is subject;
  - any processing that changes the risk profile.

Prior consultation

- ***Article 36: Prior consultation***
- Controller shall consult the supervisory authority prior to processing where the DPIA indicates a “high risk to the rights and freedoms of the data subjects”:
  - Supervisory authority shall provide written advice to the controller
  - Request for controller to provide further information
  - Information on purposes and means
  - Information on measures and safeguards
  - The contact details of the DPO
  - A copy of the data protection impact assessment
  - Any other information requested

Section 4: Data protection officers

- The realities of the role of the data protection officer
  - Legal knowledge of data protection Regulation is not enough
  - Must also have information security knowledge and skills
  - An understanding of how to deliver C, I and A within a management framework
  - A good understanding of risk management and risk assessments
  - Familiarity with and adherence to codes of conduct for industry sector
  - A good understanding of compliance standards and data marks
  - Able to carry out and interpret internal audits information security standard
  - Understand and be able to articulate privacy by design to delivery functions
  - Able to coordinate and advise on data breaches and notification
  - Able to make a cyber security incident response process work.
  - Leads co-operation with supervisory authority

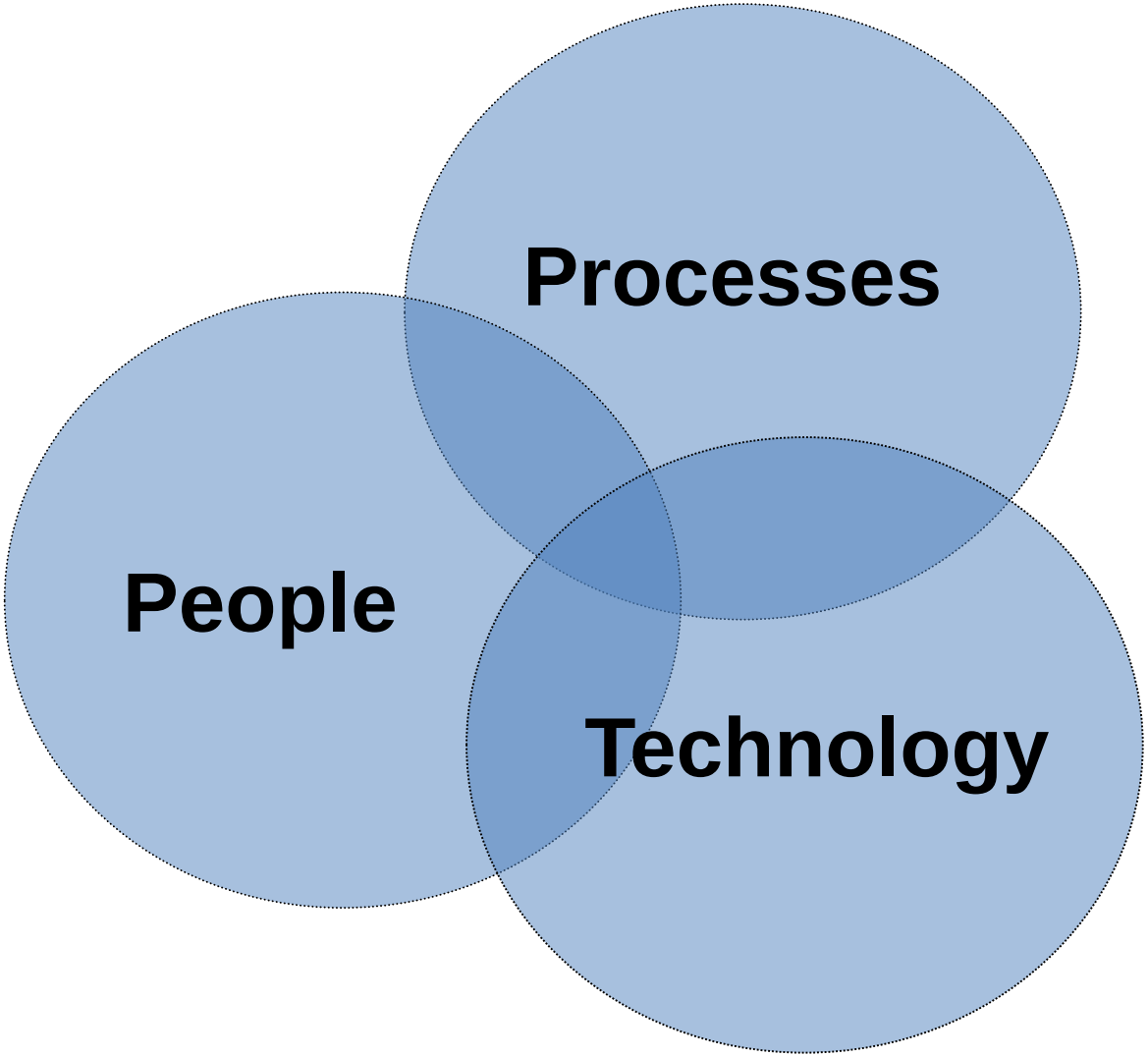
Section 4: Data protection officers

- Where does the role sit within the organisation
  - Outside delivery functions of IT or Business
  - The role is about delivering compliance
  - You cant have compliance under the direction of the delivery team
  - The DPO should sit within a Risk, Compliance or Governance function.
  - Independent of the business with direct access to the Board
  - An effective DPO should ensure that Data Protection is on Board Agenda
  - Company Directors now being considered personally liable for Data Breaches
  - Begin with EU GDPR Foundation Course

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 European Union
- Applies to all organisations processing the data of EU citizens – wherever those organisations 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
- Fines to take into account “*the technical and organisational measures implemented…*”

Information security



Cyber security assurance

- GDPR requirement – data controllers must implement:
  - "appropriate technical and organisational 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 organisational 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 organisation – 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?

aross@itgovernance.co.uk

0845 070 1750

www.itgovernance.co.uk