Data Flow Mapping and the EU GDPR

Adrian Ross LLB (Hons), MBA
GRC Consultant
IT Governance Ltd
29 September 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
- Risk management and the GDPR
- Legal requirements for a DPIA
- Why and how to conduct a data flow mapping exercise
- What are the challenges?
- What is an information flow?
- The questions to ask
- Data flow mapping techniques

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
    - The 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 Regulation was adopted by the European Council.
- 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 will apply from **25 May 2018**.
- http://ec.europa.eu/justice/data-protection/reform/index_en.htm

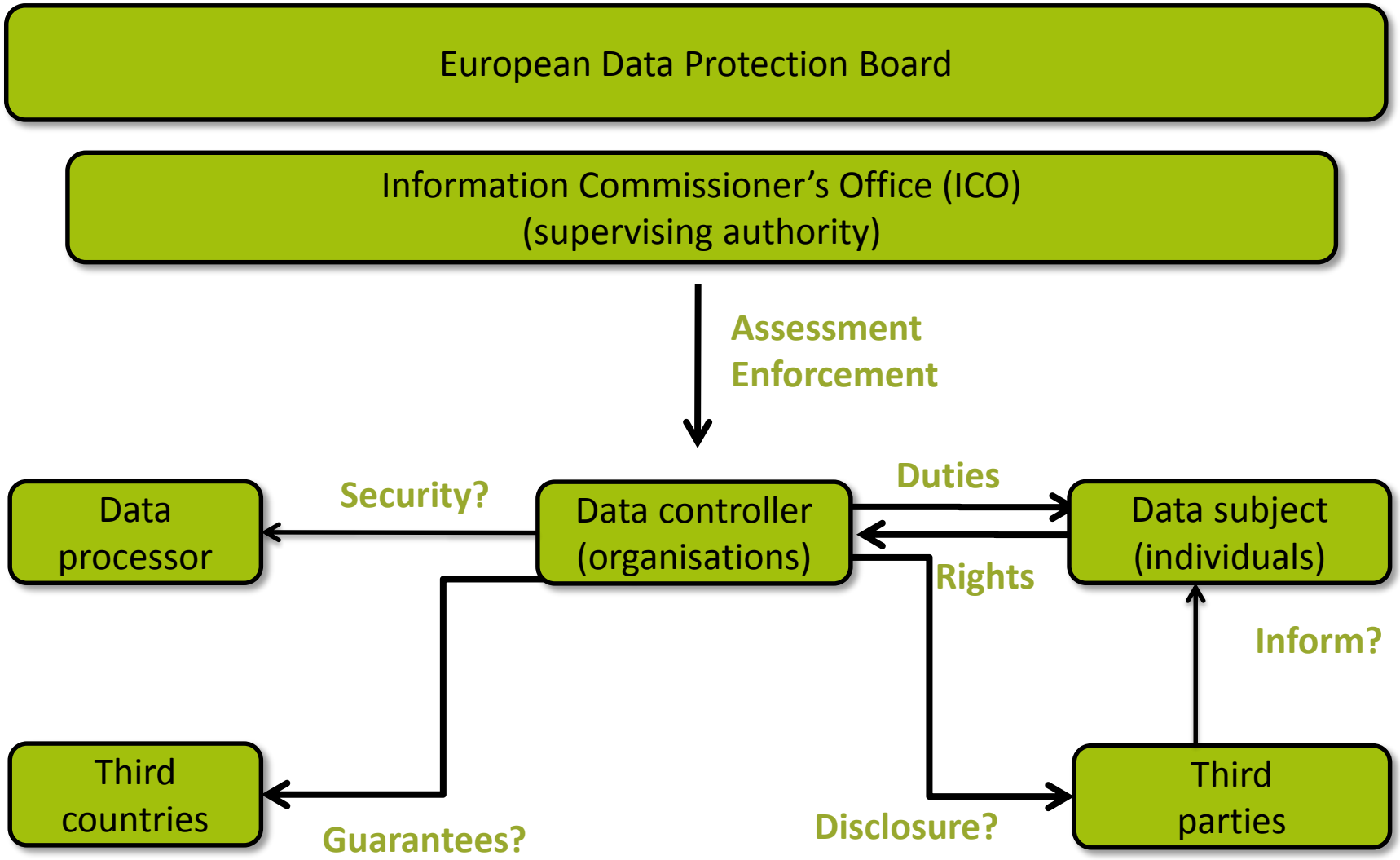
Final text of the Regulation: http://data.consilium.europa.eu/doc/document/ST-5419-2016-REV-1/en/pdf

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 the 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.
- The Regulation also applies to controllers not in the EU.

Remedies, liabilities 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.
  - A 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.
    - Fines shall take into account technical and organisational measures implemented.
  - €20,000,000 or, in the case of an undertaking, 4% of total worldwide annual turnover in the preceding financial year (whichever is higher).

Remedies, liability and penalties (cont.)

Article 83: General conditions for imposing administrative fines

- €10,000,000 or, in the case of an undertaking, 2% of total worldwide annual turnover in the preceding financial year (whichever is greater).
- Articles:
  - 8: Child's consent
  - 11: Processing not requiring identification
  - 25: Data protection by design and by default
  - 26: Joint controllers
  - 27: Representatives of controllers not established in EU
  - 26 - 29 & 30: Processing
  - 31: Cooperation with the supervisory authority
  - 32: Data security
  - 33: Notification of breaches to supervisory authority
  - 34: Communication of breaches to data subjects
  - 35: Data protection impact assessment
  - 36: Prior consultation
  - 37 - 39: DPOs
  - 41(4): Monitoring approved codes of conduct
  - 42: Certification
  - 43: Certification bodies

Remedies, liability and penalties (cont.)

Article 83: General conditions for imposing administrative fines

- €20,000,000 or, in the case of an undertaking, 4% total worldwide annual turnover in the preceding financial year (whichever is higher).
- Articles
  - 5: Principles relating to the processing of personal data
  - 6: Lawfulness of processing
  - 7: Conditions for consent
  - 9: Processing special categories of personal data (i.e. sensitive personal data)
  - 12 - 22: Data subject rights to information, access, rectification, erasure, restriction of processing, data portability, object, profiling
  - 44 - 49: Transfers to third countries
  - 58(1): Requirement to provide access to supervisory authority
  - 58(2): Orders/limitations on processing or the suspension of data flows

Risk management and the GDPR

RISK is mentioned over

60

times in the Regulation.

It is important to understand privacy risk and integrate it into your risk framework.

What is risk?

- The effect of uncertainty on objectives (ISO 31000 etc.)
- The combination of the probability of an event and its consequences (IRM)
- A situation involving exposure to danger (OED)
- Uncertainty of outcome, within a range of exposure, arising from a combination of the impact and the probability of events (*Orange Book* HM Treasury)
- The uncertainty of an event occurring that could have an impact on the achievement of objectives (Institute of Internal Auditors)

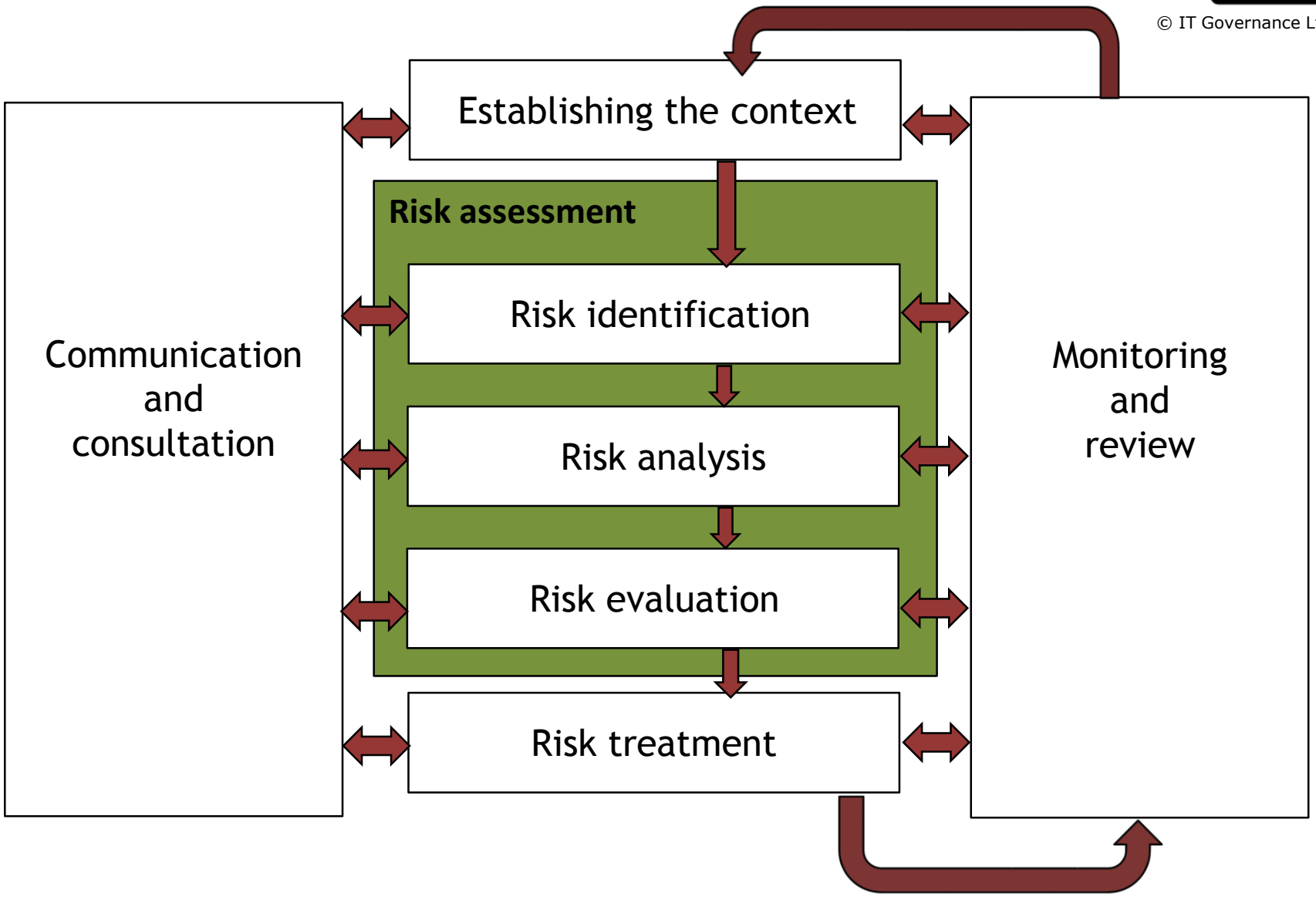
Standards and codes

- ISO 31000 – Risk management – Principles and guidelines
  - AS/NZS 4360:2004 now replaced by ISO 31000
- ISO 31010 – Risk management – Risk assessment techniques
- IRM/ALARM/AIRMIC – A risk management standard
- UK Combined Code on UK Corporate Governance
- OECD Principles of Corporate Governance
- COSO Enterprise Risk Management – Integrated Framework
- Sector specific, e.g. clinical, food
- Discipline specific, e.g. ISO 27005
- ISO 22301 – Business continuity management

ISO 31000: Risk management

- Management framework approach
- PDCA model modified in ISO 27005
- Generic (all risks)
- Very similar to a management system

Risk management process



Enterprise risk management

- Capabilities:
  - Aligning risk appetite and strategy
  - Enhancing risk response decisions
  - Reducing operational surprises and losses
  - Identifying and managing multiple and cross-enterprise risks
  - Seizing opportunities
  - Improving deployment of capital

Risk management

- Organisational risk ‘landscape’
- Strategic
  - Business performance
  - Financial performance
  - Reputation
- Operational
  - Output capacity
  - Demand response
  - Interruption and disruption
- Statutory
  - Employment law
  - Health & safety
  - Company law
- Regulatory
  - Industry/sector-specific compliance requirements
  - Licence to operate
- Contractual
  - SLA targets/levels
  - Product/service availability
  - Quality/warranty

Information security

- Preservation of confidentiality, integrity and availability of information and the assets and processes that support and enable its acquisition, storage, use, protection and disposal.
- Wide variety of assets:
  - information
  - ICT
  - infrastructure
- Prevent compromise (loss, disclosure, corruption, etc.).
- Includes IT security and other forms of security:
  - physical
  - HR
  - supply

Legal requirements for a DPIA

Article 35: Data protection impact assessment

- Controller must seek the advice of the data protection officer.
- This is particularly required in situations that involve:
  - Automated processing
  - Profiling
  - Creation of legal effects
  - Significantly affecting the natural person
  - Processing of large-scale categories of sensitive data
  - Data that relates to criminal offences or convictions
  - Monitoring on a large scale
- Conduct a post-implementation review when risk profile changes.

Legal requirements for a DPIA

Article 35: Data protection impact assessment

- DPIA must be performed where:
  - New technologies are deployed
  - Nature, scope and context of the project demand it
  - Processes are likely to result in a high risk to the rights and freedom
  - It can be used to address sets of processing and risks

Legal requirements for a DPIA

- The DPIA will set out as a minimum:
  - A description of the processing and purposes
  - Legitimate interests pursued by the controller
  - An assessment of the necessity and proportionality of the processing
  - An assessment of the risks to the rights and freedoms of data subjects
  - The measures envisaged to address the risks
  - All safeguards & security measures to demonstrate compliance
  - Indications of timeframes if processing relates to erasure
  - An indication of any data protection by design and default measures
  - List of recipients of personal data
  - Compliance with approved codes of conduct
  - Whether data subjects have been consulted.

Linking the DPIA to the privacy principles

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

Accountability

How to conduct a data mapping exercise

- The ICO staged approach to an effective DPIA:
  1. Required when there is a change in processing of personally identifiable information (PII).
  2. **Determine the information flows throughout the organisation** in order to make a proper assessment of the privacy risks.
  3. Identify the risks related to privacy and processing, including the necessity and proportionality of the change in processing.
  4. Identify possible privacy solutions to address the risks that have been identified.
  5. Assess how the data protection principles have been applied throughout the organisation.
  6. Sign-off and record the DPIA, including details of which privacy solutions are too be implemented.
  7. Integrate the result of the DPIA back into the project plan.
  8. Conduct a post-implementation review where risk profile of PII data has changed.

Why and how to conduct a data mapping exercise

Data mapping – what are the challenges?

Identify personal data

Identify appropriate technical and organisational safeguards

Understand legal & regulatory obligations

Trust and **confidence**

What is an information flow?

A transfer of information from one location to another. For example:

- Inside and outside the European Union.
- From suppliers and sub-suppliers through to customers.

When mapping information flow, you should identify the interaction points between the parties involved.

NB: Cloud providers present their own challenges.

Describing information flows

Walk through the information lifecycle to identify **unforeseen** or unintended uses of the data.

Ensure the **people** who will be using the information are **consulted** on the practical implications.

Consider the potential **future uses** of the information collected, even if it is not immediately necessary.

Information flow – identify the key elements

Data items		
Name, email, address	Health data, criminal records	Biometrics, location data
Formats		
Hardcopy (paper records)	Digital (USB)	Database
Transfer methods		
Post, telephone, social media	Internal (within group)	External (data sharing)
Locations		
Offices	Cloud	Third parties

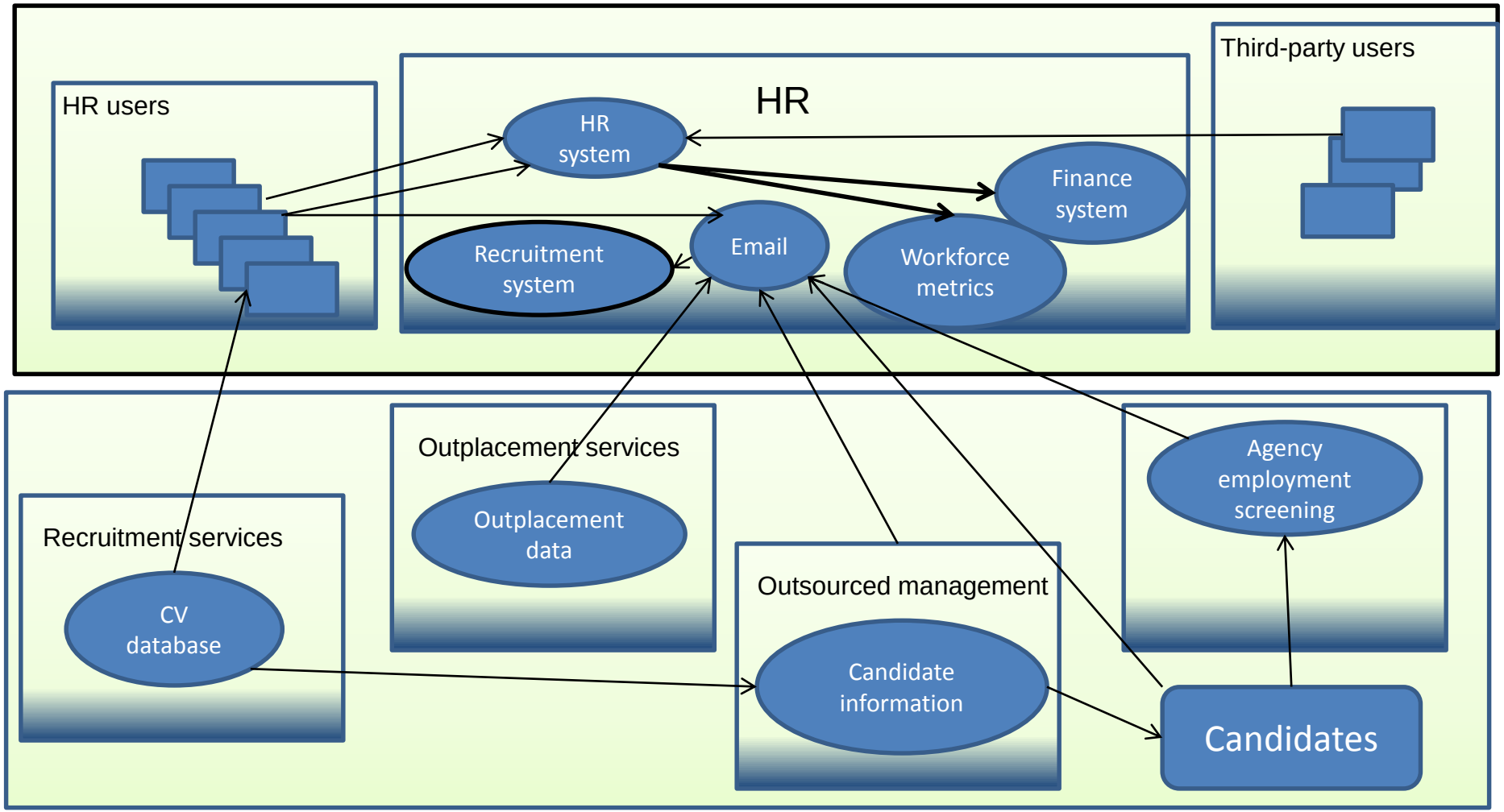
Data flow mapping – questions to ask

- Workflow inputs and outputs:
  - How is personal data collected (e.g. form, online, call centre, other)?
  - Who is accountable for personal data?
  - What is the location of the systems/filing systems containing the data?
  - Who has access to the information?
  - Is the information disclosed/shared with anyone (e.g suppliers, third parties)?
  - Does the system interface with, or transfer information to, other systems?

Data flow mapping – techniques

- Inspect existing documents
- Facilitation workshops
- Questionnaires
- Observation
- Whiteboard – freeform diagrams
- Template drawings (Visio, mind map tools)
- Post-it notes

Example information flow



IT Governance: GDPR one-stop shop

- Accredited training, one-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:
  - http://www.itgovernance.co.uk/shop/p-1824-certified-eu-general-data-protection-regulation-practitioner-gdpr-training-course.aspx
- Pocket guide: http://www.itgovernance.co.uk/shop/p-1830-eu-gdpr-a-pocket-guide.aspx
- Documentation toolkit: http://www.itgovernance.co.uk/shop/p-1796-eu-general-data-protection-regulation-gdpr-documentation-toolkit.aspx
- Consultancy support :
  - Data audit
  - Transition/implementation consultancy
  - http://www.itgovernance.co.uk/dpa-compliance-consultancy.aspx

Questions?

aross@itgovernance.co.uk

0845 070 1750

www.itgovernance.co.uk