Revising policies and procedures under the new EU GDPR

Richard Campo, CISM
GRC Consultant
IT Governance Ltd
1 Sept 2016

Introduction

- Richard Campo
- GRC consultant
  - Data protection and information security
  - Lead auditor
  - Lead ISO27001:2013 implementer
  - GDPR compliance
  - 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, liability and penalties
- Principles of the EU GDPR
- Policies - GDPR reference (Recital 78, Articles 4, 24, 39)
- What if we don’t have policies in place?
- What policies are required?
- How to develop a policy?

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

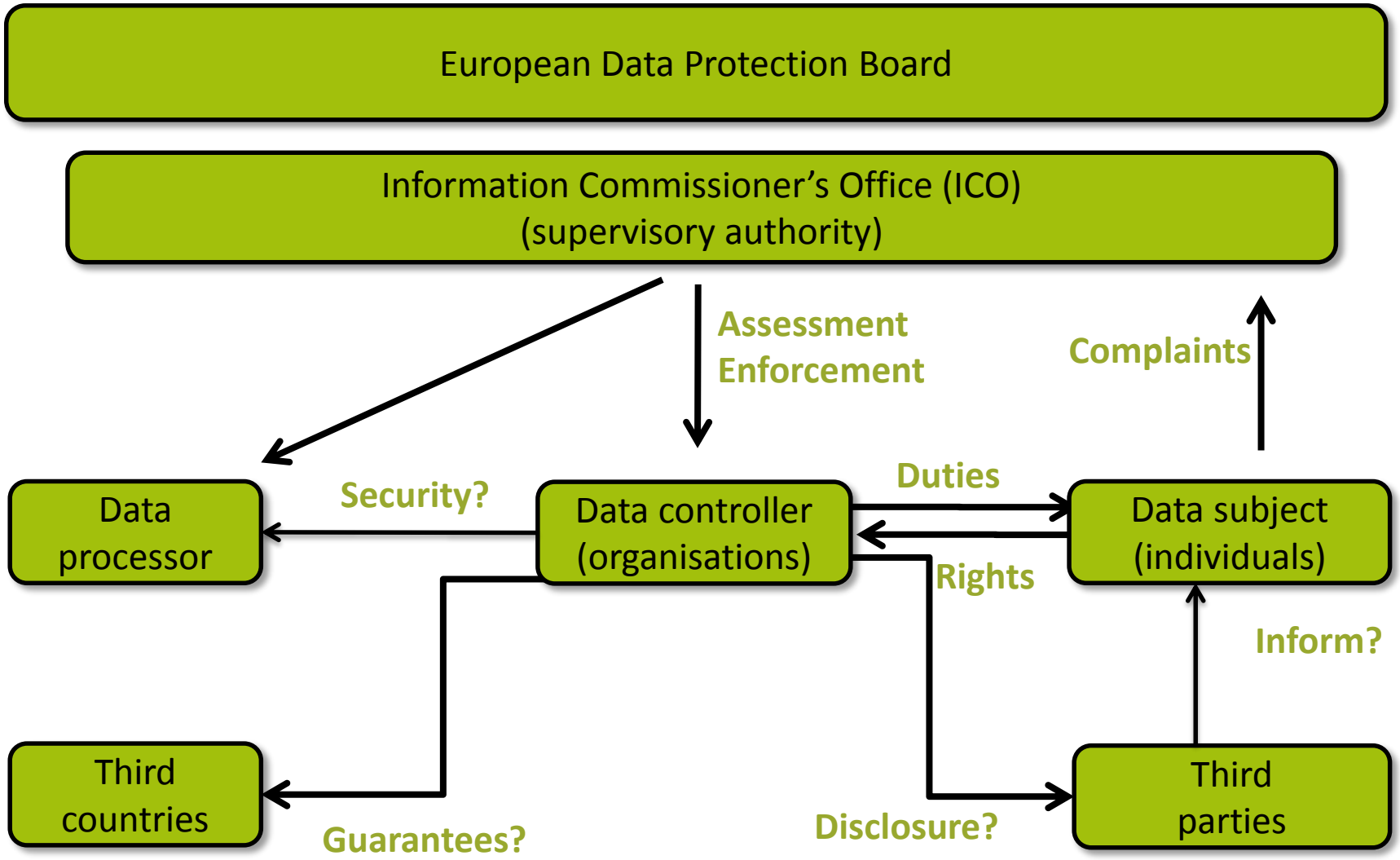
Final text of the Regulation: http://data.consilium.europa.eu/doc/document/ST-5419-2016-REV-1/en/pdf

GDPR

The GDPR 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, liability 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, 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.
  - 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

Recital 78 – Demonstrating compliance

"In order to be able to demonstrate compliance with this Regulation, the controller ***should adopt internal policies*** and implement measures which meet in particular the principles of data protection by design and data protection by default."

Article 4 - Definitions (20)

‘Binding corporate rules’ means personal ***data protection policies*** which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity.

Article 24 – Responsibilities of the Data Controller

Where proportionate in relation to processing activities, measures shall include the ***implementation of appropriate data protection policies*** by the controller.

Article 39 - Tasks of the data protection officer

To monitor ***compliance*** with this Regulation, with other Union or Member State data protection provisions and **with the policies of the controller or processor** in relation to the protection of personal data.

What should a Privacy Policy include?

Article 13: Information to be provided where personal data collected from the data subject

- When obtaining personal data, the controller shall provide the data subject with all of the following information:

  - the identity and contact details of the controller and their representative;
  - the contact details of the data protection officer, where applicable;
  - the purposes of the processing of as well as the legal basis for the processing;
  - the legitimate interests pursued by the controller or by a third party;
  - the recipients or categories of recipients of the personal data, if any;
  - the fact that the controller intends to transfer personal data to a third country and the existence of adequacy conditions.

What should a Privacy Policy include?

Article 13: When obtaining personal data the controller shall provide the data subject with the following further information to ensure fair and transparent processing:

- the period of time that the data will be stored;
- the right to rectification, erasure, restriction, objection;
- the right to data portability;
- the right to withdraw consent at any time;
- the right to lodge a complaint with a supervisory authority;
- the consequences of the data subject failure to provide data;
- the existence of automated decision-making, including profiling, as well as the anticipated consequences for the data subject.

What should a Privacy Policy include?

Article 14: Information to be provided where the personal data have not been obtained from the data subject

- Where personal data has not been obtained directly from the data subject:
  - the identity and contact details of the controller and their representative;
  - the contact details of the data protection officer, where applicable;
  - the purposes as well as the legal basis of the processing;
  - the categories of personal data concerned;
  - the recipients of the personal data, where applicable;
  - the fact that the controller intends to transfer personal data to a third country and the existence of adequacy conditions.

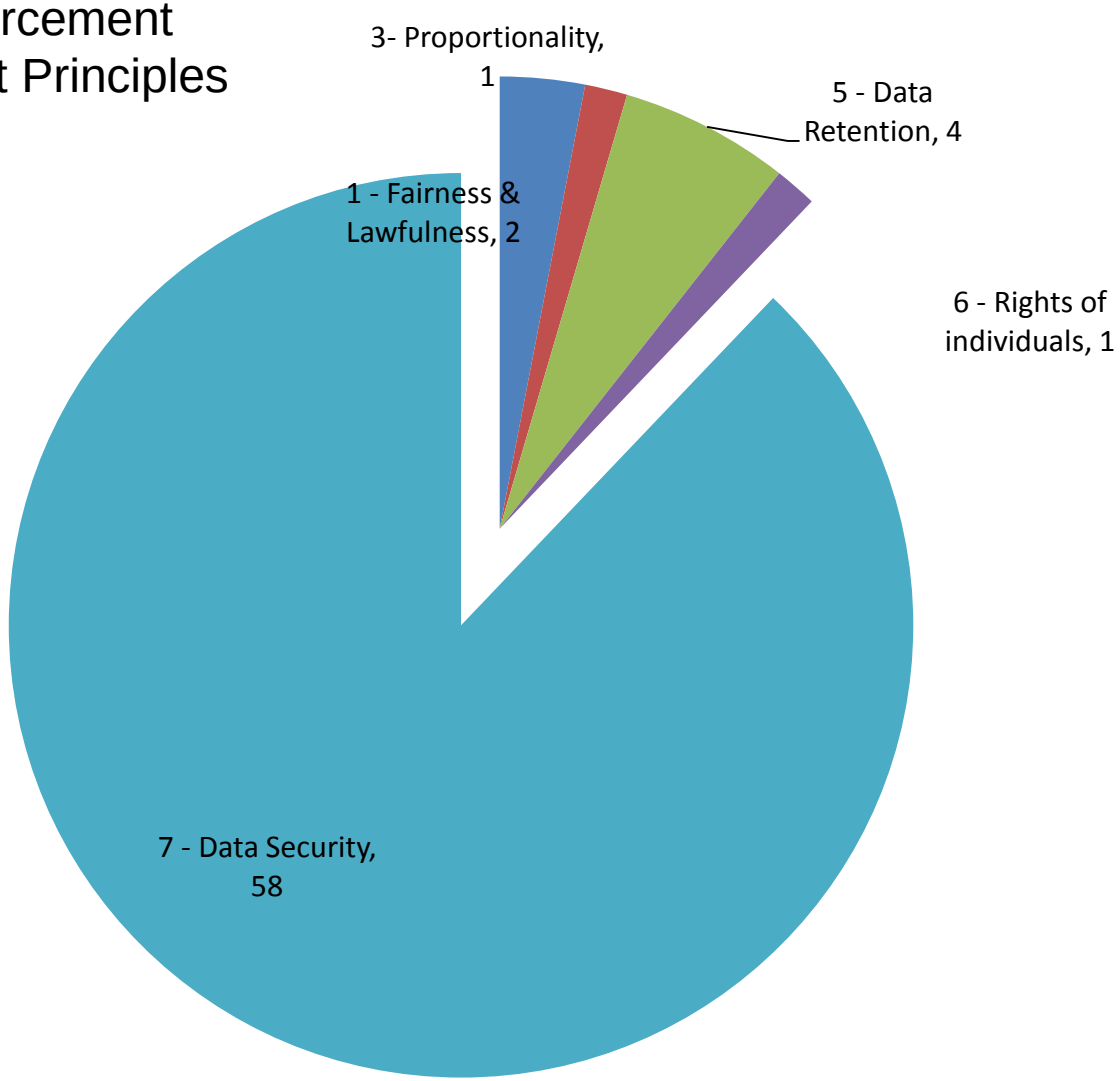
Data breaches in the UK

- 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

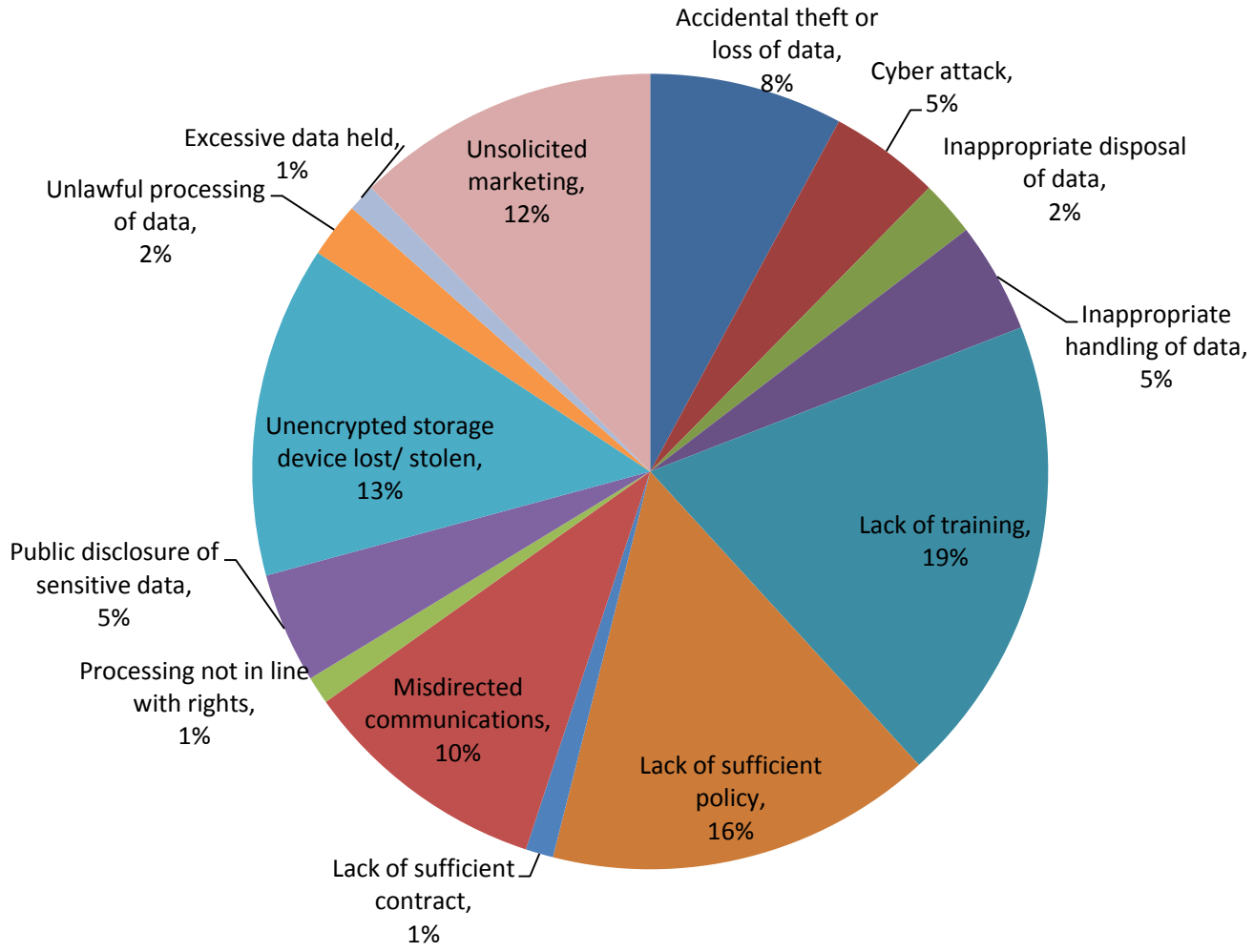
Enforcement action - Principles

Count of enforcement action against Principles



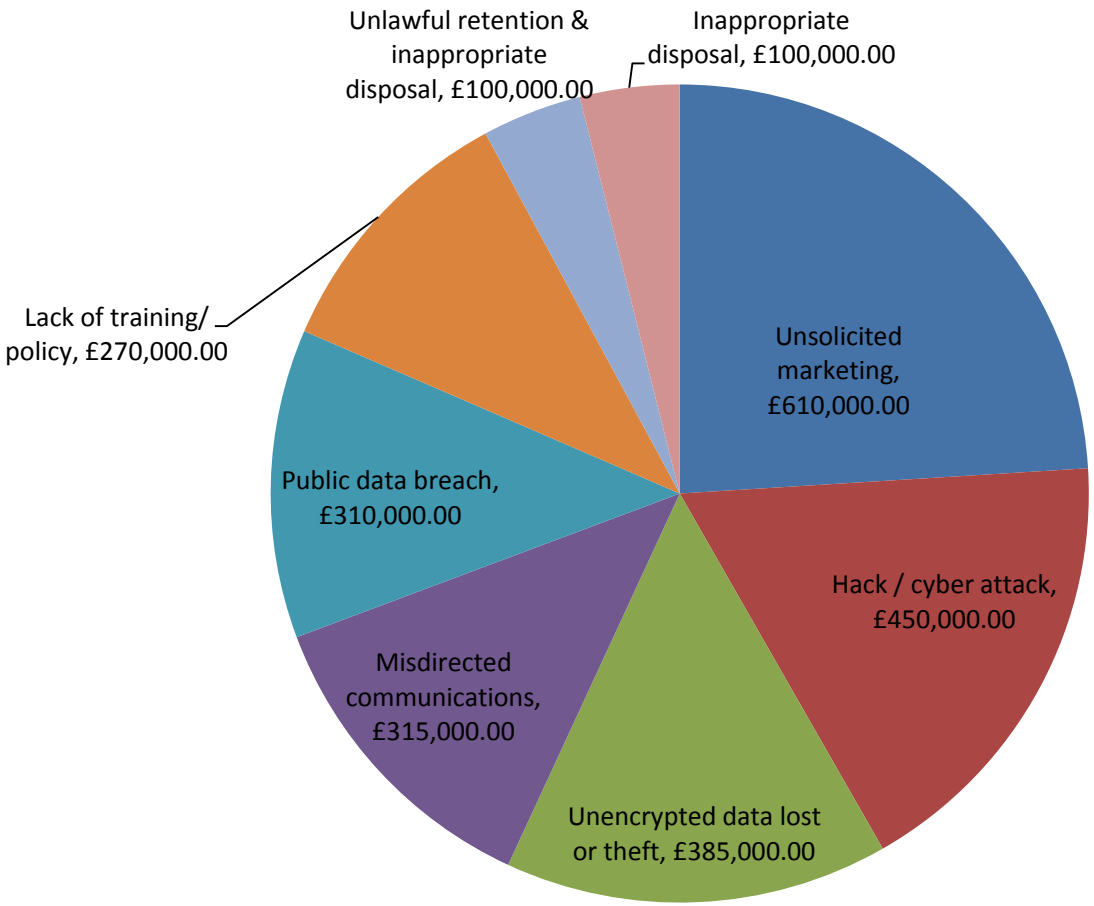
Source: ICO

Enforcement action - Reasons



Source: ICO

Enforcement action: Monetary penalties

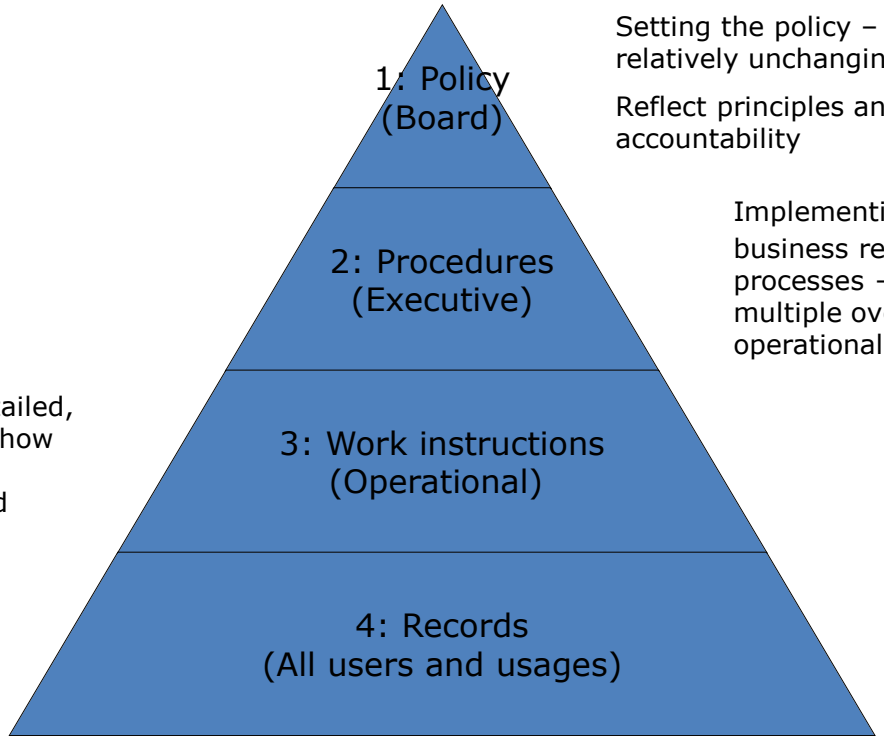


Source: ICO

What is a policy?

- Policies are documents that define the objectives of an organisation.
- A policy is a statement of intent.
- Procedures outline what people must do in order to deliver the policy objectives.
- Guidelines provide advice on how to comply with policies.
- Policies are generally adopted by the Board of or senior governance body within an organisation.

Documentation structure



Setting the policy – strategic, high level, relatively unchanging – board approved

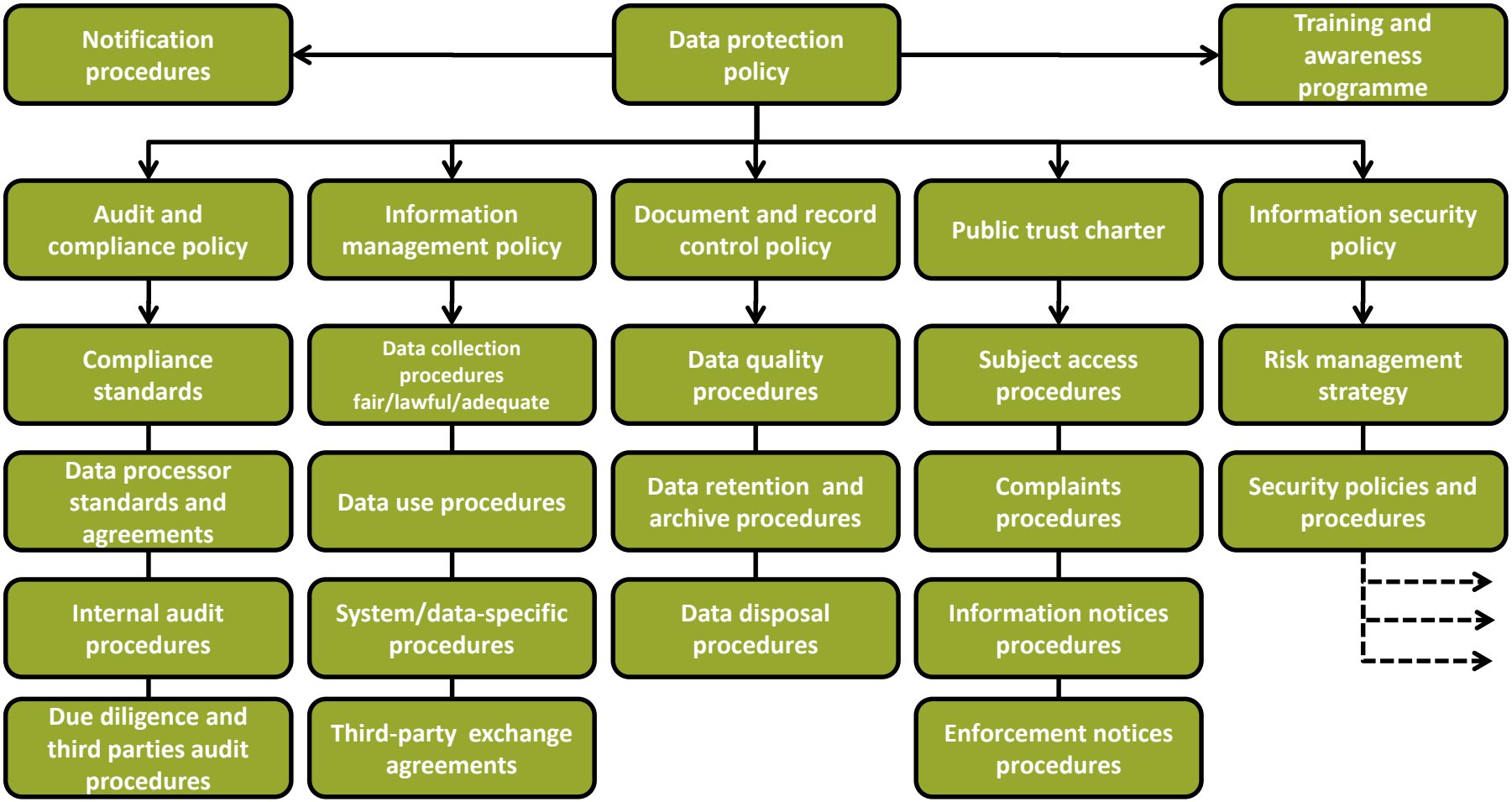
Reflect principles and demonstrate board accountability

Implementing the policy – setting out business requirements, procedures and processes – change infrequently but have multiple overlaps and impacts on operational activity and business behaviours

Making the policy work – detailed, step-by-step descriptions of how to perform individual tasks – subject to regular review and improvement

Records of what happened – minutes, logs, reports, etc – information about how the ISMS is performing

What policies and procedures are required?



Steps to develop a policy?

Step 1: Identify the policy objectives

Identify the needs and expectations of interested parties that should inform the policy.

Steps to develop a policy?

Step 2: Develop a policy framework

The policy framework should have a few high-level policies that inform the more granular components such as procedures and processes.

Steps to develop a policy?

Step 3: Communicate and enforce the policies.

Communication should apply to all those within the scope of the policy. Audit the policies' effectiveness.

Steps to develop a policy?

Step 4: Review and update the policies

Policies shouldn’t change too often, but they are living documents and require periodic reviews to keep them relevant.

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 residents – 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 *("Right to an effective judicial remedy against a controller or processor")*
- Fines to take into account *"the technical and organisational measures implemented…"*

IT Governance: GDPR one-stop shop

- Accredited training – 1-Day Foundation Course
  - London OR Cambridge: www.itgovernance.co.uk/shop/p-1795-certified-eu-general-data-protection-regulation-foundation-gdpr-training-course.aspx
  - ONLINE 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?

rcampo@itgovernance.co.uk

0845 070 1750

www.itgovernance.co.uk