EU GDPR and you: requirements for marketing

Richard Campo
GRC Consultant
IT Governance Ltd
27 October 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, liabilities and penalties
- Privacy notices
- The rights of data subjects
- Consent
- Data processing
- Profiling or “automated individual decision-making"
- International marketing and data transfers

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 GDPR is a regulation

Article 99: Entry into force and application

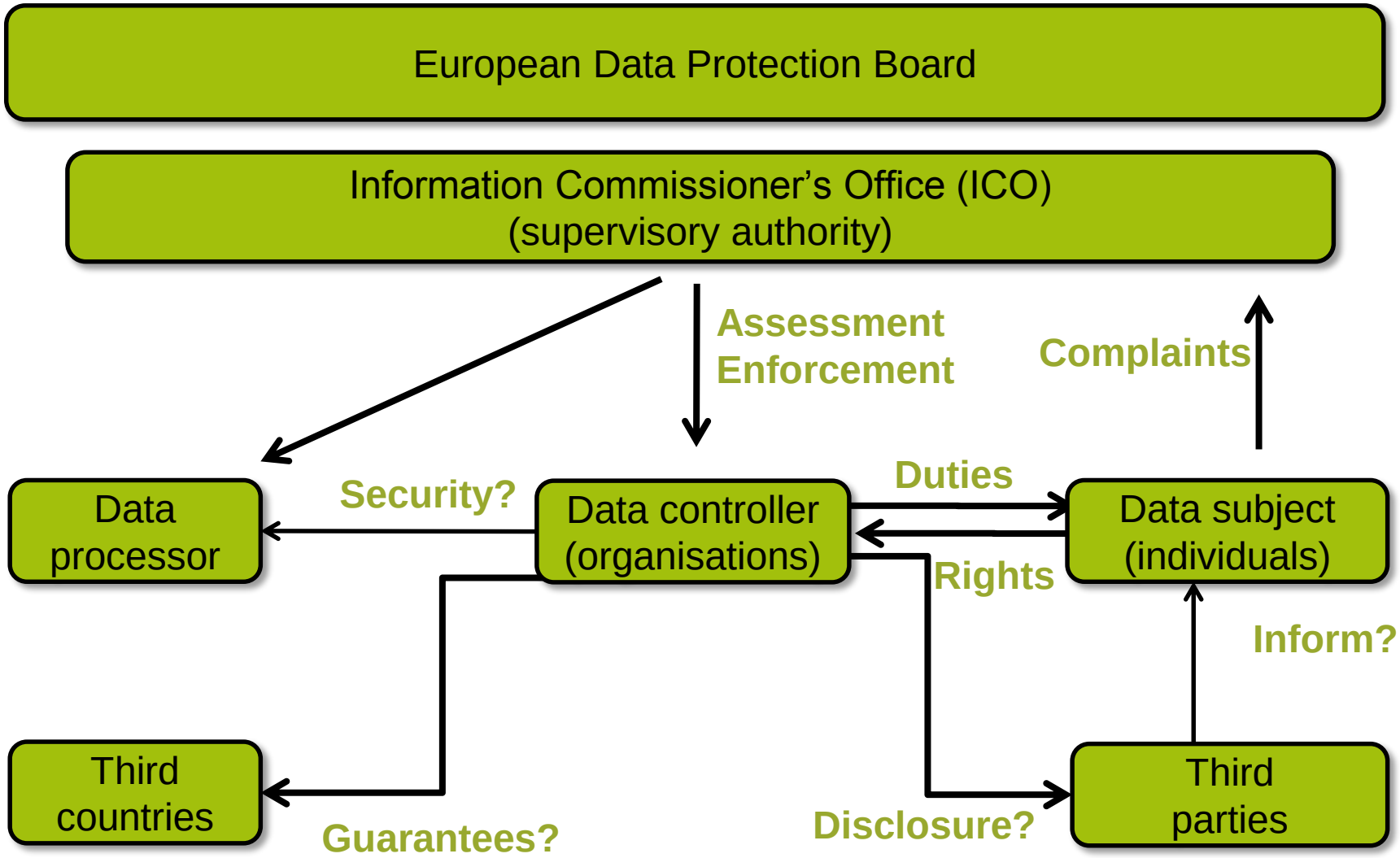
This Regulation shall be binding in its entirety and directly applicable in all member states.

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 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

Data protection model under the GDPR



Articles 1 – 3: Who and where?

- A **natural person** is defined as 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.
- ***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.
  - €20,000,000 or, in 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 case of an undertaking, 2% 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 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

Lessons from marketing breaches

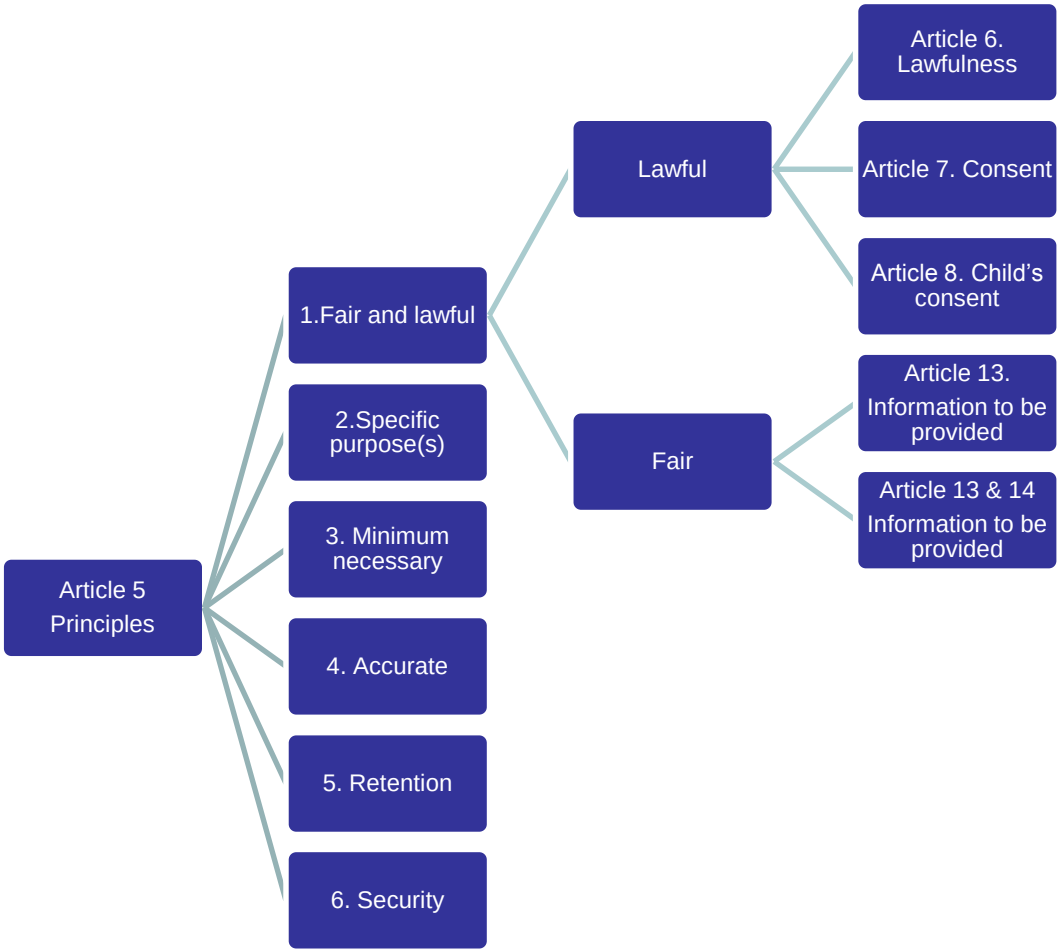
- A car finance brokerage company that used a public telecommunications service for the purpose of instigating 65,000 unsolicited direct marketing text messages has been fined £30,000 by the ICO.
- A debt management company that sent unwanted marketing texts has been fined £40,000 by the ICO.
- A company that made 1.6 million nuisance calls to try and sell solar panels and green energy equipment has been fined £60,000 by the ICO.
- The ICO has issued a stop order against a company that falsely claimed it was phoning people as part of a lifestyle survey – a practice known as “sugging”.

The GDPR 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 integrity & confidentiality

Accountability

From principles to specific obligations.



Privacy notices (Article 12)

- Processing shall be **lawful only** and have at least one of the following criteria apply:
  - Data subject provided **consent for processing data** for specific purposes.
  - Processing is required in carrying out a **contract**.
  - Where processing is necessary for **compliance with legal obligation** and the controller is a subject.
  - In the situation where processing is essential to **protect vital interest** of the data subject.
  - Under circumstances where processing the performance of a task carried out in the **public interest** of official authority vested in the controller.

- The controller is required to **take appropriate measures** and provide data subject with the following information:
  - The identity and **contact details of controller** *(if applicable, the controller's representative).*
  - The **data protection officer (DPO)** details *(if applicable).*
  - The **purpose** for which personal data is processed and intended.
  - The **legal basis** for the processing.
  - The **legitimate interest** pursed by controller in processing the data where the data subject is a child.
  - The recipients or **categories** of recipients of personal data.

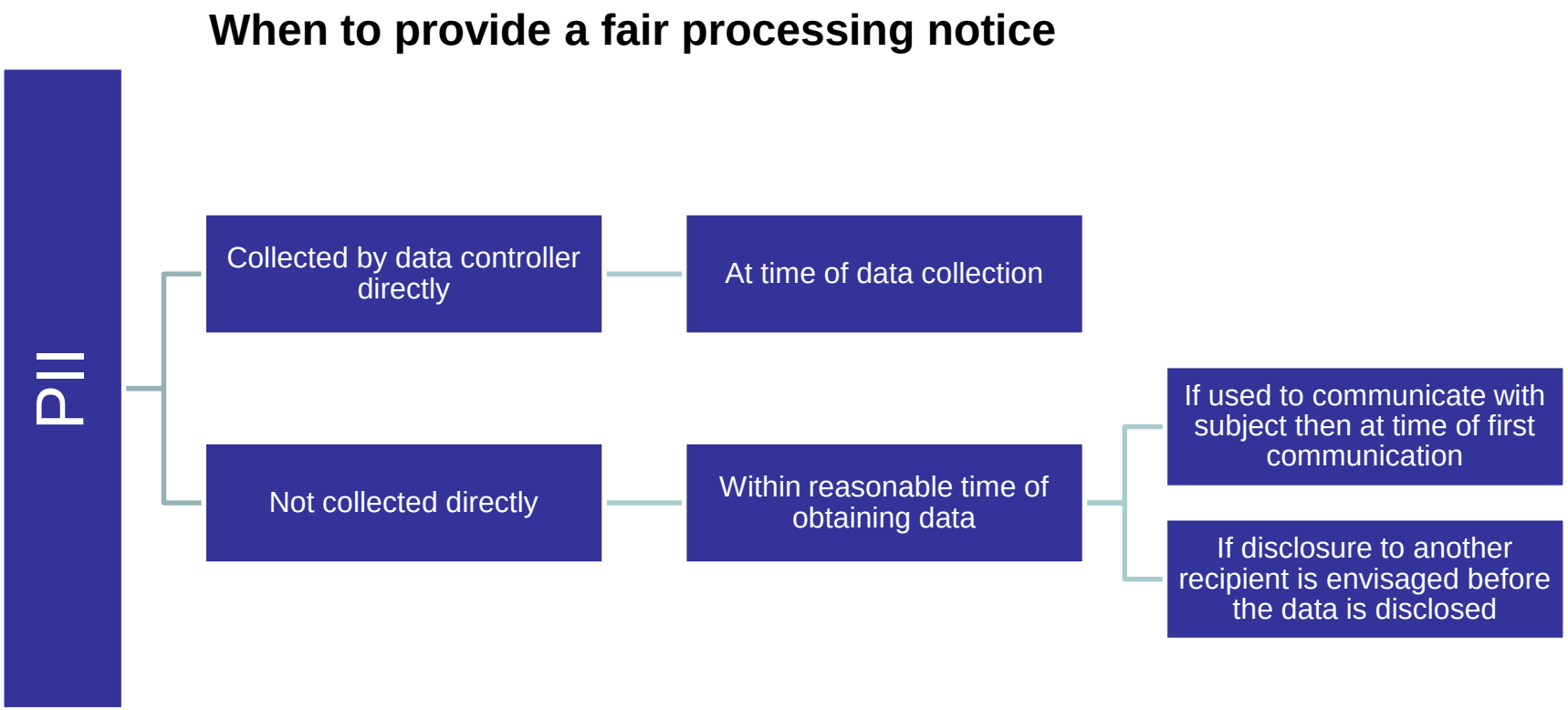
Fair processing notice

(Recitals 39, 42 and 58; Articles 13 and 14)

The notice must be:

- Concise
- Clear and in plain language (consider notice if addressed to child)
- Available and easily accessible to data subjects

When to provide a fair processing notice



Consent

Recitals 32, 33, 38, 42, 43 and 54; Article 4

The GDPR defines consent as:

"must be freely given, specific, informed and unambiguous indication of the data subject's wishes by which a statement or clear affirmative action, signifies agreement to the processing of personal data relating to the subject."

Conditions for relying on consent

Recitals 32, 33, 38, 42, 43 and 54; Article 4

- “The controller must be able to **demonstrate** that the data **subject has consented** to the processing.”
- Data subject must be able to withdraw consent at any time.
- It shall be as **easy to withdraw** consent as to give it.

Consent

Recitals 32, 33, 38, 42, 43 and 54; Article 4

Conditions for relying on consent

- Consent should cover all processing activities carried out for the same purpose(s).
- If processing for multiple purposes, consent should be given for all of them.
- Specific rules applies to children (e.g. verify age, seek parental consent).
- Consent should not be considered freely given if data subject has no genuine or free choice.

Consent

Recitals 32, 33, 38, 42, 43 and 54; Article 4

Demonstrating compliance

- Cannot rely on silence, inactivity or pre-ticked boxes.
- Policy or process in place to inform how to withdraw consent.
- Separate consent if purpose changes.
- Link your privacy policy to tools that enable individuals to control how the information is used and shared.

Eight rights of data subjects

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision-making and profiling

Data subjects' right to object

Article 21

- Data subjects have the right to **object at any time to processing personal data** on grounds relating to a particular situation concerning the data subject, profiling or automated decision-making.

- Unless **legitimate grounds** for processing are demonstrated, the controller can no longer process the personal data.

- Data subjects have the right to object to any use of data for direct marketing or **profiling related to direct marketing**.

- Data subjects whose personal **data is processed for scientific or historical research purposes or statistical purposes** have the right to object to processing of personal data, unless "the processing is necessary for the performance of a task carried out for reasons of public interest".

Profiling or "Automated individual decision-making"

- Organisations are **required to inform data subjects** before first communication through explicit wording clearly and separately from other information about the **existence of profiling**.

- Profiling comprises data subject's:
  - personal preferences;
  - interests;
  - behaviours;
  - location;
  - movements;

- With the exception of some contracts, data subjects have the right to **object to profiling**.

- The use of the privacy policy is strongly encouraged for **notifying data subjects**.

International marketing and transfers

- The EU GDPR applies to European Union member states and provides a **standardised framework** across the EU.

- Organisations trading in Europe benefit from **harmonisation** in data protection legislation and an equal playing field.

- **US-EU Safe Harbor:**
  - The agreement on transatlantic data sharing between US and EU was **declared invalid** in October 2015.
  - Until new transatlantic agreement is validated, businesses are encourage to evaluate **alternative frameworks** to ensure compliant data transfers.

Summary of marketing rules

Method of communication	Direct to data subject	Business-to-business
Live calls	• Screen against Telephone Preference service • Provide opt-out	• Screen against Telephone Preference service • Provide opt-out
Recorded calls	• Data subject must have given specific consent to make recorded marketing calls	• Data subject must have given specific-consent to make recorded marketing calls
Emails or texts	• Data subject must have given sender-specific consent to send marketing emails/texts • Provide opt-out	• Cam email or text corporate bodies • Good practice to offer opt out • Individual employees can opt out
Mail	• Name and address obtained fairly • Provide opt-out	• Can mail corporate bodies • Individual employees can opt out

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 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, one-day Foundation course:
  - London, Cambridge, Manchester, Edinburgh, Dublin: www.itgovernance.co.uk/shop/p-1795-certified-eu-general-data-protection-regulation-foundation-gdpr-training-course.aspx
  - ONLINE (GMT, EST, CET live 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