JOHNSTON CARMICHAEL

Where sharp minds meet

Business Boosters: GDPR

Sarah Pumfrett, FCCA, CMIIA, SIRM
Audit Director – Business Risk Assurance

NOTE: *This presentation and associated commentary are not legal advice and no reliance should be placed upon its completeness, accuracy or validity. GDPR is a complex principle based law, open to interpretation and configurable by Member States. Limited reliable guidance currently exists and supervisory authorities and courts may take different views to those expressed during this presentation as the legislation becomes embedded.*

Sarah Pumfrett, Audit Director – Business Risk Assurance

FCCA, CMIIA, SIRM

- Chartered Certified Accountant;
- Chartered Internal Auditor; and
- Specialist Member of the Institute of Risk Management.

- Background in internal audit covering assurance across all aspects of business risk in both public and private sector.

- Experience of information and data audits both for business efficiency and legislative compliance.

What is GDPR?

EU General Data Protection Regulation

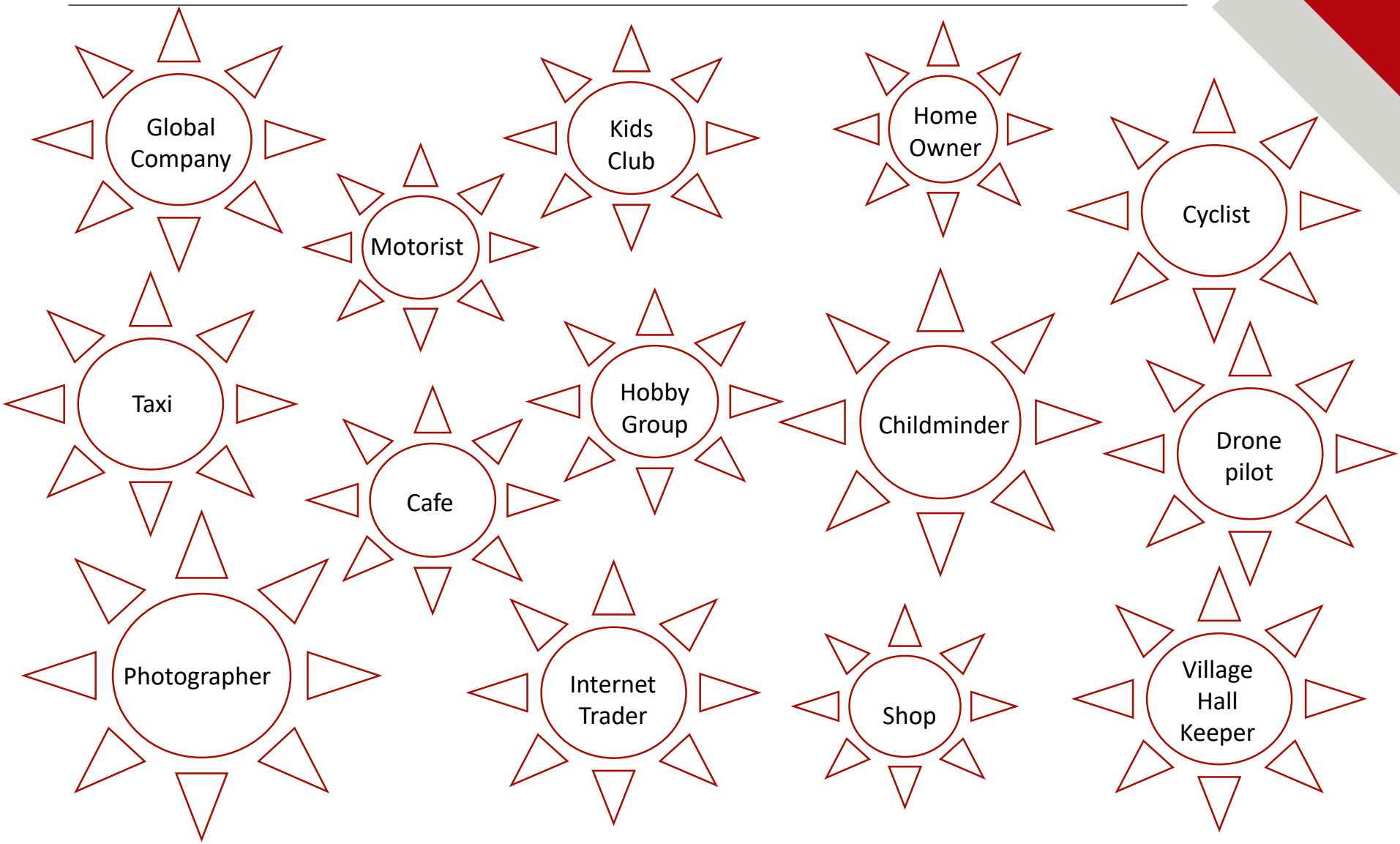
- An EU regulation;
- It covers personal data;
- It comes into effect, Friday 25th May 2018;
- It replaces the Data Protection Act of 1998;
- It applies to entities of all sizes;

What is GDPR?

EU General Data Protection Regulation

- It covers EU subjects and is extra-territorial;
- Data Controllers and Data Processors jointly responsible for correct management of data;
- It ensures responsibility and liability for compliance sits with those at the top of the organisation;
- It applies to both data and information in all media.
- Fines up to 4% of Global Turnover or €20M for a serious breach or 2% or €10M for failing to report a breach, conduct an impact assessment or maintain appropriate records.

Who must comply with GDPR?



GDPR – Jurisdiction relevance

- GDPR is designed to standardise:
  - data protection laws across Europe;
  - protection for EU data subjects globally; and
  - the manner in which organisations approach data protection.

GDPR – Jurisdiction relevance to disclaimer

- This presentation and associated commentary are not legal advice and no reliance should be placed upon its completeness, accuracy or validity.
- GDPR is a complex principle based law, open to interpretation and configurable by Member States.
- Limited reliable guidance currently exists and supervisory authorities and courts may take different views to those expressed during this presentation as the legislation becomes embedded.

GDPR – The Principles (paraphrased)

Personal Data shall be:

- Processed lawfully, fairly and with transparency for individuals;
- Collected and processed for legitimate, defined purposes;
- Adequate, relevant and restricted to what is required;
- Accurate and up to date;
- Destroyed in a timely manner once no longer required; and
- Protected from unauthorised access, processing or destruction.

GDPR – How to prepare

- Ensure key people have **Awareness** of obligations under GDPR;
- **Identify the data** and information you hold;
- Determine and document your **legal bases** for personal data processing;
- Establish or update **policies, procedures & contracts**
- Consider your responsibilities in relation to **international data transfers**
- **Communicate Privacy Information**
- Determine requirement for **Data Protection Officer**
- Establish how you ensure you are meeting **Individuals Rights**
- Review your data and **information security**
- Revisit everything and **confirm you're comfortable with the risk management** for your organisation.
- Periodically **audit your risk management** and consider if the assumptions and controls are still valid.

GDPR – Individuals Rights

- Be informed;
- Access;
- Rectification;
- Erasure;
- Restrict processing;
- Data portability;
- Object; and
- Automated decision making (including profiling).

GDPR – Privacy by design

- Data Security is linked to Confidentiality; achieved through a combination of logical and physical controls.
- Logical controls include anti-malware, passwords, identity and access management including least privileged access.
- Physical controls include access controls to buildings, data stores and computers.
- Data encryption prevents access without the key. Useful for email and laptop hard drive.
- Information security standards such as IASME, Cyber Essentials [+] or ISO 27001 are a good starting point.

GDPR – Marketing

- Opt out

- GDPR, PECR and ePR
  - The Privacy and Electronic Communications (EC Directive Regualtions 2003)
  - e-Privacy Regulation will take precedence over GDPR

GDPR – Breaches

- 72 hours to notify ICO
- Notifying affected data subjects
- €10M and 2%
- €20M and 4%

Blockers to implementation

- Clarity
- Business Change Management
- Culture
- It takes two
- Historical Baggage
- Snake Oil
- 3rd Party processors
- Training

GDPR – Where to get help

- The Information Commissioners Office website:

  ICO.org.uk

- Your professional advisers (lawyer, accountant and IT supplier);
- Google (other search engines available)!

  NOTE: Ensure you are running anti-malware when performing the search and only use links to legitimate sites.

Questions? Raise your right hand
Answers – Raise your left hand

JOHNSTON CARMICHAEL