General Data Protection Regulation (GDPR)

HOSPA - IT COMMUNITY MEMBERS EVENT

15th March 2018

Jonathan Gray, Partner

pitmans law

pitmans law

Agenda

- The Law
- Are you a “data controller” or a “data processor” under GDPR?
- Short term and long term actions.

pitmans law

What is the GDPR?

- Replaces regime under Data Protection Act 1998 in the UK
- Comes into force **25th May 2018**
- Introduced in response to technological advances, making it easier to collect, store, disseminate and manipulate data
- Intends to harmonise the framework for protecting personal data across the EU
- UK expected to adopt similar national data protection regime after Brexit
- Data Protection Bill – making its way through the House of Lords
- Supervisory authority in the UK – the ICO

pitmans law

What is the GDPR? (continued)

- Applies to:
  - processing of **personal data** of individuals in the context of activities of a **data controller** or **data processor** established in the EU, regardless of where processing takes place. Includes non-EU organisations that offer goods or services to data subjects in the EU;
  - **data subjects**, regardless of nationality or place of residence;
  - automated and manual processing;
  - electronic and hard copy data;
  - personal data which form/are intended to form part of a **filing system** (a structured set of personal data, accessible according to specific criteria).

pitmans law

Personal Data

- Now includes identification numbers, location, online identifiers and factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
- Still includes information about activities when linked to an identifier
- Sensitive data now includes genetic and biometric data
- Criminal records now occupy a separate category and are treated distinctly

pitmans law

Controllers and Processors

The GDPR applies to ‘controllers’ and ‘processors’.

- A controller determines the purposes and means of processing personal data.
- A processor is responsible for processing personal data on behalf of a controller.
- If you are a processor, the GDPR places specific legal obligations on you; for example, you are required to maintain records of personal data and processing activities. You will have legal liability if you are responsible for a breach.
- However, if you are a controller, you are not relieved of your obligations where a processor is involved – the GDPR places further obligations on you to ensure your contracts with processors comply with the GDPR.

pitmans law

Lawful processing

- **Contract** – necessary for the formation or performance of a contract between the controller and subject
- **Obligation** – necessary for performance of a legal obligation, or discharge of a statutory function
- **Vital interests** – to protect the vital interests of the data subject or someone else
- **Special data** – additional conditions must be satisfied to be able to process special data

pitmans law

Lawful processing - Consent

- Consent must be freely given, specific, informed and unambiguous by “some form of clear affirmative action”
- It cannot be signified by inaction, silence or be a precondition to other actions
- It must be as easy for a subject to withdraw consent as to give it – form and substance
- Remember that processing under consent gives the data subject wider rights than other lawfulness gateways

pitmans law

Processes – Risk assessment

- Identify each of the processes of your business which engage personal data
- Do you process as controller or processor – what is the lawfulness gateway?
- Is the processing proportionate to the objectives?
- What measures of safeguarding are appropriate anonymisation/pseudonymisation; encryption; permissions; policies

pitmans law

Processes – Breach notification

- Now mandatory for breaches: “leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data”
- Notification must be made within 72 hours of detection
- Data subjects must also be notified “without undue delay” where the breach poses a high risk to their rights
- Think about the steps that will need to be taken in those 72 hours – processes need to be in place already

pitmans law

Short-term actions

➔Carry out data mapping exercise

➔Contact service providers to request their standard contract updates – allow time in case terms need to be renegotiated

➔Formulate project plan to get you to 25th May 2018

pitmans law

Longer-term and ongoing actions

➔Policies, procedures, contracts

➔Record keeping

➔Customer communications

➔Ongoing training requirements

pitmans law

RISKS

Fines

- up to **EUR10m or 2% of total global annual turnover** (whichever is higher) for certain breaches;
- up to **EUR20m or up to 4% of the total global annual turnover** (whichever is higher) for more serious breaches e.g. processing without a lawful basis.
- ICO will take into account factors including:
  - Nature, gravity and duration of infringement;
  - Purpose of the processing;
  - Number of data subjects affected and level of damage;
  - Categories of personal data affected;
  - Intentional or negligent infringement;
  - Action taken to mitigate damage suffered by data subjects;
  - Manner in which data breach became known to the ICO.
- Percentage based fines relate to ‘undertakings’.

Criminal penalties

- Regulation allows Member States to lay down the rules on criminal penalties for infringements – Data Protection Bill contains criminal offences

pitmans law

Questions?

Thank you

Jonathan Gray – Partner Pitmans Law
jgray@pitmans.com
02380837785

Jonathan leads the hospitality team at Pitmans Law and provides a broad range of legal advice including data protection, employment, licensing and immigration. He has significant experience in providing corporate support work and advice on TUPE issues. He has an excellent reputation for advocacy at Employment Tribunals and Employment Appeal Tribunals and is also an employment law mediator as well as a regular speaker and trainer for clients and professional bodies.

pitmans law