Michelmores

The General Data Protection Regulation

Michelmores

GDPR: Scope and date in-force

The General Data Protection Regulation 2016: What is it?

- European legislation
- Directly applicable in all EU member states
- Largely replaces the Data Protection Act 1998
- Many new and enhanced obligations, with more severe consequences for breach
- Wider jurisdictional reach – businesses outside EU now caught

KEY DATE: 25 May 2018. PREPARE NOW!

Fines and powers

Tiered approach to fines:

- Max. of higher of 4% of annual worldwide turnover and €20,000,000 e.g. for breach of principles
- Max. of higher of 2% of annual worldwide turnover and €10,000,000 e.g. for breach of notification requirement
- Other investigatory powers and risk warnings
- Compensation to individuals
- Damage to reputation

But Brexit means it won't apply, right?

- Wrong.
- Article 50 was triggered in March
- Negotiations will continue for 2 years and in the meantime we will be required comply
- Even after Brexit, it is likely that we will need to comply with equivalent rules if we want to maintain trade with the EU

Michelmores

GDPR: Concepts and principles

What type of data is protected by GDPR?

‘personal data’

- information relating to an identified or identifiable natural person (‘data subject’);
- an identifiable natural person is one who can be identified, directly or indirectly, …
- …in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to factors specific to physical, physiological, genetic, mental, economic, cultural or social identity

‘Special categories of data’

- Racial or ethnic origin
- Political opinions
- Religious beliefs
- Trade union membership
- Physical or mental health
- Sexual life;
- Genetic and biometric data (such as fingerprints)

criminal offences are dealt with separately but under similar extra safeguards.

Controllers and Processors

- **Controller** – the entity who decides the purposes and means of processing (whether alone or jointly with others)
  - Bears the majority of the statutory obligations
- **Processor** – entity processing *on behalf of* a controller

The role of processors

KEY CHANGE: Processors have direct obligations under GDPR for the first time.

- Service sector cannot hide behind the fact that they are merely a processor in chain. Obligations include:
  - Maintaining written record of processing activities carried out on behalf of each controller
  - Where not in EU, appoint a representative in certain circumstances
  - Notify controller of data breaches without undue delay
  - Comply with rules on cross border transfers

Data protection principles

- Principles are broadly the same as under previous legislation, but enhanced.
  - lawfulness, fairness and transparency
  - purpose limitation
  - data minimisation
  - accuracy
  - storage limitation
  - integrity and confidentiality
- Accountability: the controller shall be responsible for, and be able to demonstrate compliance with the above principles.

KEY TIP: Audit your processing activities

Principle: Lawfulness, fairness, transparency

- Conditions to processing:
  - Consent
  - Necessary for performance of a contract with a data subject or to take steps preparatory to such a contract
  - Necessary for compliance with a legal obligation
  - Necessary to protect vital interests of a data subject / another person where data subject incapable of giving consent
  - Necessary for a task carried out in the public interest or official authority vested in the controller
  - Necessary for the purposes of legitimate interests

Principle: Lawfulness, fairness and transparency II (special categories)

- For special categories of personal data, narrower conditions apply, for example
  - Explicit consent
  - Necessary for carrying out obligations and exercising rights of controller or data subject in the field of employment and social security provided that it is authorised by laws or collective agreement which provide appropriate safeguards for the rights & interests of the data subject
  - Protection of vital interests of the data subject.

[Note: This is not an exhaustive list; but the most commonly relied upon conditions]

Lawfulness of processing: Consent

‘freely given, specific, informed and unambiguous’

- The conditions for obtaining consent have become far stricter:
  - The data subject must have the right to withdraw consent at any time;
  - There is a presumption that consent will not be valid unless separate consents are obtained for different processing activities - presumption that forced, ‘omnibus’ consent mechanisms will not be valid

Consent (cont.)

- **NOTE: draft ePrivacy Regulation –to govern emarketing and telemarketing, but has not been passed by European Parliament**
- **Soft opt-in**

KEY TIP: Review existing consent mechanisms to ensure they present a genuine and granular choice

The other principles

- Broadly consistent with current law:
  - **Purpose limitation:** Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.
  - **Data minimisation:** personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
  - **Accuracy:** personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

- **Storage limitation:** personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- **Integrity and confidentiality:** personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
- **Accountability:** the controller shall be responsible for, and be able to demonstrate compliance with the above principles. [NEW]

Note: transfers outside the EEA are dealt with separately.

Michelmores

GDPR: Rights of individuals & transparency

Transparency: fair processing notices

- Controllers must provide information notices to ensure transparency of processing
  - Identity & contact details.
  - Purposes and legal basis for processing.
  - Recipients (actual or categories).
  - Details of transfers outside EU, including how protected.
  - The retention period or the criteria used to set this.
  - Rights of individuals (access, portability, erasure, rectify etc.)
  - Complaints to supervisory authority.
  - Any contractual or statutory basis for collection of data.

KEY TIP: Audit notices/privacy policies and update them.

Transparency: fair processing notices (when?)

- Where controller is obtaining information from the individual: At time collected. Must also inform what consequences of not providing data are
- Other cases (must disclose sources at same time)
  - Within reasonable period from having obtained (one month max)
  - If data used to communicate (e.g. marketing), when first communicated
  - If disclosure to another recipient – at latest before disclosed
  - Carve out:
    - for disproportionate effort, provided individuals' interests are protected;
    - If processing required by law

Data subject’s rights

- Right of access.
- Right to rectification and right of erasure (plus obligation to notify each recipient to whom data has been disclosed, unless impossible or disproportionate).
- Right to restriction of processing.
- Right to be forgotten.
- Right to data portability.
- Right to object (in respect of processing for legitimate interests or tasks of in an official capacity in public interest).
- Right to object to decisions based on automated processing including profiling.

Data subject's rights: timescales and fees

- Timescale: one month from request (can be extended if complex).
- Fees: none (although can charge a reasonable fee for additional copies or if requests are unfounded).

Michelmores

GDPR: DPOs and Breach notification

Data Protection Officers (DPO)

- Mandatory for
  - public authorities
  - organisations whose *core activities* require:
    - "Regular and systematic monitoring" of data subjects on "a large scale"
    - "large scale" processing of special categories of data or criminal records
  - those obliged to do so by member state law
- "Core activities" – "inextricable part" of controller/processor's pursuit of its goals (not staff admin)
- "Regular and systematic" – all forms of tracking and profiling.
- "Large scale" – not yet clear, possibility of thresholds in guidance

Data Protection Officers (DPO)

- Must be selected by reference to professional qualities and expert knowledge – likely to be a limited pool at first
- Not personally liable
- Controllers/processors are *obliged* to support the DPO by providing resources
- Must be free to exercise role without instruction from controller/processor
- Reports to highest management level

Breach notification

1. Processors to notify controllers without undue delay
2. Controllers to notify supervisory authorities
3. Controller to communicate data breaches to data subjects
   - But no reporting to data subjects if (i) breach is unlikely to result in a risk to rights and freedoms of natural persons (ii) technical and organisational measures were in place (iii) disproportionate effort

   Also, both processors and controllers must maintain a register of breaches

Breach notification

Note max. fine for failure to notify is the greater of €10,000,000 or 2% worldwide turnover

KEY TIPS: Review internal processes, training and reporting mechanisms.

Controller's dealings with processors

- New rules requiring controllers to ensure that written contracts between controllers and processors include specific provisions covering:
  - Processing on controller instructions
  - Ensuring persons authorised to process commit to confidentiality
  - Security measures
  - Approval of controller for sub-processing
  - Assist controller in dealing with data subject's rights
  - Return of data on termination
  - Provide information regarding compliance with the above.

KEY TIP: Audit supplier contracts and ensure they contain the required terms.

International transfers

- The current prohibition on data transfers outside of the European Economic Area unless appropriate safeguards are in place remains
- Model Clauses
- Binding Corporate Rules
- New: codes of conduct and certification schemes
- What amounts to an “appropriate safeguard” has changed: businesses can no longer self-assess

KEY TIP: review any international data transfers where you have “self-assessed”

Michelmores

Any Questions?