GDPR

Overview- New rights and Obligations

FIDUCIA

What is the GDPR?

- New obligations on organisations and new rights to individuals
- Directly applicable in all EU states from 25 May 2018
- Will apply post-Brexit – applies to organisations outside the EU that offer goods and services to individuals in the EU
- New Data Protection Bill currently going through Parliament

FIDUCIA

Key Terms/Concepts

Data subject –the individual to whom the personal data relates.

Data controller –the person/ organisation who determines the purposes for which and the manner in which any personal data is to be processed.

Data processor –any person/ organisation (other than an employee of the data controller) who processes data on behalf of a data controller.

FIDUCIA

Personal Data?

Anything that can identify a living individual

Personal Data?

- Expression of opinion about the individual
- Any indication of the intentions of the data controller or any other person in respect of the individual
- Posts on social networking websites, and computer IP addresses, genetic data

FIDUCIA

Sensitive Personal Data

- Racial or ethnic origin
- Political opinions
- Religious beliefs or other beliefs of a similar nature
- Membership of a trade union
- Physical or mental health or condition
- Sexual life or sexual orientation
- Criminal record

FIDUCIA

Legal Basis

Six available:

- consent
- performance of a contract
- legal obligation
- vital interests
- public interest
- legitimate interest

FIDUCIA

Consent

Must be:

- Freely given
- Specific
- Informed and unambiguous
- Clear and affirmative action
- In plain language
- Not inferred from silence or pre-ticked boxes

FIDUCIA

Consent

- Unbundled – separate from other T&Cs
- Granular – separate consents must be given for different types of processing
- Named – name the organisation and any 3rdparties who will rely on the consent
  - no categories of 3rd parties

FIDUCIA

Consent

- Documented–keep records to show what the data subject has consented to, what they were told, how and when they consented

- Easy to withdraw –tell the data subject they have the right to withdraw consent and how they can do it

- Freely given –there must be no imbalance in the relationship between the data subject and the organisation

FIDUCIA

Performance of a contract

- you have a contract with the individual

- and you need to process their personal data to comply with your obligations under the contract.

It does not apply if you need to process one person's details - but the contract is with someone else.

FIDUCIA

Legitimate Interest

3 part test

- identify a legitimate interest;
- show that the processing is necessary to achieve it; and
- balance it against the individual's interests, rights and freedoms.

FIDUCIA

Legitimate Interest

The legitimate interests can be your own interests or the interests of third parties.

They can include:

- commercial interests,
- individual interests, or
- broader societal benefits.

FIDUCIA

Legitimate Interest

The processing must be necessary

- If you can reasonably achieve the same result in another less intrusive way, legitimate interests will not apply.

A balancing act

- If they would not reasonably expect the processing, or if it would cause unjustified harm, their interests are likely to override your legitimate interests.

FIDUCIA

Legal Obligation

Certain data/documentation must be held by law:

<u>Examples:</u>

- Proof of Right to work – up to 2 years after last engagement/employment

- Accounts/ VAT records – 6 years

FIDUCIA

Sensitive Personal Data

Explicit consent is the only legal basis!

FIDUCIA

Sensitive Personal Data

Explicit consent is the only legal basis!

FIDUCIA

Sensitive Personal Data

Explicit consent is the only legal basis!

FIDUCIA

Rights of Data Subjects

- Right to withdraw consent –no further processing of data.
- Right of rectification of inaccurate or incomplete data
- Right to erasure
- Right of data portability –i.e. to transfer personal data to another party
- Right to object
- Rights re automated decision making

FIDUCIA

Right to withdraw consent

- Only applies to personal data collected by consent.

- Must be as easy to withdraw consent as to give consent.

FIDUCIA

Right to erasure

Exists where:

- Personal data is no longer necessary for the purpose for which it was originally collected/processed
- Consent has been withdrawn
- No overriding legitimate interest in processing
- Personal data was unlawfully processed
- Legal obligation to erase

FIDUCIA

Right to data portability

Allows data subjects to obtain, reuse and transfer their data for their own purposes across different when:

- Data subject has provided their data to a controller
- The processing is based on consent/performance of a contract; and
- When processing is carried on by automated means.

FIDUCIA

Right to object

- A data subject has the right to object to their data being processed.

- The data controller should cease processing their data unless it has compelling legal grounds to continue that processing which overrides the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

FIDUCIA

Right to data portability

- Individuals have a right not to be subject to a decision based on automated processing

- Certain exceptions apply –including that, the individual has given explicit consent

FIDUCIA

Obligations

Central theme of the GDPR:

Data protection by **design and default**

FIDUCIA

Obligations – Accountability principle

- Demonstrate compliance with the GDPR
- Document processing activity
- Data protection officer?
- Privacy impact assessments
- Transparency -allow individuals to monitor processing
- Improving security features on an ongoing basis.

FIDUCIA

Obligations – Accountability principle

Records must be in writing and must include the following:

- the name and contact details of the data controller or data controller's representative;
- the purpose of the personal data processing;
- a description of the categories data subjects and personal data;
- the recipients to whom personal data has been or will be sent including to those internationally;
- any transfers of personal data internationally, including the identity of the third country or international organisation to which the data is transferred;
- the time limits placed on an individual's right to erasure; and
- a description of security measures that have been used to manage risks.

FIDUCIA

Data Protection Officer?

- Mandatory for public sector bodies.

- Also required when the core activities of the data controller:

- revolve around processing operations which require repeated and systematic monitoring of data subjects on a large scale; or

- processing special categories of data on a large scale.

FIDUCIA

Data Protection Officer?

- The DPO should have expert knowledge of data protection laws and practices.
- They must have sufficient time and resource to deal with data protection issues.

FIDUCIA

Data Protection Officer?

- Can be filled by an internal member of staff or an external person but they must be independent and able to report into the highest level of management.
- The DPO should not have a conflict of interests because of another internal role they have.
- The DPO should not be dismissed or penalised for performing their duties.
- The DPO will not be personally liable for an data breaches by the data controller.

FIDUCIA