GDPR
Facts and guidance sheet

What is it?

The General Data Protection Regulation is new law from the EU government. It came into practice in 2016, but it will be enforceable from 25th May 2018.

A few parts of how it is implemented can be decided by member states under a 'directive'. For this, the UK have the Data Protection Bill**,** which is going through parliament.

Who it applies to

The activities of an establishment processing personal data within the EU or processing personal data about a person (data subject) who resides in the EU.

What are the aims?

1. To enforce accountability
2. To update privacy laws in respect of the digital age
3. To unify how all EU residents can expect their data to be protected

Fines

The most serious infringements will be subject to fines capped at a maximum of €20million or 4% of total worldwide turnover, whichever is the highest.

6 Key principles

Article 5 requires that the controller shall be responsible for and able to demonstrate compliance with each of the principles as follows:

1. **Lawfulness*, fairness and transparency** – in relation to the data subject
2. **Purpose limitation** – collected for a specified, explicit and legitimate reason
3. **Data minimisation** – collect only what is necessary and relevant
4. **Accuracy** – take every step to ensure data is up to date (with regard to the purpose)
5. **Storage limitation** – kept in a way that identifies a person for no longer than is required
6. **Integrity and confidentiality** – ensure security using appropriate measures

What are the * lawful bases for processing data?

To obtain and process personal data lawfully, at least one of the following criteria **must** apply:

1. Consent
2. Contractual requirement
3. Legal obligation
4. Vital interests
5. Public interest
6. Legitimate interest

What is 'personal data'?

Article 4 defines it as: "any 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 one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

What is 'special category data'?

This is what we currently refer to as 'sensitive data' (but there are slight changes).

Article 9 defines it as: "data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation".

Processing this type of data is **prohibited** unless there is a legitimate requirement, or the data subject has given explicit consent.

Brexit

The UK's Data Protection Bill incorporates all the GDPR. This means that even after Britain leaves the EU, compliance will still be a legal requirement and the same level of fines and enforcement will apply. This has been confirmed by the ICO.

Regulation

There are a few ways in which the principles of the GDPR will be regulated:

- Trust marks
- Data seals

(Check for accreditation by the EU Data Protection Board.)

- ISO27001 – (A current information security standard.)
- Civil court rulings
- Criminal court rulings

HR Solutions' 5 steps for compliance:

1. **Audit** your personal data
2. Identify who is in the **key roles**
3. Implement **'privacy by default and design'** (you may be required to complete a **Data Protection Impact Assessment**).
4. Set up **records** of data processing if you employ 250 people or processing frequent, risky or involves special category data.
5. Be prepared to make a serious **breach notification within 72 hours.**

Key Roles

1. Data Controller
2. Data Processor
3. Data Protection Officer (DPO)*
4. Data Subjects
5. Third Parties
6. Recipients

* A DPO is only required if:

a) processing is carried out by a public authority or body

b) core business activities require regular and systematic monitoring of data subjects

c) core business activities require regular large-scale processing of special category data or data relating to criminal convictions

Data Protection Impact Assessment (DPIA)

This will be required for each process that uses personal data if any of the following conditions apply:

- The processing is likely to put the rights of a data subject at a high risk.
- An automated, systematic evaluation of data subjects takes place which may produce legal effects.
- Special category or criminal conviction data is processed on a large scale.
- There is systematic monitoring of a publicly accessible area on a large scale.

Data Protection Impact Assessment continued….

A DPIA must include the following steps:

Purpose: A clear statement of the purpose for collecting or processing the data

Legal basis: Identify the lawful basis that applies

Proportionate: Assess if the data is necessary to achieve the purpose.

Processes: A step by step account of processes (e.g. recruitment, new starter onboarding, leavers) must be set out

Risks: Identify risks to rights and of breaches

Measures: To minimise the risks and ensure compliance. These must be both technical and organisational. This must include security.

Views (Recommended): Solicit views of data subjects

If the criteria for a DPIA do not apply to an organisation, the steps above will still be a good guide to ensure that processes have been thought about thoroughly and adapted for GDPR compliance = privacy by design.

Record Keeping

Organisations must keep records if:

- They employ 250 people or more
- It is likely that the rights of data subjects could be at risk
- Processing of personal data is regular or frequent
- Special category data is processed
- Information relating to criminal convictions is processed

The GDPR does specify what constitutes adequate record keeping.

Breach Notification

All breaches must be documented in order to demonstrate compliance with Article 33 of the Regulation.

Organisations must report a **serious breach** to the relevant supervisory authority (SA) within 72 hours of awareness!

The GDPR does specify what must be included in the notification. There is currently no guide on how to notify an SA.

For organisations whose key business decisions are made in the UK, a breach must be reported to the Information Commissioner's Office (ICO). If key decisions are made in a different EU member state, the SA of that state must be notified instead.

What is a serious data breach?

A breach likely to result in a risk to the rights and freedoms of natural persons, particularly if the breach results in loss, damage or theft or gives rise to discrimination.

Subject Access Requests

0 Fee – 1 month latest!

It is no longer lawful to charge a fee for a reasonable request. It may be possible to charge a reasonable fee for a repeat request of the same information. complied with in 1 month.

It may be possible to refuse a request or charge a 'reasonable' fee, where requests from a data subject are "manifestly unfounded, excessive or repetitive." Article 12.