General Data Protection Regulation (GDPR)

What is the EU GDPR?

The EU General Data Protection Regulation has been in EU law since 25th May 2016 and applies to any EU member state or anyone processing personally identifiable data on EU citizens. Its purpose is to protect the rights and freedoms of EU citizens (known as the data subject) by governing how personally identifiable data relating to them is processed.

25 MAY 2018

The EU GDPR takes effect on 25th May 2018 and will replace the UK Data Protection Act.

The EU GDPR applies to EU member states or anyone processing personally identifiable data about EU citizens outside of the EU.

Ahhh but Brexit...?

The UK Data Protection Bill means that EU GDPR applies even after Brexit.

What happens if I don't comply with the EU GDPR?

Ultimately, amongst many new parts of this regulation is the setting out of administrative fines for data breaches imposed by our supervisory authority in the UK, the Information Commissioners Office (ICO).

The EU GDPR states that the imposition of administrative fines will in each case be effective, proportionate, and dissuasive.

The fines are up to

£17m

or 4% of global turnover

whichever is greater

Fines must take account of:

- the nature, gravity and duration of the infringement;
- the intentional or negligent character of the infringement;
- any action taken by the controller

Any mitigating factors will be taken into account so its time to get serious about information security!

What is personal data?

Personal data is any information about a natural living person (the data subject) that can directly or indirectly uniquely identify them. Examples include name, address, email address, telephone numbers, genetic data and so on….

What do I do if I have a data breach?

Firstly, you should have all of the necessary organisational and technical controls such as policies and procedures in place to prevent data breaches from occurring.

However…

If you do have a data breach, the breach must be reported to the Information Commissioners Office (ICO) without undue delay but within 72 hours of becoming aware of it.

What else is new over and above the Data Protection Act 1998?

Lots and lots……the EU GDPR really strengthens regulation around the consent of the data subject and lawfulness of processing of personal data. The responsibilities of the data controller and data processor are very clearly set out.

Consent to data processing by the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Most of all, the data controller is held ACCOUNTABLE.

Public bodies and those undertaking large scale data processing must appoint a Data Protection Officer (DPO) who has clear roles and responsibilities under the EU GDPR.

There are six principles of the GDPR to ensure that you are up to speed with. Personal data must be;

1. Processed lawfully, fairly and in a transparent manner
2. Collected for specified, explicit and legitimate purposes
3. Adequate, relevant and limited to what is necessary
4. Accurate, and where necessary kept up to date
5. Retained for only as long as is necessary
6. Processed in an appropriate manner to maintain security

Am I a data processor?

You are a data processor if you are performing any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Am I a data controller?

If you are determining the means and purpose of the data processing then you are a data controller.

Article 24 of the EU GDPR states the responsibilities of the data controller. The data controller must;

- Implement appropriate technical and organisational measures.
- Implement data protection policies.
- Adhere to codes of conduct to demonstrate compliance.

More advice on the EU GDPR can be found on the ICO website;

https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/

Kindertons are working hard to comply with the EU GDPR by 25th May 2018.

If you have any questions on Kindertons GDPR compliance project then please contact privacy@kindertons.co.uk

Plantec Assist · JigsawLaw · Kindertons accident management · jpmorriss · SOVEREIGN automotive