The General Data Protection Regulation

GDPR

The Data Protection Regulation is being replaced by the General Data Protection Regulation (GDPR) on 25th May 2018.

These notes have been prepared as a reminder of some of the key points of GDPR for your information.

Theses notes are for general information only and are not intended to be advice to any specific business. You are recommended to seek specialist advice before taking or refraining from taking any action on the basis of the contents of this publication.

GDPR

- Applies to any business dealing with the personal data of individuals residing in the EU, regardless of the business's location.
- Individuals can apply for compensation if businesses do not comply.
- The fines for non-compliance are punitive. Fines can be up to 4% of global turnover or €20 million.
- GDPR will continue to apply after Brexit
- ICO (Information Commissioners Office) continues to be the authority for dealing with GDPR compliance.

Individual's Rights under GDPR

GDPR applies to all personal information stored electronically or physically.

Under GDPR an individual has the right to:-

- be informed about the way their data is processed;
- request access to a copy of their personal data;
- object to their data being processed for some specific purposes;

- restrict a business from processing their personal data if it's inaccurate, or if the reason for processing it is contested;

- correct or erase mistakes in the personal data a business stores about them;

- make their personal data portable so that they can share the data with other data controllers;

- not to be subject to automated profiling and decision making;

If these rights are compromised an individual has the right to seek compensation.

Data Controller or Data Processor

GDPR distinguishes between two roles:

1. Data Controller: responsible for how and why personal data is processed.

2. Data Processor: acts on behalf of a Data Controller.

It is possible that some businesses will be both a data controller and a data processor of personal data.

Data controller and data processor: responsibilities

Data controller: - review points:-

- What data are you collecting? And is it relevant?

- How long do you store data?

- Data must only be stored while it is still required – have clear data retention policies in place.

- Notify individuals of your policies regarding the above points.

- Check your security procedures to ensure that only authorised personnel have access to data.

- Document your GDPR policies and practices.

Data controller: - review points:-

- Where is data stored? There are restrictions on storing and transferring data outside of the EU.

- Review your security procedures and practices. This applies to physical security and cyber security.

- Ensure that you are only using the data for the purpose that the data controller has authorised.

- Document your GDPR policies and practices.

Where to go for further information?

The first point of call for reference and continuing compliance should be:

Information Commissioner's Office (ICO)

https://ico.org.uk/

ICO 12 step action plan:

1. **Awareness**

You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have in respect of personal data.

2. **Information you hold**

You should document what personal data you hold, where it came from and with whom you share it. You may need to organise an information audit.

3. **Communicating privacy information**

You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.

4. **Individuals' rights**

You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.

5. Subject access requests

You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.

6. Lawful basis for processing personal data

You should identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it.

7. Consent

You should review how you seek, record and manage consent and whether you need to make any changes. Refresh existing consents now if they don't meet the GDPR standard.

8. Children

You should start thinking now about whether you need to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity.

9. Data breaches

You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.

10. Data Protection by Design and Data Protection Impact Assessments

You should familiarise yourself now with ICO's code of practice on Privacy Impact Assessments as well as the latest guidance from the Article 29 Working Party, and work out how and when to implement them in your organisation.

11. Data Protection Officers

You should designate someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements. You should consider whether you are required to formally designate a Data Protection Officer (DPO).

12. International

If your organisation operates in more than one EU member state (i.e. you carry out cross-border processing), you should determine your lead data protection supervisory authority. Article 29 Working Party guidelines will help you in respect of this.