EU General Data Protection Regulation (GDPR)

This is the most important change in data privacy regulations in over 20 years. It is coming into force on the 25th May 2018 and it will repeal the current legislation, Data Protection Acts 1988 & 2003.

GDRP will place very onerous accountability obligations on enterprises to demonstrate compliance. The Regulations primary objection is to give European Union citizens tighter control of their personal data. However, it also extends beyond the EU to all global organisations that process data of EU citizens.

All Business Owners, Sole Traders and Directors need to be aware of the new compliance issues being introduced because ultimately it is their responsibility to ensure compliance to this new Regulation. The issues that each organisation will face may be very varied however the one main fact is that every organisation should ensure compliance because the fines are significantly higher than under the current legislation.

GDPR is a very complex and therefore responsibility should be assigned to an individual in your business who can identify the main issues that will impact your organisation and understand them in detail.

Below are the main areas of change, outlined in very high-level terms:

- **Definition of personal data** – broader definition, under GDPR it "means ***any*** information relating to an identified or identifiable natural person".
- **Accountability** – data controllers need to be able to demonstrate compliance i.e. have a data protection infrastructure including Policies & Procedures etc.
- **Privacy and Cookie Statements** – additional information is required i.e. for privacy statement state any recipients of data, details of transfer of data to countries outside the EEA and the relevant safeguards in place, retention periods and the right to withdraw consent at any time; and cookie statement must state the actual cookies being used etc.
- **Consent** – needs to be freely given, specific, informed and unambiguous. It must take the form of an affirmative action or statement.
- **Data Protection Impact Assessments (DPIA)** – for any new technology or project being introduced, Organisation need to carry out a DPIA which will highlight the impact this new project/technology could have on the privacy of an individual. In some cases, organisations will need to refer the outcome to the Office of the Data Protection Commissioner (ODPC) for approval prior to implementing this new project.
- **Mandatory Data Protection Officers (DPO)** – organisations that have core activities in either processing large amounts of sensitive data or regular and systematic monitoring of data subjects on a large scale will need to hire a DPO. Public bodies will also need to hire a DPO.
- **Financial penalties** – easier for the ODPC to administer fines. Currently all fines need to be process through the court system, however, going forward there will be Administration

fines. The highest of which is 4% of the organisations global turnover for the preceding year or €20m whichever is the highest.

- **Access requests –** increased rights for Data Subjects i.e. right to portability, no fee for requesting an access request and shorter response time, now 1 month.
- **Breach notification –** now **all** breaches need to be notified to the ODPC within 72 hours unless the data was anonymised or encrypted.
- **Controller/Processor relationship** – must ensure a binding legal agreement is in place and clear instructions need to be provided to the Data Processor.
- **Data Processor** – direct compliance obligations will be placed on data processors, very different to the very light obligations under the current legislation.
- **Right to compensation and liability** – Data Subjects will be entitled to compensation for both material and non-material damage.
- **Transfer of Data outside the EEA** – this is a very complex area and one that should be reviewed in detail if your organisation carries this out.

In order to ensure compliance, your organisation needs to understand the current level of compliance within the business and know what compliance issues need to be addressed by 25th May 2018. This task needs to be carried out by management, delegated to an employee or outsourced. This is the first step in becoming compliant.

Once you are aware of the compliance issues, then systematically they will need to be addressed, so that by 25th May 2018 the organisation has all compliance issues under its control.

Awareness training is mandatory under GDPR and training records need to be retained. It is a fact that most data breaches are the result of human error, so training can benefit your organisation in the long run.

Some steps to take towards compliance:

- Ensure your website is compliant i.e. privacy and cookie statements and cookie banner.
- Become aware that the law is changing and begin to factor this into future planning.
- Understand the current level of compliance within your business.
- Address any gaps between current level of compliance and the compliance required under GDPR.
- Make a list of all personal data that you hold.
- Understand & document the legal basis for processing the personal data.
- Understand & ensure your organisation can comply with personal privacy rights i.e. data access requests etc.
- Implement breach notification procedures within your organisation.

This is a brief overview of the changes that organisations will be facing, however, if you would like to understand any of these issues in more details you can contact me directly.

Ruth Hallinan FCCA, CDPP, CDPO
Data Privacy Solutions
E: ruth@dpsolutions.ie
M: 087 2207471
W: www.dataprivacysolutions.ie