The General Data Protection Regulation (GDPR)

From 25 May 2018, the General Data Protection Regulation (GDPR) replaced the 1998 Data Protection Act and as such there some changes all UK companies and European companies will need to make. The focus is on data you process that is personal data.

According to GDPR…

'Personal data' means 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.

Why do we need it?

The EU Directive was drafted prior to the exponential growth of the Internet and is now not 'fit for purpose.' Personal Data is now being used in ways that were not envisaged at the time, E.g. mobile phones, online behavioural advertising, social media and more.

What are the main differences?

- Enhanced documentation to be kept by data controllers – You need to prove what you say you do, you do. This needs to be fully documented and includes all High-Risk data processing of data that includes Peoples personal information as outlined above.

- Enhanced Privacy Notices – You will need to review what and how you tell people about how their data is processed, stored, deleted.

- More prescriptive rules on what constitutes consent. Your company will need to review all marketing to ensure it fully complies else risk having marketing efforts restricted by ICO.

- Mandatory data breach notification requirement. 72 hours is the maximum time to inform ICO of any significant breach so Your company needs to consider it's breach plan in line with GDPR.

- Enhanced Data Subject Rights – 2 new rights and new rules about advising them. Also, some tighter restrictions around the time it takes you to provide that information. (now 1 month from 40 days.) There is no longer an applicable fee allowed also in normal request circumstances.

- New obligations on Data Processors. If you use 3rd parties to process data about staff or Your company clients, you will need to prepare for this. There is an impetus on you to gather some additional guarantees around how the data they process for you is processed. E.g. outsourced payroll, IT service provider, CRM system and more.

- Expanded territorial scope – You will need to understand just where in the world data is processed, think through third parties and who they use. This will include who your suppliers use (sub-processors)

- Appointment of Data Protection Officers. Certain organisations will need to appoint a data protection Officer (DPO) – It is considered you will NOT need a DPO.

- Significant increase in the size of fines and penalties. The fines are significant, but it is wrong to focus on the motive of GDPR adherence being fear led. The ICO are more likely to impose sanctions than fines for breaches.

Accountability – What is it and how do I comply?

The new accountability principle means that you must be able to show that you are complying with the principles. In essence, you cannot just state you are compliant; you have to prove it and provide evidence. To do this there are a number of actions you should take, such as documenting the decisions you take about your processing activities and various other ways that show compliance.

How do I show that I am processing personal data lawfully?

Under the GDPR, it is now necessary for you to explain the lawful basis for processing personal data. It needs to be fully aware of where data is, who has access to it, how it is used, how it is shared, how it is stored, how it is deleted and how it is documented and reviewed. It needs to be monitored, reviewed and assessed when necessary.

Your company can consider how best to do this but as a guide Your company ought to follow this suggested path.

The GAP Analysis – where are you against the current Data Protection Regulation and where do you need to be in order to meet compliance standards.

The DISCOVERY – Identify all data storage locations to include servers, PC's, cloud storage,

3rd party suppliers and others. Your company needs to demonstrate all data has been found

The MAP – Your company needs to understand the legal lawful basis for processing all personal data, in particular HIGH-Risk customer, supplier and staff data

The ASSESSMENT – Your company needs to consider how best to risk assess any HIGH-Risk data flows to see what can be mitigated, removed or changed.

DOCUMENTATION – Your company needs to review current documentation and implement missing documentation identified during the GAP, MAP and DISCOVERY phase

Training – Your company needs to decide on a training plan to ensure staff and where appropriate, customers. For example, work needs to be done to ensure these have access to the data you process about them and how you make it available to them, upon request, at no costs as part of Your company's compliance.