First Steps for **GDPR** Compliance

1 AWARENESS

You should make sure that decision makers and key people in your organization are aware that the law is changing to the GDPR. They need to understand the impact this is likely to have across the organization. Part of this compliance audit, no matter the size of the company, is hiring a Data Protection Officer (DPO) to explain the regulations and apply them to the business.

2 KEEP A RECORD

Once businesses have a clearer idea of their readiness to meet the regulatory requirements, they need to keep a record of the process. This should be done through the keeping of a Data Register – essentially a GDPR diary. Each country has a Data Protection Association (DPA), who will be responsible for enforcing GDPR. It is this organisation that will judge whether a business has been compliant when determining any potential penalties for being breached. Should a breach occur during the early stage of implementation, the business should be able to show the DPA its progress towards compliance through its Data Register.

3 CLASSIFY YOUR DATA

You should document what personal data you hold, where it came from and who you share it with. Auditing your current methods is one of the best ways in which to prepare for GDPR. They can then determine which data is more vital to protect, based on its classification. This also means knowing who is responsible for controlling and processing the data, and making sure all the correct contracts are in place.

4 REVIEW 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. You should review how you are seeking, obtaining and recording consent and whether you need to make any changes. You should start thinking now about putting systems in place to verify individuals' ages and if needed, to gather parental or guardian consent for the data processing activity.

5 PIA & DPIA

Businesses should complete a Privacy Impact Assessment (PIA) and Data Protection Impact Assessment (DPIA) of all security policies, evaluating data life cycles from origination to destruction points.

6 CONTINGENCY PLANNING

In cases where a leak of sensitive information occurs, the EU GDPR contains a new requirement that private and public enterprises must inform the relevant authorities. Develop an incident response process for communication with both the local data protection authority and with the public so that you can control what information gets distributed once you have breached. Having a strong data governance process and full insight into your data will help you be precise in the communication.

Disclaimer: This blog is not legal advice and should be considered educational in nature. You may implement this advice at your own risk.

Sources for Research:

www.collibra.com
www.information-age.com
www.scmagazineuk.com
www.gdprcoalition.ie