Extract from CIPD website (June 2017)

According to Ireland's Data Protection Commissioner, just 14% of SMEs have begun getting ready with less than 12 months to go. The Commissioner has launched an awareness raising campaign and website to help inform individuals of their rights and organisations of their responsibilities. Over two thirds of SMEs have heard about the GDPR but 70% admitted to being unaware it will be effective from 25 May 2018.

The Commissioner has produced a 12-step guide to getting ready for the GDPR, as well as a video and other materials. Below we list the process the Commissioner identified. This summary is purely for guidance, and does not constitute legal advice or legal analysis.

What can you do now to prepare for the GDPR?

Becoming aware

Review and enhance your organisations' risk management process and identify problem areas now.

Becoming accountable

Make an inventory of all personal and sensitive data you hold and examine Why are you holding it; How did you obtain it; How long will you retain it; How secure is it; and Do you ever share it with third parties, and if so, on what legal basis?

Communicating with staff and service users

Review all current data privacy notices and policies, and make sure you keep staff and service users informed about how you use their data.

Personal privacy rights

Review your policy and your procedures to ensure they cover all the rights employees have, including how you keep data current, can delete personal data or provide data in a commonly used format when requested.

How will access requests change?

Review and update your procedures and plan how you will handle Access Requests which must, at the latest, be concluded within one month. Ensure you comprehensively map all the locations where personal data, manual and electronic, could be held.

What we mean when we talk about a 'Legal basis'

You should look at the various types of data processing you carry out, identify your legal basis for carrying it out and document it. This is particularly important where consent is relied upon as the sole legal basis for processing data, as would be common for employee data. Under the GDPR,

individuals will have a stronger right to have their data deleted where ‘customer consent’ is the only justification for processing.

Using customer consent as grounds to process data

Review how you seek, obtain and record customer /employee consent to process data, and whether you need to make any changes. Consent must be ‘freely given, specific, informed and unambiguous.’ Do your current employment contracts cover this and what additional consents do you need?

Processing children’s data

If the work of your organisation involves the processing of data from underage subjects, you must ensure that you have adequate systems in place to verify individual ages and gather consent from guardians.

Reporting data breaches

There will be mandatory reporting of all data protection breaches. Review and make sure you have the right procedures in place to detect, report and investigate a personal data breach. This carries a reputational risk as well as the risk of significant fines.

Data protection impact assessments (DPIA)

Data privacy needs to be at the heart of all future projects and data analysis. A DP Impact Assessment systematically considers the potential impact that an initiative might have on the privacy of individuals and mitigates any risks.

Data Protection Officers

The GDPR will require certain organisations to designate a Data Protection Officer. Identify your organisation’s obligations, dependent on your status and what information you systematically monitor and process.

International organisations and the GDPR

The GDPR includes a ‘one-stop-shop’ provision which will assist those organisations which operate in many EU member states. Identify where your main establishment is based in the EU in order to identify your Lead Supervisory Authority (LSA) as your regulating body. While the UK will be covered by the GDP Regulations from May 2018 to Mar 2019, their future status after Brexit is unclear.

Under the Regulations, all organisations that process data need to be aware that the General Data Protection Regulation will apply directly to them from 25 May 2018 and they are responsible to comply with its provisions. So find out more and audit your practices to ensure you are able to comply.