GDPR

Obligate

• **Who is responsible for Data Protection in your organisation?**
Having someone in your organisation who is responsible and accountable is a good place to start on your journey to compliance. Data protection is an ongoing development and shouldn't be taken lightly.

• **They must have the authority to implement necessary amendments.**
The new legislation should not cause too much disharmony within your organisation if you have complied with the Data Protection Act 1998, however there will be some changes required for the GDPR. Ensuring your member of staff responsible for implementing the GDPR has a level of authority will make the transition significantly smoother and efficient.

Identify

• **What personal data do you hold?**
Establishing what data you hold is a starting point for compliance. Identifying the type of data you hold (Name, email, payment details for example) will help you strategically further down the line. Is it customers, prospects and what about employee data?

• **Where did it come from?**
Understanding where the data came from will assist in deciding whether that data is necessary to hold or not. This information may be requested on a subject access request.

• **How long has it been stored?**
Personal data can only be held for the relevant time required. Holding excessive data for an unreasonable period is poor practice in data protection.

• **Sensitive personal data?**
Processing information on sensitive data such as racial origins, political views, religious beliefs, genetic data, data on children etc falls under a separate article (9) of the GDPR. There are stricter rulings on sensitive data, so if that is something you hold, it is important to follow the relevant rules.

Determine

• Purge any data not necessary and finalise what data you require and establish why you need it.
Once you have determined what is and is not relevant in your databases, simply remove any of the data which is surplus to requirements. Make sure the data you do keep is relevant and specific to your organisational needs.

Strategy

• **Implement internal procedures.**
What happens if there is a subject access request? Or a request to erase someone's data? Or what needs to be done if there is a data breach? Planning for the outcomes will help you when the incidents happen for real.

• **Are there any changes required? New processors/suppliers?**
Review your suppliers and processors. In some cases, both the controller and processors will be responsible and liable for any damages caused so making sure your partners are compliant is important.

Sustain

• **Evolutionary not revolutionary.**

The ICO describes the transaction between the Data Protection Act 1998 and the GDPR as evolutionary not revolutionary. The world will not stop turning on the 25th of May 2018 and neither will data protection. The deadline is the 25th of May, but more work is needed post GDPR-Day.

Sustaining good practice and principles is paramount and most importantly, always put the fundamental rights and freedoms of the individuals at the forefront of any decision you make.

Educate

• **Understanding the GDPR**
The GDPR has 11 chapters containing 99 individual articles and 173 recitals. Some articles will be more relevant than others depending on your organisational type. Having a basic understanding of the GDPR will be fundamental to compliance.

• **The Principles of the GDPR**
6 principles are outlined within the GDPR under Article 5. Following these principles throughout any data processing is essential.

• **Rights of Individuals**
The GDPR focuses on the fundamental rights and freedoms of individuals throughout. Knowing these 8 core rights is paramount.

• **Legal Ground of Processing**
There are 6 legal grounds for processing personal data. You need to identify which ground is best suited to the rights and freedoms of the individuals in question. Focus on the implementation of that ground in a fair and transparent way.

• **PECR (Privacy and Electronic Communication Regulation)**
PECR is the legislation regarding any marketing communication conducted via an electronic channel. For example, this could be email, telephone, fax, sms and cookies. Often forgotten about with GDPR, PECR is still something you need to abide by

Inspect

• **How was the data collected?**
How the data was collected is important to understanding whether you can or cannot market to the individual. Although the Data Protection Act 1998 and PECR have been in place for many years, the GDPR requires higher accountability when challenging compliance. Knowing how the data was collected is a key part to your accountability.

• **What are you using the data for?**
One of the principles GDPR outlines when processing personal data is data minimisation. Only holding and processing data which is required for the purpose is necessary. If there is no need to hold certain data, then it should be removed.

• **How long do you plan on processing the data?**
As with how long the data can be stored, personal data can only be processed for the relevant time required. Once that period expires, the data should be removed.

• **Is it fair to use?**
The GDPR holds clear views on what can and cannot be done with data. The question of 'is it fair to use?' should be asked every time you process data.

Gauge

• **Where is the data stored?**
What storage implementations do you have in place for any personal data held? Is it hard copies in a file, saved in your laptop or stored via a third party security system? Identifying and establishing whether the storage is secure enough is very important to prevent data breaches. Any sensitive data will have to be extremely secure.

• **Who processes the data?**
Only the members of staff responsible for the processing/controlling of the data in some form should have access to the data sets. Anyone who is not relevant should be prevented from access to personal data, especially if it is sensitive.

Archive

• **Document what you have done and are doing.**
Article 5(2) of the GDPR outlines the accountability required to comply with the GDPR. Privacy Impact assessments, procedure documentation, privacy policies, terms and conditions are just some good documentations to have updated in line with the GDPR. You are guilty until proven innocent under the GDPR.

insightdata
business is better with insight