With the General Data Protection Regulation (GDPR) coming into effect on 25 May 2018, companies must start pushing through necessary changes early to achieve compliance in time for its arrival, according to Paula Tighe, Information Governance Director at leading law firm Wright Hassall.

Start your plan of action to achieve GDPR compliance

Words by Paula Tighe, Information Governance Director, Wright Hassall

It's crucial that companies understand how much work is involved during the preparation stages of GDPR. The basic principles for every business will be the same and it starts with a comprehensive plan agreed between the people who will need to drive through the changes.

Remember, GDPR applies to all organisations who obtain, process and use data within the EU — the UK's decision to leave the EU has no bearing on the new ruling.

Raise awareness and register it

First, ensure all decision makers in your organisation understand that changes and that non-compliance is serious. Start recording the process of meeting the regulatory requirements; this will help mitigate any risk of incurring penalties for non-compliance.

Known as the 'Data Register', this record will show what data your company currently holds and your reasons for processing it, helping you comply with the new accountability principles of GDPR.

Rather than stopping you from doing things, GDPR is about improving standards by encouraging organisations to make existing procedures more efficient.

Review your existing digital and hard copy format privacy notices and policies; are they concise, written in clear language, easy to understand and easily found?

Finally, ensure this key information is clearly communicated to your data subjects, detailing how individuals can complain to the Information Commissioner's Office if they think you're doing something wrong.

Rights of the individual

Individuals will have more control over their personal data under the GDPR. Check your procedures and amend if necessary, detailing the format in which you will provide data, how you would delete it and how you will correct mistakes.

Individuals also have the right to have their information erased and the right to be forgotten. You must be able to prove that you have a process in place to comply with such a request.

Perhaps one of the key drivers for the changes, is the right for an individual to prevent their data being used for direct marketing purposes, as is the right to challenge and prevent automated decision-making and profiling.

Having transparent procedures in place will go a long way towards heading off any future problems with the regulator, regardless of complaints or investigations. Remember, if your organisation handles personal data correctly under the current Data Protection Act, the switch to the GDPR should pose no real issues.

Prepare for personal requests

If an individual submits a subject access request, to see what information you hold on them, you cannot charge them and you must comply within a month. You can refuse to comply if you think the request has no merit — but you must tell them why and how they can complain to the regulator.

For SMEs, it will be more important to show a willingness to comply by trying to implement all the necessary steps and creating a data register, than to be fully compliant in May 2018.

Never assume you have consent

One of the trickier areas of the new regulations is handling consent for personal data to be captured and used for more than just contact.

Individuals must give clear consent for their data to be used, but must be allowed to revoke consent easily, at any time. If you change the way you want to use their data, you must obtain a new consent.

Keep reviewing and keep recording

Where data processing could pose a significant risk to individuals because of the technology being used, or the scale of the processing, you should undertake a Privacy Impact Assessment (PIA) before beginning the project.

These assessments will help you and the regulator decide the likely effects on the individual if their data is lost or stolen and should form part of your ongoing processes.

Make someone responsible and keep it up

If you routinely monitor or process personal data on a large scale, you should appoint a data protection officer who understands the regulations and how best to drive your data privacy processes.

It's not just electronically-held data that can pose a problem; you also need to consider written records, which are also covered by the regulations — ensure all your staff are trained on the correct handling of personal data.

Record how you handle each step of the process in your Data Register. In the event of a complaint or a data breach, it will be those organisations unable to demonstrate what they did to assess risk and mitigate it that will suffer.

Organisations that can prove they have made an effort to comply, even if they are not fully compliant with every aspect of the GDPR from the word go, will do better. ■

For further information, visit ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

Paula Tighe is a qualified data protection professional.