Time to Act: 10 Steps to GDPR compliance

On 25th May 2018 the EU General Data Protection Regulation (GDPR) will come into force. GDPR will replace the UK's existing Data Protection Act, first drawn up in 1984, and is set to be the largest piece of data regulation the European Union has ever passed.

GDPR is a critical issue for businesses of all sizes as it will significantly affect how they gather, store and manage their data. If you are an organisation that wants to collect data from EU citizens for business or research purposes, then GDPR applies to you.

This checklist highlights 10 steps you can take now to ensure that your organisation is prepared to demonstrate GDPR compliance:

1 Raising awareness in your organisation

The first step involves making sure that the key decision makers and other relevant people within your organisation are aware of the changes that GDPR will make to the current law. They need to be aware of the impact GDPR will have and understand what is required to be compliant under GDPR.

2 Assessing the data your business holds

The next stage is assessing the information you hold. Organising an information audit will help you understand your data and how it should be processed. Start by documenting what personal data you hold, where it came from and how you use it. Doing so will also ensure that you comply with the GDPR accountability principle, under which organisations must show how they comply with the data protection principles.

3 Reviewing your privacy notices

At present, when you collect personal data you are required to provide accessible information to individuals about your identity and how you intend to use their information. The most common way to provide this information is through a privacy notice.

Under GDPR there will be some additional information you need to share. You will need to explain your lawful basis for processing the data, your data retention periods and also make it clear that individuals have a right to complain to the ICO if they believe that their data is being handled incorrectly. You should prepare by reviewing your current privacy notices and make any necessary changes in good time.

4 Protecting the rights of individuals

As part of GDPR it is your duty to ensure that your procedures cover and protect all the rights of individuals. They have the right to know how you will provide data and how you will delete personal data.

The rights of individuals under GDPR include:

- The right to be informed
- The right of access
- The right to erasure
- The right to object
- The right to restrict processing

If you ensure that your organisation is prepared to give individuals their rights now, then this will make your transition to being GDPR compliant much easier. How would your organisation react if someone asked to have their personal data deleted? Start by checking your current procedures and create a strategy for how you would respond and whether you need to

5 Update your procedures

You will be required to update your procedures and establish a plan that outlines how you will handle subject access requests. Your plan must abide by the following rules:

- In most cases you will not be able to charge for complying with a request.
- You will have a month to comply with requests, instead of the current 40 days.
- You can refuse or charge for requests that you deem to be manifestly unfounded or unnecessary.
- If you do refuse a request, you must inform the individual of the reason why and notify them of their right to complain to the supervisory authority and to a judicial remedy.
-

If your organisation handles a large number of access requests, you should ask yourself whether it would be practical to develop a system that allows individuals to access their information easily online instead. Or you may need to have a contractual agreement in place with your service provider who processes your data, to action these requests within the specified time.

Time to Act: 10 Steps to GDPR compliance

6 Lawful basis for processing personal data

Under the GDPR, organisation's lawful basis for processing personal data will be different to the current law which doesn't have any practical implications. Organisations will be required to explain their lawful basis for processing personal data in your privacy notice and when answering an access request. You are also required to document your lawful bases in order to help you comply with the GDPR's 'accountability' requirements.

7 Consent

The GDPR requires you to obtain consent and a positive opt-in for data processing. Consent must be freely given, specific, informed and unambiguous. Consent guidelines should be separated from additional terms and conditions and include clear instructions on how to withdraw consent. In order to prepare your organisation, you should review how you acquire and manage consent and refresh your consent mechanisms if they do not meet the GDPR standard.

The GDPR also introduces restrictions on the ability of children to consent to data processing. It states that if the child is under the age of 16 then you will need to obtain consent to process the child's data from a parent or guardian. You should also ensure that your policy notice is written in clear language that will be understandable to children.

8 Data breaches and data protection

You are responsible for making sure that your organisation has the correct procedures in place to detect report and investigate a personal data breach. Should your organisation suffer a personal data breach, you may be required to notify the ICO or another body. Under the GDPR, it is the duty of all organisations to report certain types of data breach to ICO and in some cases to the affected individuals. This applies when a breach is likely to result in risk to the rights and freedoms of individuals. Failure to report a breach when necessary could result in a fine.

Again you'll need to make sure you have an agreement in place with your service provider that any data breach incidents are reported to you (so you can inform your clients) and the ICO promptly.

PretaGov

Delivering Digital Transformations

9 Data protection officers

A data protection officer is the person who takes responsibility for an organisation's data protection compliance. If you organisation falls under the below categories, you will be required to appoint a data protection officer under GDPR:

- A public authority
- An organisation that carries out regular systematic monitoring of individuals.
- Or an organisation that carries out large scale processing of special categories such as health records or information about criminal convictions.

10 International Business

If your business operates in more than one EU member state then you will be required to determine and document your lead data protection supervisory authority. The lead authority is the supervisory authority in the location where your central administration in the EU is. However, this is only applicable where you carry out cross-border processing.

With the deadline fast approaching, follow these 10 simple steps and your organisation will be GDPR ready in no time.

At PretaGov we understand the importance of being GDPR-compliant, so we're here to help you make sure your business is fully prepared. There is no one quick silver bullet to ensure total compliance.

But it's imperative to get started now to ensure you're compliant by the GDPR enactment date of **25 May 2018**.

PretaGov can assist with GDPR compliance, for more information please get in touch on 0208 819 3887.