

GDPR

Are you ready?

August 2017

After four years of wrangling, the EU's [General Data Protection Regulations](#) come into effect from 28 May 2018. That gives everyone affected less than a year to make sure they are ready for the changes, and that they comply to the letter of the law.

Currently, the UK has the [Data Protection Act 1998](#) in force. This, however, will be superseded by the new regulations, with bigger fines for non-compliance, and giving people greater say over what information is retained by companies, and what they do with that data. It's also designed to unify data protection regulations across the EU.

But aren't we leaving the EU?

We are, but because the GDPR comes into force before we shut the door and give the keys back, they will still apply even after we've left. That means you are going to have to comply, whether you're a Remainer or a Brexiteer.

So what do I have to do?

Firstly, make sure everyone in your organisation is aware of the changes, especially key decision makers and those who are directly responsible for the collation and management of data.

Make sure you have a record of the kind of data you hold, where you got that data from, and who you share it with. That may mean an information 'audit' that also checks on your processing activities and how you log the use of data stored. If you have inaccurate data that has been shared with other organisations, then you will need to tell them about the inaccuracies so that data can be corrected downstream as well as within your own organisation.

You will need to review your privacy notices and plan any changes that may need to be added. Under the new regulations, you must:

- tell people who you are and how you intend to use their data;
- demonstrate that you have a lawful basis for processing their data;
- explain how long you will hold that information; and
- inform individuals that they can complain to the ICO if they are unhappy at the way you are handling their data. Check the ICO's [Privacy notices code of practice](#) for more information.

Individuals' rights

Most importantly, you need to make sure that your procedures ensure the rights of individuals whose data you hold. The new GDPR means that individuals have:

- the right to be informed what data is being held about them;
- the right to access that information;
- the right to ensure any mistakes are rectified and corrected;
- the right to have information that is not relevant erased;
- the right to restrict the way the data is processed;
- the right to object to having their data held; and
- the right not to be subject to automated decision-making, including profiling.

An additional right is the right to [data portability](#), which only applies to personal data provided by an individual, where processing is based on the individual's consent for the performance of a contract, and when processing is carried out by automated methods.

These procedures are key to compliance to the new regulations, so it's vital that you check you're up to date before 28 May 2018.

Access to data

One of the most important changes is in the procedure is to allow access to data. Compliance is now restricted to a month, rather than 40 days, and you cannot charge (in most cases) for complying with a request. If you refuse a request for data access, then you must provide a valid reason as to why.

You will also need to identify the lawful basis for your data processing activity, and update your [privacy notice](#) to make sure it is clearly explained.

Protection for children

For the first time, the new GDPR rules include special protection of children's personal data, particularly for social networking. If data is to be collected on children under the age of 16 then parental or guardian consent must be sought first.

Data breaches – what to do if your data is hacked

Hacking is a huge issue, and personal data protection is key. Some organisations are already required to notify the ICO and other bodies (such as the Police) if there is a data breach. The new legislation introduces a duty of care on all organisations and even individuals to [report data breaches to the ICO](#) if there is a possibility it could result in personal information leading to financial or personal damage, discrimination, or damage to reputation. It's time for all companies to take cyber security seriously, especially when it comes to personal details of customers, clients, or even patients.

If you're unsure as to how the new regulations may affect your business, talk to an expert. They will be able to review your current policies and procedures, and recommend where you can make changes to ensure you comply with the new regulations. Remember, you only have until the 28 May 2018 to get ready for GDPR, so it's important to act now.

Veronica Hartley
020 7299 6922
veronica.hartley@riaabg.com
www.riaabarkergillette.com



Note: This is not legal advice; it is intended to provide information of general interest about current legal issues.

