# The General Data Protection Regulation – five steps to compliance

by Andrew Humphrey


**If a client asks how you're complying with GDPR, how can you respond?**

The General Data Protection Regulation ('GDPR') is a piece of European Union law that will be enforceable from 25 May 2018. It will replace the current data protection regime set out by the Data Protection Act 1998, and brings in new rights – but also new responsibilities. What are the risks of not complying with the new rules? Fines of up to 2% - 4% of global turnover from the Information Commissioner's Office ('ICO').

If a client asks you about how you're complying, there are a few easy steps you can take.

**1. Show your commitment to getting it right.**

The first step that you can take is to commit to following the new rules. The Regulation itself is a heavy read, but there are plenty of resources online that can give you a rough idea of what to expect. Some of the key changes are in relation to the rights of data subjects (you and I), and in how you can obtain and process people's personal (and sensitive) data. The legal justifications for doing so have been amended, and you can't assume consent any more.

Recording your organisation's decision to get its GDPR obligations right is the first step. If you're a limited company, then you can use board minutes for this.

**2. Taking stock of where you are.**

You can also conduct a data protection impact assessment, to work out how you're doing against current standards and the new GDPR standards. You could do this internally or ask someone to come in to help you with it. Some example issues to watch out for are:

- Retaining data – how many times have you discovered old files on your computer? Does your system enable you to provide full access to the data you hold on an individual? Does your system enable you to delete all data you hold on an individual? Consider using encrypted or password protected emails for the exchange of sensitive data.
- Presumptuous consents – do you assume that the data subject consents, by using pre-ticked form boxes? If you don't have consent, do you have a justification for holding the data?
- Your website – is the public face of your business and is one way you receive personal data. Are the website cookies compliant? What about analytics providers?
- Conducting a data protection impact assessment sounds like a big task, but if it's done properly it should only take a day or so. It shows your clients that you're taking the GDPR (and them) seriously, and it has commercial benefits too. You might discover inefficiencies and overlaps in the data flows inside your organisation, or gaps where there should be some control of information.

**3. Making changes if needed.**

In conjunction with your solicitors and IT department, you can use the results of the assessment to guide any changes that you need to make. One easy solution is to amend your terms and conditions to cover GDPR, so that you can show clients you are complying because you've contracted with them on that basis. This is essential because the GDPR imposes an obligation on you to check that your clients comply, and on your clients to check that you comply. They should want to see this. You should also review your current contracts to check whether they're still compliant.

On the IT side, you should check with your supplier on your current arrangements. Do they provide the necessary systems to build in privacy by design? The GDPR's IT impact is much deeper than simply having strong external security.

**4. Preparing for things if they go wrong.**

As a client, the only thing worse than your data being breached is finding out the data holder doesn't have a plan for how to respond.

Breaches do happen – Uber lost 57 million users' data in the United States. If it happens to you, then having a solid strategy on how to respond is essential. This is especially important because you'll have 72 hours from discovering the breach to decide:

- Whether to inform the ICO; and
- Whether to inform the data subject.

You'll need an incident plan, and template letters to send to both the ICO and clients. You'll also need to incorporate PR into the response plan. This will give clients the comfort of knowing you've thought about contingencies.

**5. Developing your team.**

You may need to appoint a Data Protection Officer, otherwise a suitable person with overall responsibility for all data issues. However, if they're off or out of the office, then all of your team should know how to react to breaches; and what the business' key obligations are under the GDPR. This means implementing a training scheme for the team, and regular updates to check for understanding.

Some, all, or even one of the above will help show your clients that you are reacting to the new legislation. They demonstrate that you are taking the GDPR seriously and that you are thinking about not just your business, but them – they are obliged to check that you are complying, just as you are with them.

Andrew Humphrey is a senior associate at Bishop & Sewell LLP, and leads the Employment and Business Regulations team. Andrew's practice has a strong tech focus – he has advised app developers, e-advertising agencies and social media start-ups on how to navigate current data legislation, and the new GDPR. He is also the director of his own tech company, and uses this experience to understand the competing interests of compliance and effectiveness. Andrew writes on data protection issues and the changes that regulated industries need to make to adapt to the new data landscape.

For further information on this topic, please contact Andrew Humphrey at ahumphrey@bishopandsewell.co.uk or your usual Gerald Edelman contact.