Is Your HR Department GDPR Compliant?

If you're anything like me, you'll have spent most of May receiving hourly emails telling you that a company values your privacy and so won't email you again unless you specifically opt in to receive their emails. It gave me a slight warm glow to think that after 25 May, I'd not be inundated with weekly emails from a company I once bought a pair of shoes from in 2004. And it's all to do with GDPR.

The General Data Protection Regulation (GDPR) is designed to protect the personal data of individuals. It imposes strict rules on how personal data is handled and secured, and provides people with rights that will keep them in control of their data.

What are the obligations for HR?

In the simplest terms, HR need to know what data they hold, where they hold it and why they hold it.

What?

Conducting an audit is the best way to capture the information; start by asking the team what information is held and inputting this into a 'data register'. The data register should include the legal basis for processing data; and you have to determine which basis fits which data process. In most cases in HR, if your systems and policies are well written and you have a tight approach to data control, the viable basis will be 'legitimate interest'. It's a legitimate interest to hold the data you need to employ and pay someone (name, address, NI number, bank details etc.), and it's a legitimate interest to track absence data in order to administer your sick pay or absence policy.

Where?

If your teams are anything like ones I've worked in, HR people have a tendency to download data from the central database and store it on their own drives in Excel spreadsheets, whether to make their own reports or to monitor their client database. It's these 'hidden' data processes that need to be brought to light, and action taken to remove and delete. Most HR departments will have a personnel system which holds all HR data and the likely question to the software provider is: "Is the software GDPR compliant?". Generally, the answer to this question is that a software product on its own is not likely to be either GDPR compliant or non-compliant; it is a business that is compliant (or not), and in relation to software compliance depends on how a system is used, and with what personal data.

So, for example, you might be entirely comfortable that all data is held securely on your personnel system, but if you have a post-it note with your password stuck to your computer screen, you've failed. Similarly, if you religiously take photocopies of passports with the 'right to work' as per our legal obligations, but keep these in an unlocked filing cabinet, you've failed.

> The General Data Protection Regulation (GDPR) is designed to protect the personal data of individuals

Why?

Is all of the information requested (and held) strictly relevant? Yes, I need to know a new starter's name, address, NI number and right to work in the UK. Do I need to know their marital status, or how many kids they have? Probably not. Application forms can ask for a lot of information which is hard to justify under the new regulations; and is irrelevant anyway. It's a good opportunity to look at what documents you ask applicants or new starters to complete, and ask yourself exactly what information is required, and why it is necessary to hold. Minimise the data you hold wherever possible so you're only keeping data which is necessary to effectively run your HR department. Finally, you'll need to make someone responsible for ensuring that the data is protected, which is often the HRM or HRD.

Third Parties

There are generally a lot of third parties with whom you'll share information; payroll, pension providers, training companies, benefit providers, insurance companies... the list will go on. Make sure you capture which information is being passed to whom, and why. Check it's being sent in the correct format, so encrypted and secure.

Telling Employees

Providing each employee with a clearly written statement telling that what data is held, why it is held and their rights is an important part of GDPR. It should also include the legal basis for processing the data, the retention periods for the data, and the way to complain to the ICO. It's a fairly lengthy document and can look intimidating, so I've taken the approach of explaining what the Privacy Notice is in simple terms as a cover email. I've explained why we hold the data (to pay you!), or for legal obligations (demonstrate your right to work in the UK) or for regulatory reasons (ensure you have a clean criminal record).

How does an HR Department get GDPR ready?

Audit, audit, audit. Check what data you hold, check you can justify the reasons for holding and processing the data, check who has access and why, check how long the data is kept, check that people know their rights under GDPR including rights to complain to the ICO...

... and let's enjoy our slimmed down email inboxes, and watch to see how the law develops, in the UK and abroad.

VICKI FIELD
HR Director of London Doctors Clinic, a private London GP clinic.