Citation

Is your business GDPR ready?

From 25 May 2018 onwards, all businesses that handle personal data must comply with the new General Data Protection Regulation (GDPR) legislation. With hefty fines on the table, this isn't something you'll want to put on the backburner.

If you're sick of sifting through legislation jargon and just want to know if and how this will affect your business, then you're in luck, because we're here to simplify GDPR.

What is GDPR?

The GDPR is a regulation designed to strengthen and unite the data protection process for all individuals within the EU.

Who does the GDPR apply to?

1. It applies to both 'controllers' and 'processors'. Controllers are the organisations and bodies who stipulate how and why personal data is processed, and processors are those that act on the controller's behalf.

2. It applies to businesses operating within the EU.

3. There are a few instances where the GDPR does not apply. For example, processes covered by the Law Enforcement Directive, processing for national security purposes and processing by individuals for personal/household activities.

What information does the GDPR apply to?

The GDPR applies to both personal data and sensitive personal data – known as Special Categories of Personal Data under the new regulation. Personal data includes information such as an employee's name, email address or ID number. Sensitive data could be an employee's racial origin, political opinion, or religious belief, for example.

What will happen to the Data Protection Act (DPA) now?

The DPA 1998 was originally brought in to bring the UK's law in-line with EU legislation. Because the EU legislation was filtered through its member states as a directive, individual states were forced to pass their own legislation to comply.

Because the GDPR is a regulation, it doesn't require member states to pass national legislation. Essentially, this means the regulation is directly applicable as national law, without any further action.

The DPA is being repealed, however, it is being replaced by the Data Protection Bill. This domestic legislation is currently under review and therefore isn't finalised yet, but it'll cover areas where the UK will differ from GDPR, like law enforcement processing, immigration and national security.

Do we still need to comply since Brexit?

In short, yes.

Britain might be in the process of leaving the EU, but with that comes a lot of unknown factors. Once isolated from the EU, the GDPR would fall away from UK legislation – unless its decided to keep all or some parts of the legislation under domestic legislation.

The Information Commissioner's Office (ICO) have issued a statement to confirm that all UK data controllers and processors must comply with the GDPR – regardless of Brexit. We expect further guidance will be issued in due course but, until then, ensuring your business is compliant with GDPR is mandatory.

What data handling changes do I need to make?

Unfortunately, this question isn't as simple as it may seem. Before you can plan any changes to your business' processes, procedures, systems or departments, you need to first understand your data ecosystem.

To start, you need to get your head around how your business processes both personal data and sensitive personal data. We'd recommend you map this out the same way you would with a process map or workflow. This document should:

- Cover all departments and all systems in contact with said data – this includes manual filing systems.
- Be updated whenever a process, employee or system changes. As an example, let's pretend you've a finance manager called James, who's responsible for looking after all employee bank details. If James leaves the business and you replace him with a lady called Laura, you'd need to update the employee names in your process document to reflect this.

Once you've completed this piece of work, you'll have a better understanding of your data ecosystem and the departments that process personal data (internal or external). This should help you see where amendments need to be made.

Considerations will vary largely depending on the business you're in. Here are some broad consideration examples:

- **Lawful processing:** you must meet the conditions set out in the GDPR for processing personal data. Although the same concept was present in the DPA, in the GDPR, the legal basis now impacts an individual's rights – for example, an individual has the right to have their data deleted. There are, however, separate conditions for this depending on the category of data.
- **Consent:** under the GDPR, you must be able to prove that you've received consent to process an individual's personal data. Consent needs to be 'freely given', 'specific', 'informed', 'unambiguous' and delivered through a 'clear affirmative action'.

From marketing and sales, to HR and finance – to name just a few, both of the above examples can affect many departments within your business. This is why it's important to have clear processes in place to gain or confirm consent from employees, customers, clients and suppliers, to name just a few.

Those involved with marketing and sales should also make note of the ePrivacy Regulation, which is currently going through the approvals process within the European Council. Although not finalised, this legislation will complement GDPR in an electronic communications context.

Employee data – accountability

If your business has more than 250 employees under its belt, you'll also need to keep detailed records of your processing activities. The following details must be included in your records:

- Name and details of your business – where applicable, other controllers, your representative and Data Protection Officer (DPO), too
- Purpose of the processing
- Category descriptions for both the individuals and personal data
- Categories of recipients of personal data
- Details of transfers to third parties, including documentation of the transfer mechanism safeguards in place
- Retention schedules
- Descriptions of technical and organisational security measures.

If your business has less than 250 employees, you only need to keep records relating to higher risk processing, like outsourcing payroll and sending data to third parties, for example.

Do I need a DPO?

This isn't a one size fits all question. Some businesses might need to appoint a DPO, others might not. Here are few questions to ask yourself to assess the need for a DPO in your business:

1. Is your business a public body? This excludes courts acting in their judicial capacity.

2. Does your business carry out large, automated monitoring of individuals? For example, call listening, screen or CCTV recording.

3. Does your business process large volumes of sensitive personal data, or data relating to criminal convictions and offences?

If the answer to any of these questions was yes, it's likely your business will need to appoint a DPO. If the answer to each was no, then it's unlikely you'll need to appoint a DPO.

As it stands, there's a lot of uncertainty as to what qualifies as a 'large quantity' of data in the legislation. This is something the Article 29 Working Party are looking to address, and they'll publish an update when it's clarified.

What's a DPO?

In brief, a DPO should be an employee within your business who, as set-out by the Article 29 Working Party, is:

- In charge of ensuring and monitoring compliance with the legislation
- Accountable to the regulator
- Responsible for breaches.

As an employer, you hold additional responsibilities to your DPO. It's down to you to ensure your business' DPO:

- Reports to the highest level of management within your organisation
- Is completely independent and isn't penalised for performing their duties
- Has the required resources to meet their obligations.

Although your DPO should be an employee within your business, it is possible to outsource the role to an external contractor.

What happens if my business doesn't comply with the GDPR?

Currently, the ICO has the authority to impose a Monetary Penalty Notice of up to £500,000. This applies to data controllers where a breach or non-compliance with the DPA has been confirmed.

While the DPA only allowed action to be taken against data controllers, the GDPR allows the ICO to take action against data processors too. The GDPR also comes with a change to the value of fines that can be enforced:

- Fines for processors: up to 2% of Global Company Turnover or €10 million, whichever is greater
- Fines for controllers: up to 4% of Global Company Turnover or €20 million, whichever is greater.