Joelson

GUIDE TO GDPR

What is the GDPR?

The General Data Protection Regulation (GDPR for short) is a new data protection regime which will be implemented from 25 May 2018.

The new regime, which will replace most of our existing legislation, including the Data Protection Act, will result in a number of changes to how businesses collect, use and store data. There are a number of new obligations for those that collect and use personal data and stricter penalties for those businesses which fail to adhere to them.

At Joelson we understand businesses collect, may have questions about how the GDPR will affect them and the steps that need to be taken to ensure compliance with the new regime. This guide aims to provide an introduction to how the new framework will work in practice and the policies and procedures that businesses will need to follow.

What is "Personalised Data"?

The GDPR protects all "personal data"; this means any form of information relating to a person by which they can be identified – either directly or indirectly.

The most obvious example is an individual's name, but "personal data" also extends to information such as IP addresses and telephone numbers.

There are also stronger rules around the way in which businesses should use this as an opportunity to undertake a full review of all the personal data that they need relating to customers, potential customers, employees and contacts and audit what is held, what needs to be returned, what should be deleted and consider how their policies and procedures need to be updated to comply with the GDPR going live 25 May 2018.

Glossary of key terms

Data subject – an identifiable living individual to whom personal data relates.

Data controller – An individual who determines the purposes for which, and the manner in which, any personal data is to be processed.

Data processor – A person who processes personal data on the data controller's behalf.

What are the main changes?

Even if you are familiar with the requirements of the current position under the Data Protection Act, it is important to note that the GDPR differs in a number of key areas. In this section we consider the key differences that businesses need to be aware of.

Obtaining consent (if it is needed)

The definition of consent has changed under the GDPR, which inevitably means that businesses will need to adjust their procedures.

Consent to collect and process personal data will now have to be "freely given, specific, informed and unambiguous". This means that your business will need a positive opt-in and consent must be kept separate from approval of other terms and conditions.

As part of your preparation, you should also bear in mind:

- Existing consents may need to be refreshed
- Silence and pre-ticked boxes are not acceptable
- Additional consent is required for direct marketing purposes

Demonstrating accountability and governance

From May 2018, your business will no longer be required to register with the Information Commissioner's Office (ICO) although it is likely that the ICO will still collect fees from businesses. However, you will be expected to demonstrate compliance with data protection legislation through both accountability and governance. Consent isn't always necessary and you should consider what legitimate reason your business has for collecting such data before if consent is required.

You will need to show that data protection compliance has been appropriately considered in any situation or activity which involves the processing of individuals' personal data.

Appointing a Data Protection Officer

It will be mandatory to appoint a Data Protection Officer in certain circumstances, such as where a business has over 250 employees or an organisation is classed as a public authority. However, even if you are not required to appoint a DPO you may want to consider selecting a 'go to' person for compliance within your business.

Data processors

There are lots of new obligations and responsibilities for data processors. If you process data on behalf of another business, or if you use data processors, you will need to be aware of these new obligations and will need to update your contracts with those processors to reflect the upcoming changes.

Reporting a breach

Under the GDPR, it will become mandatory for all data controllers to notify both the ICO and data subjects of certain breaches within 72 hours of your business becoming aware of an incident. There will also be increased obligations in relation to internal governance and record-keeping.

Individual rights

The GDPR places greater emphasis on individuals' rights, for example, the right to be forgotten, and the right to restrict how data is used. You and your staff need to know what these rights are and what they mean in practice.

Next Steps

As part of your preparation, your business should identify any possible areas of weakness. Careful planning and due diligence are crucial if data is to be properly protected and you are to remain compliant with data protection legislation as it changes. Here are some of the things you will need to bear in mind.

Employees

It is important that your workforce understands the risks of breaching GDPR. Without the proper training, an employee could inadvertently leave you vulnerable to a breach of the GDPR. You may wish to consider additional training in the destruction of confidential material and best practice for data protection.

Internal processes

The way you handle and process data is a possible vulnerability. In order to comply fully with the law, your business will need to keep a detailed record of how, when, and why stored data was used. You must also delete and update data where necessary.

Penalties for breaching the GDPR

The penalties which can be imposed under GDPR will be considerably tougher than those incurred under the current legal framework. Two tiers of penalty will apply.

Tier 1 – If a data breach puts 'highly important' data at risk

Fines of up to €20 million or four per cent of the previous year's global annual turnover, whichever figure is greater.

Tier 2 – Any other data breach

Fines of up to €10 million or two per cent of the previous year's global annual turnover, whichever figure is greater.

Contact Us

Inevitably businesses will have questions about how the GDPR will affect them and what steps they can take to ensure they are fully compliant with the new requirements.

If you would like to discuss any of the issues raised in this guide or have any other questions, please do not hesitate to contact the Joelson team.

Corporate

Philippa Sturt
Partner
philippa.s@joelsonlaw.com

Philippe Hails-Smith
Partner
phil@joelsonlaw.com

Matthew Overton
Senior Associate
matthew.o@joelsonlaw.com

Employment

David Greenhalgh
Partner
david@joelsonlaw.com

Reema Jethwa
Associate
reema.j@joelsonlaw.com