FACT SHEET

What you need to know about GDPR

Quick Summary

- It is necessary for all small businesses to have a good knowledge of the General Data Protection Regulation (GDPR) when it comes to the control, storage and use of data.
- GDPR exists to protect the personal details of individuals and should be enforced by every business, large or small. You should consider appointing a data protection officer to make sure your business is compliant with data storage and use and ensure all policies on data handling are kept up to date.

Introduction

The General Data Protection Regulation (GDPR) was produced to protect the personal information of individuals and was designed to be applicable to the current technological climate where 'data is everything'.

The majority of websites collect personal data around their visitors to understand their audience and maximise experience. However, websites are not the only way in which personal data is collected; research, for example, often collects personal data through a participants' demographics. As this personal data is sensitive information, it is important that it is protected, which is what GDPR aims to achieve.

Failure to comply with GDPR can result in consequences, the most serious of which includes a fine of up to €20 million or four percent of annual turnover. Below we have provided a handy guide of what you need to know about GDPR and how you can implement this in your business.

Understanding your data

If you are regularly collecting, storing or using personal data then GDPR will apply to you. It is important to note GDPR applies to **any personal data**, from consumers to employees and suppliers, and so you must make sure you understand what data you are collecting, the reasons for collecting this data and your responsibilities in handling this data.

Consumers have data rights

It is important to know the rights of those whose data you are collecting. GDPR gives people increased control over how their data is used and their rights with regards to knowing what data is being collected and why. Because of this, consumers must give active consent for their personal data to be collected and used – this is something you may have seen when a webpage uses 'Cookies'.

When asking for consent, consumers must have the opportunity to be informed around what data is being collected, why it is being collected and how it will be used. It is also important to know that people have the **'right to be forgotten'**, which means that they can withdraw their consent for their personal data to be collected.

Adequate security measures

Personal data is sensitive information, and this can cause distress to anyone who is affected by any data breaches. It is therefore important that you have adequate security measures in place to protect this information from any cyber risks or potential data breaches. In order to ensure that these security systems are working as effectively as possible, you must test these on a regular basis and fix any potential problems as soon as possible.

Report and breaches

If the worst happens and you are subject to a serious data breach, you must report this to the Information Commissioner's Office (ICO; the UK's regulator) within 72 hours. This report must include details of why the breach happened and how your organisation is responding with regards to containment and next steps. Although there is a 72-hour window for this, it should ideally be reported within the first 24 hours following the data breach. To make things easier, staff members should be trained to be able to identify and subsequently report any breaches.

Keep records

To keep you protected in the event of an enquiry as to your handling of data, make sure that you keep up-to-date records of your collection, storage and use of data, alongside a description of your security measures and proof that you have been testing these on a regular basis. These records not only show that your company is GDPR compliant but are also important to have in the event of a data breach.

Data protection officer

Small businesses with less than 250 employees can be exempt from some of the rules set out in GDPR due to having less resources available to carry these out. However, if this applies to you, this does not mean you should be more relaxed about GDPR. Even if you may be exempt, it is good practice to put things in place, especially if you're planning to grow your organisation.

One good way to ensure you are GDPR compliant is having a Data Protection Officer (DPO). A DPO ensures that the company complies with GDPR and is the contact for any data protection enquiries.
If your company handles and processes large-scale data, then you should have a DPO regardless of the size of your company.

Following these steps can help you to ensure that your business is not only GDPR compliant, but is also protecting the sensitive information of its consumers.

Need more support?

Get in touch!

For more information visit **www.businesslincolnshire.com** where you can request support from one of our advisers by filling in the online contact form.

@businesslincs

businesslincolnshire@lincolnshire.gov.uk