What Is GDPR And What Does It Mean For My Business?

What Is GDPR?

GDPR – or General Data Protection Regulation – is intended to unify and strengthen data protection across the whole of the European Union. The European Parliament, the Council of the European Union and the European Commission are all aligned in the delivery of the regulation, which has been four years in the making.

It will specify higher fines for breaches and non-compliance and will provide individuals with more control over what companies can do with their personal data.

It will also make data protection rules all but identical across the whole of the EU.

Why Is It Happening?

There are two main reasons for the introduction of GDPR:

Security

The regulation is designed to bring data protection legislation in line with the ever changing ways that data is used, for example the way that companies such as Google and Facebook now swap access to their customers' data in exchange for their services

The current legislation – the Data Protection Act 1998 – came into being prior to widespread use of the internet and

the invention of cloud-based services so, as such, it is out of date with regards to associated security issues such as data exploitation. By bolstering data protection legislation and introducing tougher enforcement and prosecution measures, the EU aims to increase trust in the digital sphere.

Legality

By introducing a clear, uniform legal realm in which businesses must operate, the EU aims to make data protection identical through the whole of the single market. The estimated cost saving of this endeavour is currently estimated $2.3billion per year.

When Is It Happening?

While the regulation came into force on 24th May 2016 when all EU members agreed to the contents, the official implementation date for GDPR to become law is 25th May 2018, ensuring you have sufficient time to implement any changes in order to ensure your business is compliant.

GDPR is a regulation, not a directive, so the same legislation will apply to all EU members.

Who Will Be Affected?

GDPR recognises that smaller businesses require different practices to large or public enterprises. Article 30 of the regulations states that organisations with 250 employees or less will not be wholly bound by GDPR, although the recommendation is that they do comply.

Companies with more than 250 employees must employ a data protection offer, to ensure full compliance to the specified regulations.

Two main groups will be affected by GDPR:

- 'Controllers' of data – those who state how and why personal data is processed. These range from online businesses to charities and even the government – essentially anyone who collects any element of personal data
- 'Processors' of data – those who actually process the data, such as IT companies

The regulations state that even if controllers and processors are not based in the EU, they still need to comply with GDPR, as the data they are collecting and/or processing belongs to EU residents.

It is the controller's responsibility to ensure their processor adheres to data protection law, whilst processors themselves must ensure they abide by the rules which determine how they record their processing activity. Should a processor be involved in a data security breach, they will be considerably more liable under GDPR regulations than they were under the Data Protection Act.

What Do I Need To Know?

While you may be aware of GDPR, you may not know what you need to do to ensure full compliance.

Lawful collection

Once GDPR become law, controllers are legally obliged to ensure any personal data is processed lawfully and transparently. It must also be collected for a specific purpose. Once the objective of that purpose has been met, the data should be deleted as it is no longer required – known as the 'right to be forgotten'.

This regulation also allows individuals to demand that their data is deleted if they've withdrawn their consent, or they object to the way it is being processed. It also specifies that the controller is responsible for telling other organisations such as Google for instance, to delete any links to copies of that data, as well as deleting the copies themselves.

The term 'lawful' is key to GDPR and it has several meanings:

- If the subject has consented to their data being processed
- If the collection fulfils a legal obligation or contract
- If the collection is in the interest of protecting an interest that is 'essential for the life of the subject'
- If processing the data is in the public interest
- If processing the data is in the legitimate interest of the controller, such as fraud prevention

At least one of these justifications must apply in order to process data under GDPR.

Consent

Under GDPR, consent to collect personal data must be an active and affirmative action from the subject, as opposed to the existing passive acceptance methods of opt-outs or pre-ticked boxes.

The regulations state that controllers must keep records of both how and where an individual gave consent for their data to be collected. The individual must also be able to withdraw their consent whenever they wish.

If your existing data collection consent method does not meet these requirements, you must either:

- Bring it in line before 25th May 2018
- Cease collecting data from 25th May 2018

What Is Classified As Personal Data?

GDPR has expanded the definition of personal data compared to the existing legislation. Anything that counted as personal data under the Data Protection Act continues to qualify as personal data under GDPR and in addition:

- IP addresses are now classified as personal data
- Economic, cultural and mental health information are now classified as personally identifiable information

Can Individuals Access Their Stored Data?

GDPR states that:

- Individuals may request access to their data at 'reasonable' intervals and controllers must respond to the request within a specified time frame of one month
- Individuals have the right to access any personal information a company or organisation may hold
- Individuals have the right to know why their personal data is being processed, how long it will stored for and who has access to it
- Individuals have the right to request their personal data, if incorrect or incomplete, is rectified when they wish

The new regulations state controllers and processors must:

- Be wholly transparent with regards to how they collect data
- What they intend to do with the data
- How they process it
- Store data in commonly used formats (such as CSV)

What Happens If Data Is Breached?

In the event of a data security breach, GDPR states that you must inform your relevant data protection authority within 72 hours of you becoming aware of the breach. The UK authority is the Information Commissioner's Office.

When you report a breach you should inform the authority of:

- The nature of the data that's affected
- Approximately how many people are impacted
- What the consequences could mean for them
- Specific measures you've already actioned or plan to action as a result of the breach

Prior to informing the Information Commissioner's Office of a data breach, you must inform the individuals affected. If you fail to do so within the 72 hour window, the penalty is a maximum of 2% of your annual revenue worldwide, or the equivalent of €10 million, whichever is higher.

What If We Fail To Comply With GDPR?

As well as the fine for failing to inform affected parties in the event of a data breach, if you don't adhere to the key principles for processing data, such as obtaining the correct consent, meeting individuals' rights over their data, or you transfer data to another country, the fines are considerable.

Your data protection authority could issue a penalty of up to €20 million (equivalent), or 4% of your global annual revenue, whichever is greater.

What Happens When We Leave The EU?

The expectation is GDPR will become law before the UK formally leaves the EU, so UK businesses must comply with the legislation.

What Are My Next Steps?

The best thing to do is to start preparing for the implementation of GDPR as soon as possible:

- Check your existing policies and provisions and, if necessary, instruct a data protection officer
- Ascertain which policies you need to update or adopt, in order to meet compliance law
- Ensure you train your staff to meet the new requirements
- If you work with any third parties who classify as processors, check their data policies comply with the new regulations

If you need any assistance or advice in preparing your business – large or small – for the implementation of GDPR, get in touch with our team of experts and we'll be happy to advise you.

Need IT Support?
Get In Touch With Cheeky Munkey

Full Name

Email

Message

SUBMIT

Previous View All Next

Categories

- Backup
- Cabling
- Cloud Services
- Internet Connectivity
- IT Services
- IT Support
- Security

Archive

- January 2018
- December 2017
- November 2017
- October 2017
- September 2017
- August 2017
- July 2017
- June 2017
- April 2017
- March 2017
- February 2017
- December 2016

cheekymunkey
IT SUPPORT

For all your IT support, covering London and the South East

8 Parkway Porters Wood
St Albans
AL3 6PA
Find us here

Studio Office
336 Old York Road
London
SW18 1SS
Find us here