A Guide to General Data Protection Regulations 2018

From 25 May 2018, how you handle your customers' personal information and data is changing and your business will need to be compliant in the new regulations.

We've created a simple Q&A guide to help support you in your GDPR journey ahead of the EU's new data rules.

K2 Management Solutions Ltd

Never heard of the GDPR?

A recent government report – The Cyber Security Breaches Survey 2017 – found that while awareness among larger businesses was widespread, many smaller businesses were 'often' unaware of the GDPR.

On the 25 May 2018, the EU's European General Data Protection Regulation (GDPR) will come in to force. And, as it is an EU regulation, the GDPR will automatically take effect without the need for it to be locally implemented by member states.

Who does the GDPR apply to?

The GDPR applies to businesses who offer goods or services to data subjects within the EU as well as those who monitor the behaviour of data subjects in the EU.

It applies to data controllers as well as data processors and substantially extends the territorial scope of companies who have to comply (in comparison to the UK Data Protection Act 1998).

We're leaving the EU – won't that mean UK businesses can ignore the GDPR?

With the GDPR's implementation date of May 2018 happening before the likely March 2019 date of the UK's withdrawal from the EU, businesses will still need to be compliant with the GDPR for a period of at least ten months.

Although the UK's data protection status after Brexit is still unknown, the government has suggested that it intends to implement equivalent GDPR rules post-Brexit in order to make sure that the movement of data between the UK and the European Economic Area continues after we leave.

Not long to go until its implementation –

25 May 2018 is the deadline for companies to be compliant and there will not be a further grace period.

We hope this guide will help you understand what actions you need to take now, as well as what will happen if you experience a data breach under the new regulations.

What is the GDPR and how does it apply to you?

Designed to help safeguard data protection rights for individuals, the GDPR introduces a single set of rules across the EU when it comes to how companies handle data relating to individuals.

That means if your business holds personal information such as names, addresses, HR records, customer lists and even online identifiers such as a computer's IP address, you could be subject to certain requirements of the GDPR.

Am I exempt as a small business?

Whether you're a large or small business you don't fall outside of the scope of the GDPR – all companies, regardless of size, have to take action when it comes to data protection.

There are some areas where it is acknowledged that SMEs have fewer resources and pose less of a risk, so may be exempt from some of the more rigorous steps (such as the need to appoint a data protection officer).

It is also worth noting that even if a small business falls within one of these exemptions, if you are contracting with a larger company that doesn't, you may find yourself having to meet the higher level of data protection set by the GDPR.

Larger companies are starting to prepare themselves for the GDPR's arrival and looking to force their supply chain, by contract, to meet certain information security requirements.

What do you, as a small business, need to do to be compliant with the GDPR?

There are several simple steps that all small businesses need to consider to make sure you are compliant by 25 May 2018.

Know what data you hold, where it is coming from and where it is going

It is important that you understand and record what 'personal data' you hold as a business, how it was captured, how it is held, how you use it, and where it is going.

The EU defines 'personal data' as: ..."any information relating to an individual, whether it relates to his or her private, professional or public life". It can be anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer's IP address.

The GDPR definition of 'personal data' is broader than under the DPA and includes IP addresses, device IDs, location data and genetic and biometric data.

Are you relying on consent?

If you are relying on consent to process a data subject's 'personal data' (e.g. for marketing purposes), the GDPR will make this a lot harder. The definition of consent has been tightened so that it must be 'unambiguous' when given. Where relied upon, consent will also have to be gained retrospectively for existing customers.

In addition, requests for consent will also have to be presented in a manner that is completely separate, so they can no longer be hidden within other policies or small print on your website.

Where you are relying on consent to process 'personal data', being able to prove how you obtained it will be vital. Silence, pre-ticked boxes or inactivity will no longer be valid and customers/prospects will have to express their consent in a more unambiguous way (i.e. by actually ticking a box).

Think about:

How consent is obtained at the moment, if at all ▫ what changes to your processes may be needed to make sure that you are able to show where, when and how people have adequately given you consent to process their data.

Data protection by design

Under the GDPR the protection of data has to be considered and implemented into any systems/processes from the outset – both in terms of the way that computer systems are designed and the policies/procedures that are in place to dictate how people should use them.

One element that gets a much higher profile and attention from the GDPR is the use of encryption. Not only is this top of the list of suggested security measures, but the broad use of encryption can also reduce some of the burden and likelihood of a penalty being applied in the event of a data breach.

Right of data access

Individuals will have a number of rights when it comes to how you look after their 'personal data'.

Make sure there are appropriate processes and templates in place so that Individuals rights can be met within the new timescales (one month).

Individuals will have the rights to:

- access all data held on the individual
- rectify inaccurate data
- object to the processing (in certain circumstances, e.g. marketing) of data
- export the data in a format that can be used in another IT environment
- completely erase all data on an individual (in certain circumstances).

Know what constitutes a data breach

Make sure you and your employees understand what constitutes a data breach and put in place a process for flagging and escalating breaches internally. This is vital to meet the strict timescales for response laid out by the GDPR.

Alongside the training needed for this, you should try to develop and encourage a culture where employees feel comfortable in self-reporting when they have made innocent mistakes – the root cause of the vast majority of data breaches

Review terms and conditions and supplier contracts

Conduct due diligence on any suppliers that process 'personal data' on your behalf, or jointly with you, to make sure that there are adequate protections in place to cater for the GDPR. This could be by either asking them to complete a form to capture what measures they have in place, (which should then be reviewed to make sure that they are sufficient) or by conducting an onsite audit.

Where your suppliers are processing 'personal data' on your behalf, you have an obligation to update your contracts with them to include a number of mandatory clauses that can be found in Article 28(3)

of the GDPR. These provisions ensure that processors are contractually obliged to provide GDPR compliant data protection standards.

It is worth noting that if you act as a data processor for other companies, they will be looking to amend your contract with them on the same basis, and new customers will increasingly focus on this.

Review your fair processing notices (your customer facing privacy notices)

Because of the requirements imposed by the GDPR, your fair processing/privacy notices are now likely to get a lot lengthier.

You will need to go into much more detail and will also need to write your policies in a way that is understandable and accessible to your customers. There are also some differences in what you are required to provide, depending on whether you are collecting the information directly from data subjects or from a third party.

The information that should be supplied includes:

- the purposes for which you're processing the personal data as well as the legal basis for the processing (e.g. consent, legitimate interests, contractual requirement etc.)
- the recipient or categories of recipients you may be sending the personal data to
- the retention period or criteria used to determine the retention period
- the existence of each of the data subject's rights

For more on the requirements, please check the Information Commissioner's Office (ICO) guidance: https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/

Privacy impact assessments

Before beginning data processing likely to result in a 'high risk to individuals', a documented risk assessment will be needed to identify and mitigate the risks and demonstrate compliance with the GDPR.

What constitutes a 'high risk to individuals' is unclear, but it could include things such as the capture/processing of sensitive data like bank account details, or health information that could be very damaging to the individual if leaked.

Understand whether you need to appoint a data protection officer (DPO)

While most businesses with fewer than 250 will be exempt.

If your core activities involve 'large-scale' monitoring or processing of sensitive data (which includes data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health), a DPO has to be appointed who must be independent of management and the team undertaking the processing.

The DPO's responsibilities cannot just be delegated to the IT person.

The EU doesn't fully define what constitutes 'large scale', but some of the examples that they have given include processing:

- patient data by a hospital
- travel data for people using a city's passenger
- transport service
- customer data by an insurance company or a bank

What if you have a data breach under the GDPR Regulations?

The GDPR defines a 'personal data breach' as 'a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data'. This means that a 'personal data breach' is more than just being hacked or losing personal data.

This also applies to data held in any form – not just electronic. Paper-based data that is structured according to specific criteria should be treated with the same level of care.

When to report a breach

Breaches will have to be reported to the ICO if they are 'likely to result in a risk to the rights and freedoms of individuals'.

The examples provided by the ICO are where the breaches may 'result in discrimination, damage to reputation, financial loss, loss of confidentiality, or any other significant economic or social disadvantage'.

Breaches will only have to be reported to the individuals concerned where there is a 'high risk' of the above – stricter reporting requirements than under the Data Protection Act.

How long before reporting a breach?

Where a breach has to be reported, it has to be done within 72 hours, and that report must contain, as a minimum:

- the nature of the personal data breach including, where possible, the categories and approximate number of both the individuals and personal data records concerned, the name and contact details of the data protection officer or other contact point where more information can be obtained
- a description of the likely consequences of the 'personal data breach'
- a description of the measures – proposed or taken – to deal with the 'personal data breach' and, where appropriate, of the measures taken to mitigate any possible adverse effects

How to prepare for breaches

Given the broad definitions of ‘personal data breach’ and ‘personal data’, it’s almost inevitable that companies will have at least a minor breach (such as sending an email to the wrong person) at some point,. It’s well worth giving some thought as to how you will respond as and when that time comes, particularly given the stringent timeframes required for notification.

A simple, but thought-out, incident response plan can make a huge difference to minimise the impact on your business.

Things to consider are:

- who should breaches be reported to internally?
- who needs to be involved in any investigation? (This could be internal or external IT service providers, or specialist IT forensics)
- what are the most critical systems and data, to prioritise protection and restoration?

What are the consequences of failing to comply with GDPR?

While compliance with the GDPR may seem labour intensive, it will ultimately exist to make sure that businesses are able to best protect their customer data.

When companies fail to protect data there can be a massive detrimental impact on their own reputation so compliance with the GDPR and the protection of customer data is in the best interests of your business and in the protection of your hard-earned reputation.

The fines for non-compliance

Failure to comply with the GDPR (not just by experiencing data breaches, but through ‘administrative failures’ such as not completing – or even just not documenting – privacy impact assessments) could result in a regulatory investigation, which in itself takes time and effort on the part of a business, and potentially a fine being levied.

The size of the fine could be up to 4% of a company’s global turnover (for the previous year) or €20 million (whichever is the higher) for the most serious of breaches, or 2%/€10 million for those matters considered administrative.

Although it would be very surprising if a small business was fined anywhere near these figures, the ICO has already demonstrated their willingness to impose financial penalties, even against SMEs, albeit paying attention to the business’s ability to continue trading following any such penalty.

Where can you get additional help/support?

If you are unsure of what to do to get your business compliant, please contact us in the first instance and we will support you:

T: 0115 784 4664
E: info@ktoo.co.uk

Further information and resources can be found on various websites regarding the implementation of the GDPR;

- the ICO provides updates for businesses including a data protection self-assessment toolkit: https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/

https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf

https://www.theagenci.com/gdpr-myth-busting/

https://www.dataiq.co.uk/blog/summary-eu-general-data-protection-regulation