highwoods & associates

General Data Protection Regulations

Everything you need to know
and the steps you need to take

The Do's and Don'ts of GDPR

- **DO** maintain a record of how, where and why consent was obtained
- **DON'T** use consent by default
- **DO** delete personal data when a customer exercises his or her right to be forgotten
- **DON'T** further process data in a manner that is incompatible with its original purpose
- **DO** report a breach to the relevant authority and affected parties
- **DON'T** leave more than 72 hours to report it
- **DO** inform your employees about cyber security best practice
- **DON'T** wait for GDPR to come to you. Seek assistance now

For further information and guidance visit www.ico.org.uk

General Data Protection Regulations (GDPR)

So what is it all about? Well, GDPR is a replacement for the Data Protection Act (DPA). The essence is that this is about bringing the legislation up-to-date with the changing landscape of data and technology.

Does it affect me as a small business?

Yes, GDPR affects everybody. Even if you don't think you process data, you probably do. Do you have employees? Do you have customers? Do you hold data about them? Names, Telephone Number, National Insurance Number? You are processing data and therefore GDPR is relevant to you. Do you hold email addresses of people? Again, you are processing data and GDPR applies.

There is a lot of information about GDPR and it is very confusing

Yes, there are a number of companies that are using GDPR to scaremonger and market their own services. This guide is aimed at cutting through the jargon and giving you an insight into GDPR. It is only a guide and the landscape of GDPR will evolve. If you identify areas within your business that you believe may have issues, then approach a GDPR expert. This booklet and information contained is not a replacement for professional advice.

> "**GDPR affects everybody.** Even if you don't think you process data, you probably do"

Key differences between GDPR and the UK Data Protection Act

GDPR looks more at how data is stored and used. You will need to maintain records of 'consent' and individuals have the right to be forgotten.

It redefines and sets new standards for consent. It's all about the customer wanting to give his or her information away and less about marketing trickery. An example could be where you have to opt-out rather than opt-in, or you sign up for a resource, but get marketed to about other products.

As a result, consent requires a positive opt-in, spelling the end for pre-ticked check boxes or any other method of consent by default. Neither should consent to be a precondition of using a service.

Request for consent should be explicit, in that it is separate from your terms and conditions. It's clear and specific and any relevant third party organisations are named. Blanket consent is not enough. **Remember: keep a record of how, when and where consent was given.**

Consent should be:

- Actively given
- Explicit
- Specific
- Kept separate to other information
- Documented

When does GDPR become effective?

The legislation was approved in April 2016 but becomes effective on 25 May 2018. So the clock is ticking. This is not something you can start doing when it becomes effective – you need to think now how it affects your business and question what you do.

How will BREXIT affect this?

The government has committed to introducing a new Data Protection Bill and it is likely that the provisions of GDPR will be contained within that bill. Also, if you deal with Europe you will still need to comply with GDPR.

What types of data does GDPR cover?

It covers personal data which can be traced back to an individual, that may include the following as well as others:

- Internal and external emails
- Other electronic communications
- Personal data held for marketing
- Personal data for running your business
- How data is transferred

Do I need to take it seriously?

Whereas previously Data Protection was often seen as not a big deal for SMEs, with GDPR it now has real teeth that could affect your business.

Fines can be imposed equivalent to 4% of your previous year's global annual turnover or up to €20m, whichever is higher for a 'highly important' data breach.

For other data breaches this is the higher of 2% of your previous year's global annual turnover or up to €10m.

The Information Commissioner's Office (ICO) has said that if businesses are open and honest and report breaches without undue delay, then the fines may be avoided.

What do you need to know?

Understanding
Not just the decision makers within your business need an understanding, everybody needs an appreciation of the impact GDPR is likely to have.

Information you have
You need to document what personal data you have and hold, where it came from and who you share it with. Do you still need it?

The rights of individuals
Your systems and procedures should ensure that you comply with all the rights an individual has. These include how you would delete information and how you provide it in a common format.

The "right to be forgotten" and may withdraw their consent
You should be able to erase data from your systems easily and have a simple request process to withdrawing data. This includes your live systems and backups.

When should data be "forgotten"? Individuals have the right to be "forgotten" from your systems.

This means removing all data that could be linked to them. Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed. Or when the individual withdraws consent. Or when the individual

"Not just the decision makers within your business need an understanding, **everybody needs an appreciation of the impact GDPR is likely to have**"

objects to the processing and there is not an over-riding legitimate interest for continuing the processing.

Under certain circumstances a company can refuse to erase data. For example, it could continue to use information to:

- **Exercise the right** of freedom of expression and information
- **Comply with a legal obligation** for the performance of a public interest or exercise of official authority
- **Support legal claims**
- **For public health purposes** in the public interest
- **For archiving purposes** in the public interest, scientific, historical or statistical

Communicating privacy information
Look at any privacy notices and review them in the light of GDPR. Do you actually have any? What do you need in place?

Subject access requests
You systemise how you will deal with these requests within the new timescales of 30 days. You should be able to supply details of data held on request and be able to justify how the data is being used and understand the rights of an individual over their data.

Lawful, fairly and transparent basis for processing personal data
Why are you processing the data? Document it and update any privacy statements to explain this.

Personal data is any information that can be related to an identifiable person. Such as a name, reference number, location data or online identifier.

Consent
Review how you obtain, record and manage consent.

Children
If you collect details of children then you need to verify individuals' ages and obtain parental or guardian consent.

Data breaches
Make sure your procedures are in place to detect, report within 72 hours of any discovery of the breach, and investigate personal data breaches. A data breach is a loss, alteration, destruction, unauthorised disclosure or access to personal data.

Detections and reporting of data breaches should be in line with the ICO's mantra "tell it all, tell it fast, tell the truth".

If there is a high risk of a data breach through your processes
You may need to complete a Data Privacy Impact Assessment (DPIA) to assess the possible issues. So identify any of these areas and look at them in detail and refine the procedures to reduce or eliminate the risk.

Data Protection by Design and Data Protection Impact Assessments
You should familarise yourself with the latest guidance and work out how to implement this within your business.

Data Protection Officers
You should designate somebody to take ownership and responsibility for Data Protection Compliance. If you have fewer than 250 employees this is not a requirement, but still good practice to do so.

International
If you work in more than one EU member state, you should determine whom your lead Data Protection supervisory authority is.

If you store or process data outside of Europe then there are strict rules governing the transfer. US companies may be covered by the Privacy Shield, but this could change. So you need to identify any data held outside the UK and whether this is GDPR compliant.

Cloud Technologies
As more processing and data storage is completed in the 'cloud' this presents it own challenges.

Whether in the EU or not the provider of these services needs to be compliant if they are handling data about individuals within the EU.

As a Data Controller it is your responsibility to ensure that the provider is compliant and that you have this documented in contracts or documentation. The supplier as a Data Processor is required to act within GDPR.

While you may assume that this would be the case with large companies, some are still working towards being compliant and are not there yet.

Therefore you will need to assess who is and who isn't and what are the plans for being compliant and by when.

You may need to consider moving away from certain providers.

The key data protection principles are:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability

Review your cyber protection
Over 50% of companies in the UK suffered a breach or attack within the last 12 months, according to gov.uk. The most common breaches were fraudulent emails, viruses and malware.

So protecting against this is one of the first steps to put in place. Cyber protection can be a complex process, but to start with do you:

- **Have current operating systems** on your computers?
- **Up-to-date antivirus**?
- **Do firewalls secure** your networks?
- **Are your computers and systems secured** by complex passwords that are forced to be updated?
- **Do you use data encryption** to transfer information?

Exemptions
GDPR generally applies to all, however there are a couple of small exemptions.

GDPR will not apply to personal data under contractual obligations, such as issuing invoices to customers.

If you have less than 250 employees you are not required to record your processing activities, unless this relates to higher risk processing such as an activity that could risk the rights and freedom of an individual.

Where to start?

Register with the Information Commissioners Office (ICO) www.ico.org.uk if you have not already done so.

Your first step should be to appoint a *Data Protection Officer* (DPO). Is this yourself or a carefully selected employee? DPOs may need to be appointed under statutory criteria. For companies under 250 employees this is not a requirement but good practice to give it focus.

GDPR is not the responsibility of one individual. You rely on everybody within your business not only to be aware of it, but to police it for you and highlight areas of weakness to be addressed before breaches happen. They need to know what a Data Breach is.

What is personal data?
Any information that can be related to an identifiable person. Such as a name, reference number, location data or online identifier.

"GDPR is not the responsibility of one individual. You rely on everybody within your business not only to be aware of it, but to police it for you and highlight areas of weakness"

The six main principles of GDPR as defined by the ICO

01.

Processed lawfully, fairly and in a transparent manner in relation to individuals.

You need to identify a lawful basis on which to process personal data. You need to document all interactions with the data, including how, when, and where you obtained it, and how consent was agreed. Pre-ticked consent boxes are not deemed 'transparent' under GDPR.

02.

Adequate, relevant and limited to what is necessary in relation to the purposes from which they are processed.

Personal data held should be no more revealing to function its specified, explicit and legitimate purpose.

03.

Accurate and where necessary, kept up-to-date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

Data should be accurate and kept up-to-date. If errors are found they should be rectified immediately.

04.

Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

Data stored should be used for the purpose you initially stored it for and should not be used to benefit your organisation in any further endeavors. For example, if your data subject gave consent to receive email marketing, they should not be contacted via telephone or post.

05.

Kept in a form, which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interests, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures, required by the GDPR in order to safeguard the rights and freedoms of individuals.

Data should be deleted as soon as it is no longer necessary to achieve the specified purpose. For example a customer who entered a competition but did not want to receive any further information.

06.

Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

You need to put in place procedures and systems, which protect the security of personal information.

	ICO GDPR Consent Checklist	
1	Ask for consent	
2	Check that consent is the most appropriate lawful basis for processing	
3	The request for consent was prominent and separate from your terms and conditions	
4	Ask people to positively opt-in	
5	Don’t use pre-ticked boxes, or any other types of consent by default	
6	Use clear, plain language that is easy to understand	
7	Specify why you want data and what you’re going to do with it	
8	Give granular options to consent to independent operations	
9	Name your organisation and any third parties	
10	Tell individuals how they can withdraw consent	
11	Individuals can refuse consent without detriment	
12	Consent is not a precondition of service	
13	Online services to children are only available if you have age-verification and parental-consent measures in place	

About Highwoods & Associates

At Highwoods & Associates, we maintain a high level of personal relationship with our clients thereby ensuring a wider range of interaction which raises trust and long-term commitments from our clients.

Our clients do not feel on their own because we do not only help with financial accounting but also on developing businesses and making taxation decisions for your organisation. This proves to be a major help since it is provided by professionals who have the know-how on facing and solving entrepreneurship and taxation hiccups in a reliable way.

In all our activities, we encourage clients to express their views and strive to create an inviting environment and atmosphere for them to do so comfortably.

support@highwoodsandasociates.co.uk

www.highwoodsandassociates.co.uk

FIND US ON SOCIAL MEDIA


highwoods
&associates