General Data Protection Regulation (GDPR)

Since 25 May 2018, all businesses that collect, store or transfer the personal data of their customers, business prospects or staff will need to comply with the GDPR and the UK Data Protection Act 2018.

The Information Commissioner's Office (ICO) describe their GDPR notes and advices as a "living document", accordingly, we will have to absorb information on this complex topic as it develops over time. The GDPR is a published EU directive and is now supplemented by the Data Protection Act 2018.

Why should you take the GDPR seriously?

Basically, because there are significant financial penalties for getting it wrong: fines of up to 4% of an organisation's worldwide turnover. Which is why larger corporations are sitting up and taking notice of the GDPR; this new regulation places respect for the rights of an individual for privacy squarely at the feet of the UK business community.

Another serious contender, if you are looking for a justification to invest time in GDPR compliance, is the likely loss of business if you don't become compliant.

Why should this be?
When your customers send you information in order that you can provide them with the goods or services you supply, they may include the personal data of their staff, or possibly other personal data under their care and control to communicate what they need from you.

As part of your customers' obligations under the GDPR they will need to seek reassurance from you that you are GDPR compliant. Without this reassurance, if you have a data breach, and their personal data is compromised, liability under the GDPR will fall on your customer. Accordingly, if you cannot give your customers confirmation that you are GDPR compliant they may well seek other suppliers who are.

New obligations

New requirements, not in the present Data Protection Act 1998, include:

- reporting data breaches. These need to be documented in a structured way so that you can evidence that you dealt with any breach in accordance with the new regulations;
- cross-border considerations;
- new rights for contacts: need to inform contacts how you are using their personal data and their rights under the GDPR to request that personal data is deleted;
- need to demonstrate that your firm is mitigating against risks of misuse of clients' personal data.

Since 25 May 2018, assessing and protecting clients' personal data (essentially protecting their privacy) needs to be of paramount concern. As we have already demonstrated, one major difficulty for businesses that do not meet the GDPR requirements will be loss of business when they are unable to meet their customers' needs to deal with companies that are GDPR compliant.

Two key concepts of the GDPR: lawfulness and consent

Article 6 of the GDPR is worth a special mention. This includes the definition of "Lawfulness of processing", and the wider implications of consent. This is important as it sets the framework within which we are required to operate since 25 May 2018.

At first glance, you may believe that you are required under the GDPR to document a customer's consent for each action you undertake on their behalf. Clearly, this would involve a radical expansion of non-productive activity within your businesses.

In fact, this interpretation is incorrect. Consent is not always required in order to meet the required "Lawfulness of processing". It is worth spelling out when consent is not required.

Consent to specific processing of personal data may not be required if:

1. it is necessary for the performance of a contract, to which the customer is party to, to take steps at the request of the customer prior to them entering into a contract;
2. processing is necessary for compliance with a legal obligation to which the controller (your business) is subject, or
3. processing is necessary to protect the vital interests of the data subject or of another natural person.

However, there is one area where you may have to seek consent, and it is when you offer customers, prospects and referral sources the opportunity to join your mailing lists, and be updated on marketing or other generalised news.

Where to start?

You will need to undertake a number of actions to achieve compliance. The major items include:

- assign a person to take charge of data compliance;
- undertake a data audit. This will involve mapping the types of personal data your business collects and stores;
- record in some detail how you process personal data in your business;
- identify, assess and track the risks associated with the processing of data;
- you will need to evidence that customers and staff know what personal data you hold by adapting privacy statements and changing contracts of employment. This will include: a review of the privacy notice posted to your website, changes to your contracts of employment and changes to your contractual terms and conditions;
- train staff to be mindful of your data security arrangements and document their participation in your GDPR training processes;
- consider systems set up to obtain consent from marketing contacts or other situations where you have no contractual obligation to retain or use personal data;
- deal appropriately with data breaches and requests from data subjects;
- if you use third parties to manage any of your online processes, and this involves placing personal data under your supervision within their care and control, then you must ensure that the third-party is GDPR compliant. Otherwise, as indicated above, you will bear liability for any breach of their data security;
- review the security of your IT systems especially those that store or transmit personal data.

You must be able to demonstrate that you are managing your GDPR obligations effectively if you want to avoid the penalties for non-compliance and the other downside risks, such as losing customers who only want to work with compliant businesses.

If you do not have the necessary skills to undertake this work in-house we may be able to help. If we judge that your circumstances require more specialist assistance, we can refer you to a third-party organisation that can guide you through the work that needs to be done.

Do not sit on the fence. None of us relish taking on yet another raft of red-tape and yet the security and management of personal data is now firmly in the legislator's sights – ignore at your peril.

Summary action list

- Identify someone in your business to take charge of the process.
- Seek professional help.
- If you set up a new business, GDPR compliance needs to be top of your to-do list.
- Don't forget that each business you manage will need to be compliant.
- Make sure your staff understand their obligations under the GDPR.
- Once you achieve compliance be sure to advertise the fact on your website.

To get more detailed information - check out the following resources:

These will assist you in becoming GDPR compliant. The resources cover aspects such as data mapping and understanding what confidential data you currently hold, communicating privacy information, consent, working internationally, how to handle a data breach and handling data on children.

www.ico.org.uk is the UK's main GDPR portal. The Information Commissioners Office has a wealth of resources to assist you in becoming GDPR compliant. Another great source is the Direct Marketing Association **dma.org.uk/gdpr**.

For an understanding of your consumer rights check out Which? **www.which.co.uk**

HEIGHTEN
Taking Your Business To New Peaks

0203 9002424
info@heightenaccountants.co.uk
www.heightenaccountants.co.uk

84 Aldermans Hill
Palmers Green
London
N13 4PP