The General Data Protection Regulation – New requirements for all businesses!

WILDS
Business Advisers & Chartered Accountants

European data protection laws are changing and come into force 25 May 2018. These new laws will affect all businesses in the UK and the current Data Protection Act (DPA) will be updated to reflect the GDPR obligations.

The GDPR is a framework with greater scope, much tougher punishments and judicial remedy for those who fail to comply with new rules around the storage and handling of personal data, be it in physical or electronic format.

Why are these new laws being introduced?

Since the DPA was introduced in 1998 technology and the internet have developed at such a rapid rate that these rules are now deemed to be ineffective. Nowadays, the ease and sophistication of data collection means that thousands of SMEs not only collect personal details, but store, move and access them online. Personal data is used in everything from sales to customer relationship management to marketing. Cybercriminals are now much more common. In 2016, companies in the UK lost more than £1billion to cybercrime. Major data breaches have given criminals access to names, birthdates and addresses and even social security and pension information.

A recent report from the Federation of Small Businesses (FSB) claims that SMEs are now more likely to be targeted by cybercriminals than their large corporate counterparts and cybercriminals consider SMEs softer targets!

The GDPR is considered a necessity for the protection of data in a modern internet based society.

It is also a chance to take a fresh look at your data security as data breaches may impact on your business reputation.

What does the GDPR mean for SMEs?

Businesses must keep a detailed record of how and when an individual gives consent to store and use their personal data. This means a positive agreement and cannot be inferred from a pre-ticked box. Customers or individuals have the right to withdraw consent. Details must be permanently erased.

This means businesses should review their existing data and delete any that they do not have a valid reason to hold it. The GDPR sets out the legal bases available for processing personal data such as needing it to perform a business contract. Businesses should review what data they hold, have they got consent and do they need to keep it?

Data should be kept secure and this will require a review of current practices to prevent data breaches.

Personal data is a key tool for SMEs looking to target and retain customers: GDPR means it must be handled with the utmost care.

You should start planning for the GDPR now and consider an information audit and, for many businesses, a change in culture.

Please see https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/ for further information on the GDPR.

We have produced a checklist of actions you should undertake before 25 May 2018 to ensure you have a policy for compliance to ensure you have the correct permissions and data is stored as securely as possible.

GDPR PLANNING CHECKLIST

The GDPR takes force from 25 May 2018. You should start planning so that on that date you can demonstrate compliance with the GDPR. Businesses are expected to put into place comprehensive but proportionate governance measures.

The following checklist will allow you to prepare for the GDPR by documenting existing procedures, looking for areas to strengthen. You will need to use your judgement to confirm you have proportionate governance measures if you complete the planning yourself or you may choose to use an external consultant. Document the actions you are planning to take and note the changes.

1. Review all data held and ask “why is it held?” and “do you still need it?” and “is it safe?” Make sure you note the different sorts of data you hold e.g. employees, customers, suppliers, third parties;

2. Look at your consent procedures as well as privacy notices on your web site and terms of business. Do you get customers to positively agree to you holding their data;

3. Document the reasons you hold data e.g. consent, legitimate interests or a legal obligations to collect and process data;

4. Plan how you will handle data requests and the right to be forgotten from individuals within the new timescales;

5. Look at your processes to keep data safe, identify any problem areas (e.g. data held on mobile devices) and decide how you can reduce the risk of data breaches (e.g. encryption). This will mean looking also at your back-up security of data, computer and passwords and identifying new technology to help you comply with the GDPR;

6. Document the procedures you have in place to detect, report and investigate data breaches and let everyone in your business know about your new data protection policy;

7. Consider who in your business will be the person responsible for the GDPR and making sure all employees are aware of the new regulations and ensuring compliance.

CLIENT GDPR REVIEW DOCUMENT

Use this review checklist to highlight areas that you could strengthen ahead of the GDPR.

1. Does the business have a summary of the data it holds and the reasons why;
2. Is there documentation outlining existing data protection and security measures;
3. Is there a list of devices where data is held;
4. Has a review of data privacy notices on the web or terms of business been done;
5. Is there a point of contact for data protection;
6. Has the business got “Cyber” Insurance and would it be beneficial;
7. Is virus and internet protection software up to date;
8. Does the business have a policy regarding personal devices and data;
9. Would the business benefit from an independent data audit;
10. Are there procedures for ensuring any confidential data is encrypted;
11. Has the business sent a memo on data protection to all employees;
12. Are there procedures for handling data requests from clients.

Recommendations: