band hatton button | solicitors
Incorporating Varley Hibbs

Data Protection

What's in Store for Your Client Database and E-marketing?

The quick answer to this is that there are big changes on the horizon next year with the implementation of the snappily titled General Data Protection Regulation (GDPR), which comes into force on 25 May 2018. Although this is European Legislation, it will come into force in the UK regardless of how Brexit progresses.

If your core business involves significant processing of personal data and records (for example healthcare, insurance and financial services etc.) you probably know about the forthcoming changes already, but it is likely that every business operating in the digital age will be affected and everyone needs to be aware of the new rules.

In the UK, the Regulations are policed and enforced by the Information Commissioner's Office (ICO) who are keen to make sure that businesses prepare for the new Regulations and the requirements of them. The ICO has published guidance about preparing now for the changes that become law next May. This is very helpful information that is being updated regularly and you should keep up to date with the material on their website: https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/. It also means that there will be no scope for leniency for procedures to be adopted and to bed in after 25 May 2018. With the power for the ICO to issue fines going up to a maximum of 4% of global turnover, or €40M, whichever is the greater, it is crucially important to make sure that your business is fully compliant well before the GDPR comes into force.

The key requirements of the GDPR are that **informed, explicit consent** is required for all types of personal data processing and direct marketing campaigns. To break that down:

- **Data Processing** means the collection, storage, use and disclosure of information so that covers just about anything as soon as a business receives any personal data about a client/customer.

- **Personal Data** is any information relating to an identifiable individual so it includes the most basic customer/client contact details.

- **Explicit Consent** means that the current usage of opt-out boxes is no longer permitted. There must be a positive opt-in and it must be capable of being easily withdrawn.

- **Informed Consent** requires several things. Firstly, when personal information is collected, the customer must be told how you intend to use that data (this is already the position and it is generally dealt with by way of privacy notices). You must also explain your legal basis for processing the data. Normally, this will be that the customer has consented but additional grounds include that the processing is necessary for the performance of a contract with the customer, a legal obligation or the rather less clear ground that it is necessary to meet "legitimate reasons" – for example to recover a debt owed to you by the customer. The customer must also be told how long the data will be held for and of their right to ask for it to be deleted – this is known as the "right to be forgotten". This means that data storage systems must enable an individual's personal data information to be easily identified, extracted and deleted either within the timescale for retention or on the request of the customer.

The issue of informed consent is particularly difficult if a business collects personal data about children, in which case age has to be identified and consent obtained from a parent or guardian.

As with most systems of regulatory compliance nowadays, all organisations are required to keep records to demonstrate compliance with the Regulations. In most companies this will require written policies and procedures and the appointment of a Data Protection Officer (this is obligatory in some organisations). All organisations will be required to notify the ICO of certain types of data breach and failure to do so will, if that breach is subsequently detected, result in a significantly increased fine.

You must also bear in mind that if you outsource data processing in any way (for example hosted data storage, marketing campaigns etc), you are responsible for ensuring that what they do for you is compliant with the GDPR.

May 2018 might seem a long way off but the consequences of non-compliance with GDPR (not only financial penalties but also reputational damage - as we know from recent high-profile cases) gives a huge incentive for all businesses to make sure that they are ready to meet their obligations and the operational challenges that they bring. We can help your business by reviewing your current operations and systems firstly to make sure that they are compliant, an also to ensure that your data collection, storage and management systems are fit for purpose and won't get you into potentially seriously expensive trouble.

To consider any of these issues further and how they will affect your own business, contact Jon Wilby who is Head of our Litigation Department & Head of Regulatory Compliance.

Jon Wilby
Partner
Direct Tel: 024 7649 3116
Email: JJW@bandhattonbutton.com