



Commercial Briefing

Managing data protection in your business

No matter what your business is, you will inevitably hold a large amount of personal data. This might include information about your customers, contacts, staff, applicants, enquirers, complainants – the list is endless. All of this information must be treated in accordance with data privacy laws which stipulate how personal data can be used. The biggest mistake which people make when they try and deal with data protection legislation is that they often think it stops them using data in many ways. Often this is not the case and it is a question of making sure that the right framework is in place to achieve compliance rather than assuming that the legislation is a barrier to business.

In this bulletin we look at some of the obligations imposed by data protection law and take a high level look at the types of measures which should be implemented to make sure that the personal data which you hold is used in the right way.

What is the data protection legislation about and how does it work?

The Data Protection Act 1998 sets out eight broad principles stipulating how personal data should be used. They cover issues ranging from data retention and security to information provision requirements and data transfers. Although these principles are wide and some say rather vague, they are nonetheless legally binding.

In addition to these general principles, there are a series of other specific rights and obligations as well as offences. Breaches can lead to investigation by the Information Commissioner, fines and even court action not to mention, more commonly than anything, adverse publicity. In the summer of 2005 the Information Commissioner also set up the Regulatory Action Division specifically tasked with taking enforcement action against businesses which fail to comply with data protection legislation.

Some key data protection issues in practice

Notification

All organisations holding personal data (known as “data

Key recommendations

- **Review all instances of data collection for example, job application forms, website pages and so on and put in place fair processing information to explain data uses.**
- **Develop a privacy policy, covering issues such as data security and guidance on how staff should treat personal data in carrying out their duties.**
- **Ensure that a notification is put in**

controllers”) should lodge a notification with the Information Commissioner. This involves maintaining certain details in a public register about how your organisation uses data. There are some limited exceptions to this but in most cases, a notification will be needed. The process is straightforward and can be done by post or online. It is also important to keep an eye on your organisation’s notification as changes in the way in which personal data is used may mean that the notification needs updating.

Data collection

Whenever data is collected, people should be given a clear explanation about what their data is to be used for. This applies irrespective of the way in which data is collected whether in paper format, electronically or over the phone. The explanation or “fair processing information” need not be lengthy or complicated but should give individuals a clear understanding of certain issues including what the data is to be used for, who will have access and whether it will be given to any third parties.

The consent issue

This is often the source of much confusion. There is a misconception that in order to be able to use personal data, it is always necessary to obtain the consent of individuals to those uses. In some cases, this may be required and in many cases it would be advisable but it is not always the case.

Whenever personal information is used, one or sometimes two conditions need to be satisfied. The legislation contains a lengthy list of what these conditions are. Getting consent is just one of them and there are other possibilities. The key is to look at the uses of the data in any given case and ensure that one of the requisite conditions applies. In the vast majority of cases it will be obvious which ones apply but where there is any doubt, take the time to look into these conditions in a little more detail.

Whilst consent is therefore very helpful and often it is advisable to obtain that consent, do not assume that a lack of it will necessarily prevent you from doing what you need to do.

Transferring data from your organisation

Businesses pass information to other organisations on a regular basis and this will often include personal information. To take an example, Company A appoints Company B to provide payroll services on its behalf. This will inevitably mean that Company A provides various staff information to Company B. However, usually Company A will still be responsible for compliance with the data protection legislation. So how does it protect its position when passing this information on?

In this situation, data protection legislation requires that there should be written provisions in place to ensure that the data transferred is treated securely and only used for specified

place and maintained with the Information Commissioner.

- **Review standard form contracts and ensure that data privacy issues are covered, incorporating where necessary, data processor clauses.**

- **Develop a policy on data management to cover issues such as retention periods, security and data cleansing.**

purposes. Therefore, it is key that when transferring or making personal data available to a third party, you ensure that the appropriate contractual provisions are put in place to protect your organisation's own liability.

Data management requirements

Another common misconception is that the data protection legislation requires records to be destroyed so that personal information is not retained unnecessarily. This represents only part of the picture. It is quite legitimate to retain data if there is a true business need for doing so. The real issue therefore is not whether the data privacy law requires data to be destroyed but rather whether business need dictates that it be retained. Another important requirement is that data should not be out of date. Therefore, make sure that you have systems in place to ensure that data is regularly updated.

Security

Data security is a key issue under the data privacy legislation and in all cases personal data must be kept safely and securely. In an age where there is an increasing amount of concern about issues such as identity theft and online fraud, the security of personal information is paramount. Not only will this help you achieve compliance but it will also instil vital confidence in your customers, staff and contacts.

The security measures which are appropriate will vary depending on issues such as the type of data held and its sensitivity, the manner in which it is held and the practical requirements of access and usability.

To discuss how Berg Legal can assist you with these issues, please contact either Stephen Foster, Head of our Corporate and Commercial Department at stephenf@berg.co.uk or Luisa D'Alessandro who is an Associate in the team at luisad@berg.co.uk. Alternatively you can call Stephen or Luisa on 0161 833 9211.

berg legal 35 peter street manchester m2 5bg
t. 0161 833 9211 f. 0161 834 5566 e. help@berg.co.uk
dx 14379 manchester 1 www.berg.co.uk Regulated by the Law Society

The information and opinions contained in this document are not intended to be comprehensive, nor to provide legal advice. No responsibility for its accuracy or correctness is assumed by Berg Legal, or any of its partners or employees. Professional legal advice should be obtained before taking, or refraining from taking, any action as a result of the contents of this document.

