Healthcare providers: Beware of new data protection regulations

Data protection law has been with us since the 1980s. For most businesses it has involved little more than registration with the Data Protection Registrar (now the Information Commissioner) and latterly compliance with the requirements of the Data Protection Act 1998.

25 May 2018 will see a radical change. The General Data Protection Regulations will come into force and all businesses that process personal data must adopt technical measures, procedures and policies to ensure that the regulations are followed and that personal data is kept safe. The onus will be fairly and squarely on the business to demonstrate compliance.

Personal data will be any information about an identified or identifiable individual (a "data subject"). It is processed whenever it is collected stored, organised, transferred, altered or deleted, whether on a computer system or in a manual filing system.

Personal data can only be processed if the data controller (the person or organisation that manages the data) follows the six data protection principles:

1. Processing must be lawful, fair and transparent
2. The data can only be collected for specific , explicit and legitimate purposes
3. The data must be adequate , relevant and limited to what is necessary
4. The data must be accurate and kept up to date – every reasonable step must be taken to erase or rectify inaccurate data
5. Data can be stored no longer than is necessary

In addition the data controller must be able to show that one of the conditions set out in the regulations authorises the processing:

Tel: 0344 967 0793 | Email: info@LA-Law.com | www.lesteraldridge.com

1. The data subject has given consent – which must be freely given, specific and unambiguous and capable of being withdrawn as easily as it was given.

2. The processing is necessary to perform a contract with the data subject.

3. The processing is necessary to comply with a legal obligation.

4. The processing is necessary to protect the vital interests of the data subject– this is a stringent test and should only be relied upon in a real emergency.

5. The processing is necessary for the legitimate business interests of the data controller or someone else and is not over-ridden by the rights of the data subject.

There are more stringent rules about special categories of personal data, such as health data, which may be considered particularly sensitive. The conditions for processing are much more stringent.

There are new rules about engaging someone else to process data e.g. a payroll bureau. There must be a contract dealing with specific matters set out in the regulations designed to ensure that the data processor complies with the regulations and that the data controller can check that it does so.

Data subjects have the right to know what information is held about them. If a data subject access request is made, the business will have one month to provide the information. A data subject can also require all of his personal data in whatever common form the data subject specifies -"data portability".

Any data breach that could result in some form of harm to the data subject such as identity theft or financial loss or if it involves a breach of confidence must be reported to the Information Commissioner within 72 hours – if a breach happens on a Friday morning, the data controller must have systems in place that would enable it to report the breach on Monday! Failure to report could in itself incur a fine.

Many of the headlines have been about the level of fines. The maximum will be the higher of 20 million euros or 4 times annual turnover. In practice warnings or a requirement for an undertaking to improve may be more common, provided that there is evidence of a high level of compliance with the regulations and it has been emphasised that fines will be proportionate. Even so, organisations, including local authorities have been fined amounts in excess of £50,000 under the current regime so complacency could be an expensive option.

This article can only outline the main themes of the new regulations. It is essential to appreciate that the regulations apply to all business use of personal data, no matter how small the business. Advice should be take on compliance. A good starting point is the advice on the website of the Information Commissioner.

Tel: 0344 967 0793 | Email: info@LA-Law.com | www.lesteraldridge.com