BERMANS
Commercial

General Data Protection Regulation: What it means to business

The Regime

The current legislation in relation to data protection in England and Wales is the Data Protection Act 1998 which was derived from the European wide Data Protection Directive (95/46/EC). The General Data Protection Regulation (GDPR) is due to come into force in May 2018. Whilst many of the provisions are already covered by the Data Protection Act, there are important new provisions of which businesses need to be aware.

The first questions many will ask is will it matter if we leave the EU? The answer is that the Regulation, when it comes into force, will be incorporated automatically into law in member states. As it looks likely the UK will still be a member state in May 2018 when the GDPR comes into force, then it will apply without the UK Government having to incorporate it into English law. When the UK exits the EU, the UK Government have made initial plans with each government department to incorporate EU law into English Law pending potential review at a later time, so it will continue to have effect.

The Risk

Currently the maximum fine in the UK for data controllers breaching data protection is £500,000. The GDPR will increase the potential fines to the greater of 2% of annual worldwide turnover or 10 million euros where the Data controller or data processor is in breach of requirements relating to:

- Internal record keeping
- Breaches of data security
- Contracts with third party data processors
- Breach notification, data protection officers
- Data protection by design and default (part of the new regime)

The fines increase to up to 4% of annual worldwide turnover or 20 million euros (whichever is the greater) for breaching:

- The data protection principles
- Conditions for consent of the date subject
- Data subjects' rights
- International data transfers

The Changes in brief

- The burden of showing the data subject has consented to the use of their data is greater
- Businesses will have to show valid consent by the data subject to processing of personal data (a pre-ticked box online, nor general acquiescence of the data subject will not suffice)
- Consent will need to be separate for each type of use of the data
- New rules will apply to use of anonymised data
- Data subjects will in certain circumstances have the right for their data to be removed or for the data subject to be "forgotten"
- The data subject can object to being profiled from information held (for example, sending details of offers your system suggests the subject may be interested in based on their use of your website)

Exchange Station
Tithebarn Street
Liverpool
L2 2QP

Cardinal House
20 St Mary's Parsonage
Manchester
M3 2LY

www.bermans.co.uk

BERMANS
Commercial

General Data Protection Regulation: What it means to business

What you need to do

- Consider appointing a data protection officer if you do not already have one (mandatory in some instances)
- Review your current practices and compliance
- Review your current arrangements with third parties who provide data processing services to you, or to which you provide data processing services
- Business will need to better maintain records of where data comes from, when it was obtained how it is used and how it is processed
- Treat data risk in the same way as health and safety risk assessments, by carrying out Protection Impact Assessments, for example, consider the risks of relevant events such as:
    - Office cleaners having night access to information on systems and paper outside office hours
    - Outside contractors working in the building
    - Contractors working on the IT system
    - External data processing
    - Data leaving the security of the building in laptops or other media
- Maintain a register of all assessments for audit purposes
- Maintain a record of processing activities
- Introduce and maintain processes for reviewing data and recording requests received from the data subject
- Record any requests by a data subject to have their details removed (the right to be forgotten)

Privacy by Design is the concept

In summary Privacy by Design would be that part of your policy whereby changes in the business process are reviewed and potential risks identified and dealt with. It would entail reviewing the way in which personal data is currently processed including obtaining or renewing consent where necessary and considering if retaining the information is justified for in the circumstances.

You should be able to respond to a breach promptly, having in place a policy on how to deal with a breach, including notifying data subjects who are affected. You need to consider whether your documentation provides sufficient details to data subjects in setting out what rights the data subject has and what your obligations are in providing such data.

Bermans would be happy to speak to clients who have concerns on the implications of the GDPR and the client's compliance with the GDPR. For further information please contact Chris McDonough.

Chris McDonough - Partner and Head of Commercial
e: chris.mcdonough@bermans.co.uk
t: 0151 224 0551

Exchange Station
Tithebarn Street
Liverpool
L2 2QP

Cardinal House
20 St Mary's Parsonage
Manchester
M3 2LY

www.bermans.co.uk