



### Key Contact

**Alex Ellerton**  
aellerton@bovill.com

*“Getting data protection wrong can bring commercial, reputational, regulatory and legal penalties...”*

**London office**  
82 Blackfriars Road  
London  
SE1 8HA

**Phone:** 020 7620 8440  
**Web:** www.bovill.com

## DATA PROTECTION AND PRIVACY

June 2008

### Overview

The FSA published in April 2008 a major report on “Data security in financial services”. As the report notes, given a number of recent well-publicised incidents of data loss, *“nobody in the UK can claim ignorance of the risk of customer data falling into the wrong hands”*.

The issue of loss of personal data is only one element however of the broader regulatory requirements in this area. Further, for those financial services firms authorised by the FSA, it is important to develop an integrated response to the broad requirements of more than one regulator. This Briefing Note sets out the main areas of consideration for FSA regulated firms, including the high level requirements under the Data Protection Act 1998 (“DPA”) and the areas of regulatory overlap with the FSA Handbook.

At a time when the related issue of financial crime is high on the regulatory agenda and as greater powers of sanction are about to be given to the Information Commissioner’s Office (“ICO”), firms should take notice of the words of Richard Thomas, the Information Commissioner, quoted in the foreword to the FSA report:

*“Getting data protection wrong can bring commercial, reputational, regulatory and legal penalties. Getting it right brings rewards in terms of customer trust and confidence.”*

### The Data Protection Act 1998

The DPA applies to information that is *personal data*. This includes information that relates to living individuals which may be held in either soft or some hard copy formats. Examples of personal data include information such as name, address, date of birth, opinions about the individual or other information from which the individual can be identified.

The DPA also distinguishes between a *data controller* and a *data processor*. A data controller is a person who “...determines the purposes for which and the manner in which any personal data are, or are to be, processed”. A data processor is a person “...who processes the data on behalf of the data controller”. Processing of personal information includes obtaining, disclosing, recording, holding, using and erasing or destroying personal information. The onus is on the data controller to comply with the DPA Principles in relation to all personal data for which he is the data controller.

“Notable FSA requirements include Principle 3, Principle 6, SYSC and record keeping requirements..”

## The Data Protection Principles

At a time when the FSA’s approach to regulation is focusing more upon high level Principles for Businesses, it is worth recognising the similar approach adopted by the DPA. The eight data protection principles can be summarised as follows:

Personal data shall:

1. be fairly and lawfully processed;
2. be processed only in line with the specified purposes for which it was obtained;
3. be adequate, relevant and not excessive;
4. be accurate and, where necessary, kept up to date;
5. not be kept for longer than is necessary;
6. be processed in line with the rights of the individual;
7. be kept secure; and
8. not be transferred to countries outside the European Economic Area unless the information is adequately protected.

## Rights of a Data Subject

In addition to imposing legal obligations on organisations that handle personal data, the DPA also confers a number of rights upon individuals who are the subject of personal data (“*data subjects*”). One of the most significant is the right to make a *subject access request*. This permits the individual to find out whether information is held about them and if so what it is. Firms must deal with subject access requests promptly and in any case within 40 days of the date of receipt of the request.

Another significant right of data subjects is to prevent data processing for the purposes of direct marketing. Where the individual notifies an organisation in writing that they wish the processing of personal data for direct marketing purposes to cease (or not to begin), the organisation must comply with the wishes of the individual.

## Enforcement: ICO & FSA

There are clearly a number of areas of regulatory overlap when considering the DPA and the FSA Handbook. Notable FSA requirements include Principle 3 (management and control), Principle 6 (customers’ interests), systems and controls requirements under SYSC and record keeping requirements from different parts of the Handbook. When it comes to enforcement however, it has been the FSA which has historically handed down the most significant penalties to firms, generally for breach of Principle 3. Whilst sanctions levied by the ICO have to date been limited to enforcement notices, new legislation will give the ICO power to issue penalty notices and fines.

## Conclusions

The message is clear; data protection is high on the regulatory agenda, with both the ICO and the FSA firmly focused on data security, albeit from slightly different perspectives. Whilst the ICO may be concerned more with the rights of the data subject, the FSA is primarily concerned with ensuring that firms have adequate systems and controls in place to manage any risk in relation to personal data. Criticism that firms are not devoting sufficient resource to data protection matters needs to be countered with prioritisation of the issue on compliance agendas.

### Manchester office

Barnett House  
53 Fountain Street  
Manchester M2 2AN

Phone: 0161 247 8562  
Web: [www.bovill.com](http://www.bovill.com)