

Briefing Note:

Record retention and information governance

Central to any information management or information governance policy is the proper management and retention of information. Yet there is currently a great deal of confusion surrounding the legal and regulatory regimes that govern the retention of documents and records in the United Kingdom. Not only are these regimes designed to provide senior management with the tools to carry out their supervisory obligations; they also provide a vital tool to regulators to enable them to perform their duties of regulatory oversight. This note aims to help dispel this confusion, to illustrate the true nature of the regimes, and the sanctions that are available to regulators should organizations breach the regimes.

Record retention obligations

Information governance means more than the management of personal data. It relates to the management of all relevant information and data irrespective of whether or not that data contains personal data. Yet no organization can claim to manage its information properly unless it also implements a proper information management and assurance policy that addresses information retention correctly. An organization's legal and regulatory obligations to retain records are related directly both to the contents and functions of its records and to that organization's activities. Together these will determine the legal and regulatory regimes which govern how the organisation operates, and how it must retain its records. Corporate governance and information governance are inextricably linked.

What is clear is that, far from being powerless to enforce information retention obligations, the current legislative framework provides ample powers to regulators to enable them to enforce the obligations should they choose to do so. The framework also makes it clear that it is for organizations to determine their retention obligations: it gives them sufficient guidance to do so.

General presumption

There is a general presumption, if not an obligation, under common law for organizations to retain records. This general presumption can be derived easily from the manner in which the Courts deal with evidence when they adjudicate a dispute. Though oral first-hand evidence is the most useful, this evidence is often backed up by or based on records, or indeed presented to explain the contents of records that have themselves been presented as evidence. Records corroborate oral evidence and oral

Points to note:

- 1 Corporate governance and information governance, including proper information management, are inextricably linked
- 2 Organizations' record retention obligations provide regulators with the requisite information they need in order to perform their regulatory oversight of those organizations
- 3 The current legal and regulatory regimes provide sufficient guidance to enable organizations to determine their retention obligations, and sufficient sanctions to enable regulators to enforce those obligations

Documents and records can often be synonymous. There is a difference, and certain statutes, such as the Companies Act 1985 and the Financial Services and Markets Act 2000 do make the distinction. This note will treat the terms 'document' and 'record' as synonymous except where it discusses the statutes mentioned above.

This note does not discuss the obligations imposed by HM Revenue & Customs. These obligations themselves comprise another regime to which organizations must conform. Notice 700 and Bulletin 37 are good starting points.

evidence corroborates the contents of records. Statutes and regulations simply illuminate and specify the records that they require in order for the laws or regulations to operate correctly. The reason for requiring organizations to retain records is simple. Without access to these records, regulators would be prevented from performing their duties of regulatory oversight.

The Companies Acts

If the organization is regulated under the Companies Acts then it must look to the Companies Act 2006 to help it ascertain its record retention obligations under the Companies Acts. Section 1135 imposes a general duty to keep company records, defined in subsection 1134(a) as ‘any register, index, accounting records, agreement, memorandum, minutes or other document required by the Companies Acts to be kept by a company’, and subsection (b) as ‘any register kept by a company of its debenture holders’.

The Act also defines certain specific types of records that it requires companies and their officers to retain. For example, section 248(2) requires a company to retain minutes of all directors’ meetings for at least ten years; section 355 to keep records of company resolutions, meetings, and decisions for at least ten years; and section 388(4) to keep accounting records for a minimum of three years, in the case of a private company, and six years, in the case of a public company, and so forth.

Offence of destroying ‘documents’

The Companies Acts impose a general duty to preserve any and all documents that are relevant to indicate clearly the internal affairs of the company. Section 450 of the Companies Act 1985, as amended by schedule 3 of the Companies Act 2006, imposes this duty implicitly, as the section creates an offence, punishable by up to seven years imprisonment and/or an unlimited fine, should an officer of a company destroy, mutilate, or falsify, or be privy to the destruction, mutilation or falsification of a document relating to the company’s property or affairs. The duty, therefore, is to retain such documents until they are no longer required or can no longer be subject to a legal investigation or challenge. The definition of the term ‘document’ means that this offence covers a wider set of information than the failure to retain company records under section 1135 of the Companies Act 2006. The courts have rightly described section 450 as the ‘heavy artillery of company law’.

The oversight and enforcement of some of the obligations under the Companies Acts are the responsibility of a myriad of agencies that come under the Department for Business Enterprise & Regulatory Reform. Others are the responsibility of the organization itself.

The Acts place a great deal of emphasis of enabling relevant investigators to access information that they require.

The term ‘document’ is defined in section 450(5) of the Companies Act 1985 to include ‘information recorded in any form’.

Section 450 reverses the burden of proof and required defendants to prove that they had no intention to conceal the state of affairs of the company or to defeat the law.

An officer is defined in section 1121(2) of the Companies Act 2006 to include ‘any director, manager or secretary, and any person who is to be treated as an officer of the company for the purposes of the provision in question’.

It is for companies to show that they have retained the information that is required to indicate the state of their internal affairs.

Financial Services and Markets Act 2000

If an organization is regulated under the Financial Services and Markets Act 2000, then it must look to that Act and the regulations passed under that Act to ascertain its record retention obligations under that Act. As

the text of the FSA Handbook makes clear, these record retention obligations are designed to provide the regulator with the ability to confirm that regulated organizations are conforming to their regulatory obligations.

Regulated organizations must comply with the Handbook. Many such organizations point hopefully to schedule 1 of the New Conduct of Business Sourcebook (COBS), a component of the Handbook, as a definitive list of records that they should retain, their argument being that if they do not produce a record set out in the table in schedule 1 then they have no record retention requirements. A simple reading of this schedule shows that this argument is false. Indeed Schedule 1 of COBS states bluntly '[the table] is not a complete statement of those requirements and should not be relied on as if it were.'

Offence of destroying 'documents'

Section 177 of the Act sets out an offence that is similar to that set out in section 450 of the Companies Act 1985. Again this offence refers to 'documents' which, as with section 450, are defined widely as including information recorded in any form. The main difference between this offence and the offence under the Companies Acts is that, whereas the amended section 450 imposes a penalty of up to seven years, the offence under section 177 currently carries a penalty of only two years.

Rule 9.1.1 of the Senior Management Arrangements, Systems and Controls sourcebook (SYSC), for example, makes it clear that an organization must arrange for orderly records to be kept in order to enable any relevant competent authority under MiFID to monitor the organization's compliance with its obligations under the regulatory system.

COBS reminds organizations of the general record keeping requirements set out in SYSC.

The definition of 'document', set out in section 417, goes further than the definition in the Companies Act 1985, and states that 'in relation to information recorded otherwise than in legible form, references to its production include references to producing a copy of the information in legible form'.

Section 177 reverse the burden of proof in the same manner as section 450 of the Companies Act 1985.

Data Protection Act 1998

It is a myth to suppose that the retention of records is governed only by, or primarily by, the Data Protection Act 1998. The reality is more complex. The Act only comes in to effect where records contain personal data, and it applies only to those records. The Act imposes controls on how the organization may handle those records, and on what personal data that organization may process.

The Act does not prevent or excuse organizations from retaining records to meet their legal and regulatory record retention obligations. The Act makes this clear. So too does article 7 of the Data Protection Directive, subsections (c) and (f) of which refer directly to the ability to process data to meet the data controller's legal obligations. The Act simply requires organizations to process personal data lawfully and to destroy any records that contain personal data once, and only once, their need to retain those records to fulfil their legal obligations ends. Organizations must implement proper information management and assurance policies in order to be able to conform to this requirement. This regime differs from those discussed above in one important aspect: it does not specify what records an organization is required to keep. Rather it controls what personal data an organization may process and how it must do so.

Directive 2002/58/EC, the Directive on privacy and electronic communications, also makes it clear that there is no dichotomy between record retention and data protection.

Regimes operate concurrently

The discussion above highlights four regimes which organizations need to keep in mind when looking at their record retention obligations. The regimes outlined above are not mutually exclusive, but operate concurrently. Each of these regimes defines obligations that the organization must satisfy, regardless of whether or not the organization also comes within another regime. Each of these regimes is policed and enforced by different government departments or agencies. This means that an organization and its records can therefore come under the jurisdiction of different departments or agencies, each of which will police and enforce its own regime independently of the others.

For example, a company will not only fall within the general duty under common law, but will also need to retain its records in line with the requirements of the Companies Acts. If it is regulated by the Financial Services Authority then it will also have to satisfy the requirements of the Financial Service and Markets Act and the FSA Handbook. Where its records contain personal data, the company will need to ensure that it complies with the Data Protection Act with regards to those records in addition to its other obligations.

An organization that is not regulated under the Companies Acts, but which is regulated by the Financial Services Authority will have to satisfy the requirements of the Financial Service and Markets Act and the FSA Handbook. Again, where its records contain personal data, the organization will need to ensure that it complies with the Data Protection Act with regards to those records in addition to its other obligations.

Conclusion

Record retention is a fundamental component of any information governance practice. It provides the necessary information to senior management to enable them to perform their supervisory duties. It enables regulators to perform their regulatory oversight duties.

An organization's activities will subject it to various legal and regulatory obligations, the nature of which will depend on its activities. These will all impact on the organization's record retention obligations. They will also mean that the organization will be subject, where relevant, to the jurisdiction of several government departments and agencies, from the Financial Services Authority to the myriad of agencies under the Department for Business Enterprise & Regulatory Reform.

© 2008, Kalypton Limited. All rights reserved
www.kalypton.com

Registered in England & Wales No. 04288948
Registered office:
Crown House
37 High Street
East Grinstead
West Sussex
RH19 3AF
United Kingdom