

Making Sense of Data Law White Paper

A review by InTechnology of legislation and regulation concerning data storage in the UK and Europe

Introduction

The retention of data has become one of the most pressing issues facing business today. It has forced itself from the back office to the boardroom as governments and international bodies cast an increasingly complex web of laws, regulations and standards to ensnare the unprepared.

By some counts, there are over 120 laws affecting data retention in the UK alone. Many have differing purposes and place conflicting demands on business. It is small wonder that organisations as diverse as police authorities and energy regulators have demonstrated confusion over how to comply with the law.

By early 2004, Government and regulators had recognised the need to improve this understanding. Industry-specific guidelines and codes of practice are being encouraged. Heavily regulated sectors such as financial services, local and central government already have standards to which they must comply; the most comprehensive and universally useful of these being from the Public Records Office.

While focussing on the complexity of data legislation, many commentators have overlooked the fundamental common law duty to preserve all documents that could be required in a court of law. Company directors and senior managers could be held personally liable for their organisation's inability to produce relevant information, whether it was deleted, inadequately stored, or stolen.

Some lawyers who specialise in this area are advising clients that rather than deleting information at the earliest opportunity or introducing expensive and unreliable sorting regimes, the most prudent option is to store all data with appropriate safeguards:

- Data protected physically (anti-tamper seals on equipment, for example), and electronically, by encryption.
- Access to data strictly controlled with a formal procedure in place.
- Strict audits that record all access to and any alteration of data.

In the meantime, while closely monitoring regulatory and legislative developments, those engaged in the storage and processing of information would do well to heed the UK Information Commissioner's recent advice: "Organisations must use their own judgement to balance what they want or need to do against the need to safeguard the privacy of individuals and to ensure their personal information is handled properly."

This paper outlines the principal legislation, regulations, standards and guidelines concerning data retention in the United Kingdom and Europe, both current and impending. It has been drawn from a wide variety of sources but does not constitute legal advice. Organisations reviewing their data retention requirements should seek appropriate legal counsel.



Background

Data retention concerns everyone and covers more or less all information. Whether an organisation is in the public or private sector, quoted or not, if it has any type of electronic record management system then the rules apply. This is especially true as existing paper records are digitised and new records originated electronically. Unwanted files can no longer be simply deleted, especially in the financial or healthcare sectors.

In the United States, the Sarbanes-Oxley Act obliges companies to keep business information, including some e-mails and voice-mails, for several years and stipulates that the data should be retrieved easily. The new Basel II capital accord will require financial services companies to store a vast amount of customer data so they can reduce the amount of capital set aside to cover risks.

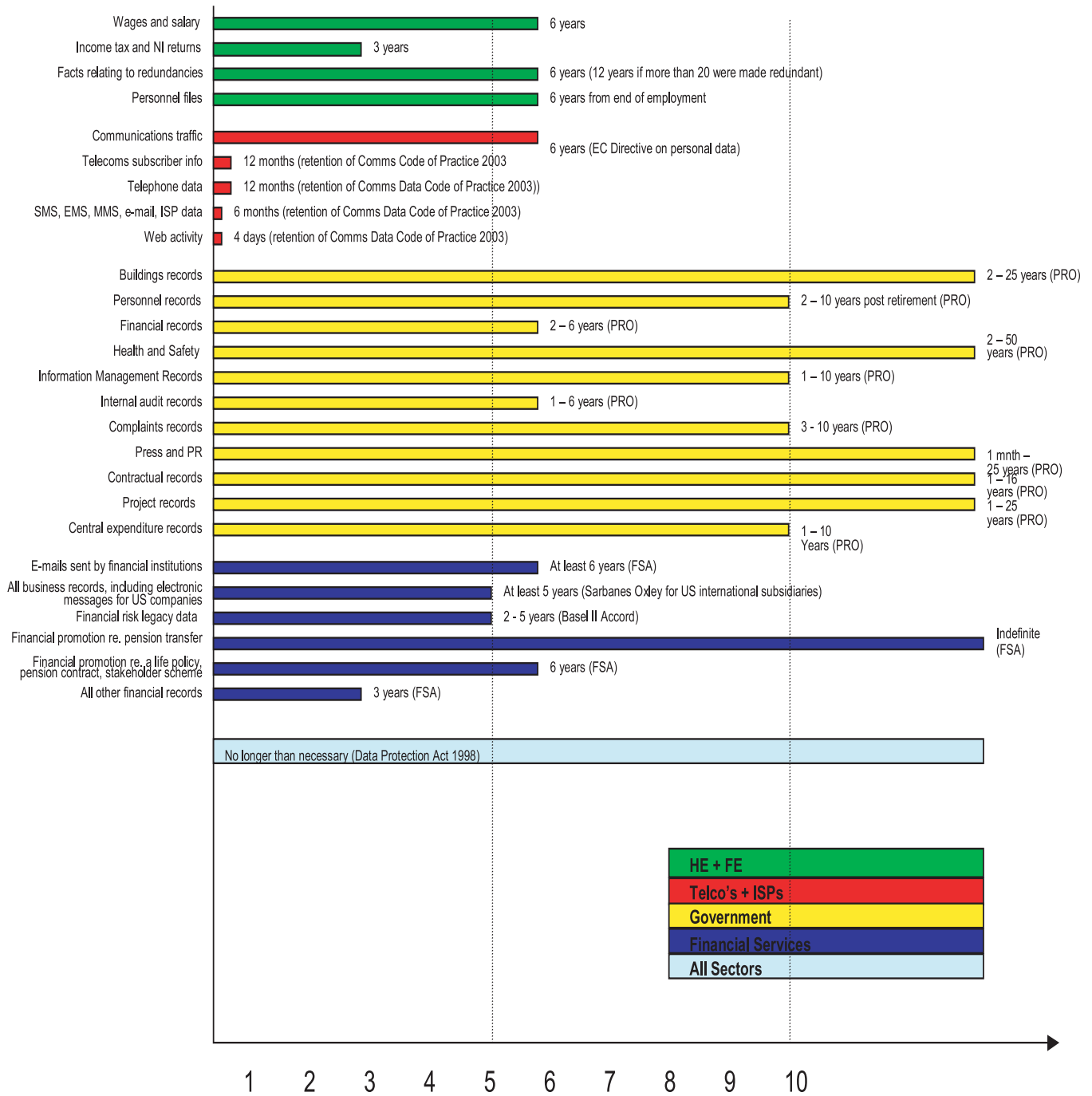
In the United Kingdom, Europe and globally, restrictions on the type of data stored, the uses it is put to, and the time it must or can be retained have put enormous pressure on organisations to comply. But while laws and regulations make retaining information mandatory, there are obvious business benefits to be gained from better access to and control over data resources. Many organisations are already working to implement compliance solutions that will deliver true transparency through real-time monitoring and fast, continuous business process improvement. A recent PeopleSoft survey in the United States revealed that 65% of respondents are seeking to leverage their compliance initiatives to achieve process improvements and competitive advantage.

Organisations therefore need to look beyond mere compliance. But if they are to make the correct strategic decisions, they must first understand the complex driving forces behind much data legislation. Originally conceived to protect the individual's right to privacy, later laws seek to enforce good corporate governance and accountability. Most recently, governments have co-opted business in the war against terrorism and international crime, requiring companies to store data in a readily accessible form for longer than previously allowed.

Despite criticism from industry and civil liberties groups on the grounds of cost, efficiency and human rights, the Retention of Communications Data Code of Practice came into force in the UK in December 2003, allowing companies to voluntarily retain data for up to 12 months. The government is understood to be considering offering £20m over five years to the whole ISP industry to compensate for the cost of retaining and retrieving data over and above normal business needs. At the same time, it was reported that America Online alone had spent £15.8m on systems to store and retrieve customer data for just three months.



SUMMARY OF UK DATA RETENTION REQUIREMENTS



Source: InTechnology, April 2004



How big is the challenge facing private and public sector businesses and how prepared is the UK to face it?

Electronic mail has become an essential part of working life. Eighty percent of business people now believe it to be a more important means of communication than the phone, according to a recent survey by the META Group. Industry analyst IDC predicts that by 2006 the number of e-mails sent daily will exceed 60 billion worldwide, almost doubling the 2002 figure of 31 billion. In 2004, most organisations will see mailbox increases of around 48%, it says.

E-mails, Powerpoints and other documents are often termed "reference data". Unlike structured data such as databases, which have been the focus of storage systems until now, reference data is far harder to manage. Companies increasingly need systems and storage devices that enable them to archive business e-mails in a systematic manner, facilitating the easy retrieval of specific messages when required.

Analysts at The Enterprise Storage Group see a 92% compound annual growth rate (CAGR) in reference data between 2001 and 2006, accounting for over half of all stored data by 2007. The volume of data subject to data retention rules globally will increase at a CAGR of 64% between 2003 and 2006, according to ESG, with the life sciences industry showing the fastest growth of 96% CAGR.

With many corporate decisions now taken online, there is growing regulatory pressure to store and audit e-mail. The latest accounting standards, for example, require companies to explain how decisions were reached. The law even extends to instant messaging, now a significant component of online communication. A Vanson Bourne Research survey revealed that IM is widespread in half of the UK's corporate and investment banks. But just how compliant or prepared are they?

E-mail storage has become an important issue within the financial sector. The Financial Services Authority (FSA) requires all financial institutions to store all business e-mail sent and received for up to six years, some indefinitely. Yet a 2002 study by the Information Commissioner reported that a staggering 83% of banks failed to comply fully with the Data Protection Act. Forty-five percent of businesses that agreed to take part in the study, and 55% of those that refused, fell short of compliance.

Early results from a Department of Trade and Industry study, to be published in April 2004, show that data back-up procedures among UK companies also give cause for concern. The survey of 1,000 companies of all sizes - conducted as part of the DTI's 2004 Information Security Breaches Survey - found that two-thirds of large businesses suffered an incident where they had to restore significant data from back up during the last year. Around half of the businesses that had a systems failure or physical theft suffered major disruption, leading 95% of firms to establish some sort of back up. Only a third of businesses store their back-ups off site, and less than 20% back up their desktops. Only eight percent of companies have tested their disaster recovery plans.



How Big is an Exabyte?

Kilobyte (KB)	<p><i>1,000 bytes OR 10^3 bytes</i></p> <p>2 kilobytes: a typewritten page. 100 kilobytes: a low-resolution photograph.</p>
Megabyte (MB)	<p><i>1,000,000 bytes OR 10^6 bytes</i></p> <p>1 Megabyte: a small novel OR a 3.5 inch floppy disk. 2 Megabytes: a high-resolution photograph. 5 Megabytes: the complete works of Shakespeare. 10 Megabytes: a minute of high-fidelity sound. 100 Megabytes: 1 metre of shelved books. 500 Megabytes: a CD-ROM.</p>
Gigabyte (GB)	<p><i>1,000,000,000 bytes OR 10^9 bytes</i></p> <p>1 Gigabyte: a pickup truck filled with books. 20 Gigabytes: a good collection of the works of Beethoven. 100 Gigabytes: a library floor of academic journals.</p>
Terabyte (TB)	<p><i>1,000,000,000,000 bytes OR 10^{12} bytes</i></p> <p>1 Terabyte: 50,000 trees made into paper and printed. 2 Terabytes: an academic research library. 10 Terabytes: the print collections of the US Library of Congress. 400 Terabytes: National Climactic Data Center (NOAA) database.</p>
Petabyte (PB)	<p><i>1,000,000,000,000,000 bytes OR 10^{15} bytes</i></p> <p>1 Petabyte: 3 years of NASA Earth Observing System data (2001). 2 Petabytes: all US academic research libraries. 20 Petabytes: production of hard-disk drives in 1995. 200 Petabytes: all printed material.</p>
Exabyte (EB)	<p><i>1,000,000,000,000,000,000 bytes OR 10^{18} bytes</i></p> <p>2 Exabytes: total volume of information generated in 1999. 5 Exabytes: all words ever spoken by human beings.</p>

Source: "How Much Information?" 2003; University of Berkeley
School of Information Management and Systems



1: Data Protection Act 1998

The current data protection regime in the UK was established by this Act. Its principal aim is to protect individuals' privacy and to ensure that they have access to and can correct information held about them. The Act has eight central principles. Data handlers must ensure that data is:

1. Fairly and lawfully processed
2. Processed for limited purposes
3. Adequate, relevant and not excessive
4. Accurate
5. Not kept for longer than is necessary
6. Processed in line with individuals' rights
7. Secure
8. Not transferred to countries without adequate protection

The Information Commissioner may serve enforcement notices on companies found to be violating these principles.

Personal data—any information that may identify a living individual.

Many sorts of information can identify an individual. The definition of 'sensitive data' includes information about a person's ethnicity, religious belief, health, etc. Such data may only be collected under precisely defined circumstances.

Websites that collect personal data must be listed on the Data Register.

The Data Register is maintained by the Information Commissioner and lists all companies in the UK that process personal data, defined as Data Controllers.

Personal data must be collected, processed and stored securely.

All collection and transmission of personal data must be encrypted, using HTTP rather than HTTPS, or it is breaking the law.

The extent and use of personal data must be declared to individuals before collection.

Companies must state the information required and its purpose, including to whom it may be passed and may not 're-purpose' data after collection.

Only personal data necessary for processing may be used.

A company may not provide more information to a third party than is necessary.

Individuals have the right of access and control over information held about them.

Within 40 days of the access request by an individual, companies must provide full copies of all records kept (with unintelligible terms explained). Individuals may also request that information about them is corrected, blocked or erased.

The Act enshrines worthy principles but is often vague on the specifics. For example, it requires that information should be kept "no longer than necessary" without giving any precise guidelines.

2: Anti-Terrorism, Crime and Security Act 2001/ Regulation of Investigatory Powers Act 2000

The Anti-Terrorism, Crime and Security Act (ATCS) 2001 contains provisions that allow communications service providers (CSPs) to retain data about their customers' communications for national security purposes.

The Regulation of Investigatory Powers Act 2000 is concerned with the interception of communications, the disclosure of communications data, the carrying out of surveillance and related investigations by Government and State agencies.



The Retention of Communications Data Code of Practice prescribes maximum retention periods for communications and traffic data:

- Subscriber information and telephony data are to be retained for a maximum of 12 months,
- SMS, EMS, MMS data, e-mail data and ISP data for a maximum of six months;
- web activity data for a maximum of four days.

In comparison, the London Internet Exchange (LINX) current best practice on traceability recommends that ISPs retain log data for three to six months.

Some commentators believe that because the scheme is voluntary it will be applied inconsistently and that compulsion will be necessary. The Government stresses that a 'double lock' safeguard would only grant access to certain types of information, such as itemised telephone call records, after prior approval by a judicial independent third party, such as the Interception of Communications Commissioner.

3: The Privacy and Electronic Communications (EC Directive) Regulations 2003

These regulations give greater privacy rights by creating new obligations for businesses that use mobile phones and the internet in direct marketing, including:

- An opt-in regime for direct marketing to individuals by SMS, e-mail and other electronic communications.
- Requiring those who use cookies on their web sites to provide certain information to users and a means to decline cookies.
- Allowing use of traffic and location data for value added services, if subscriber consent is first obtained.
- Giving subscribers the right to refuse to be included in a public directory.

Non-compliance with the regulations may result in the offending organisation having to pay compensatory damages.

4: Other Statutes

Police Act 1997

Part IV of the Police Act deals with criminal records certificates, allowing data sharing for pre-employment background checks. It is currently being scrutinised by the Bichard Inquiry into the Soham murders.

Human Rights Act 1998

This incorporates the European Convention on Human Rights into UK law. See European Law, Article 8 of the Charter of Fundamental Rights.

Freedom of Information Act 2000

The FOI makes provision for the disclosure of information held by public authorities and persons providing services to them. From January 2005, public bodies must deal with individual requests for information, normally within 20 working days. The Lord Chancellor's Department has issued two codes of practice on the duties of public authorities under the Act and the management of records.



Companies Act 1985 update

The Companies (Audit, Investigation and Community Enterprise) Bill is currently at the Committee stage in Parliament. It will tighten the regulation of auditing and increase powers to investigate companies. Company directors will be required to state that they have not withheld information and courts may interpret the inability to produce evidence as contempt of court.

Civil Contingencies Bill

This will update emergency legislation relating to terrorist incidents and major natural disasters. It will oblige organisations like energy utilities and transport companies to share information with emergency planners. Draft regulations and guidance will include business continuity planning, information sharing, and emergency planning. After further public consultation, the Bill is expected to become law in early 2005.

5: European Law

The key European Union Directives are:

Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data - 1995

This is the "framework" European data protection Directive. It concerns the EU and the European Economic Area and consists of rules about the provision of prior information, data quality, criteria for fair and lawful processing, data security, data exports and imports, data subject rights and the obligations of Member States. Most European law is based on this Directive.

Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector - 2002

This and the 1995 Directive require traffic data to be erased or anonymised at the end of the communication except for information required for billing purposes. This information can be retained for the period in which the bill can be disputed or the fee due pursued: usually six years in the UK.

Another major plank of this European framework is Article 8 of the Charter of Fundamental Rights of the European Union - 2000 which proclaims:

- Everyone has the right to the protection of personal data concerning him or her.
- Such data must be processed fairly for specified purposes and with the consent of the person concerned or another legitimate legal basis laid down by law.
- Everyone has the right of access to data that has been collected concerning him or her.
- Everyone has the right to have such data rectified.
- Compliance with these rules shall be subject to control by an independent authority.

Proposed EU Transparency Directive

This Directive aims to enhance transparency in EU capital markets. It would establish rules for companies listed on EU stock markets to disclose periodic financial reports and major shareholding changes. There are similar requirements for bond issuers. The proposal is part of the Commission's Financial Services Action Plan that aims to create a single European financial services market by 2005. Approved by the European Parliament at the end of March, the Directive must now be agreed by EU finance ministers and could come into effect by the end of 2005.



6: Basel II—the new Capital Accord

A new framework for international financial regulation, Basel II is intended to mitigate the risks that affect modern financial markets. It will update capital charges contained in the first Basel Accord, agreed in 1988, by making capital requirements -- the percentage of capital that banks have to keep to issue loans -- reflect risk more accurately. The scale and complexity of the data requirements will be enormous, requiring between two to five years of legacy data to create the required picture of organisational exposure. This could be achieved using a data warehouse with queries formulated by data mining tools. The Financial Services Authority's assumed implementation date is 31st December 2006.

7: Sarbanes-Oxley Act 2002

A response to the Enron and WorldCom financial scandals, Sarbanes-Oxley aims to protect shareholders and the general public from accounting errors and fraudulent practices. The Act is administered by the Securities and Exchange Commission (SEC) which sets deadlines for compliance and publishes rules of requirements. The Act affects all US companies and their subsidiaries worldwide. The deadline for compliance is June 2004.

Sarbanes-Oxley is not a set of business practices and does not specify how a business should store records; rather, it defines which records are to be stored and for how long. The Act states that all business records, including electronic records and electronic messages, must be saved "for not less than five years". The consequences for non-compliance are fines, imprisonment, or both.

Everything from financial records to e-mail is affected, particularly data management, maintenance and archiving. As under Basel II, companies must invest in storage that makes available all data relevant to their business activities, including proof that the processes that led to the creation of the data conform to the rules. Private companies that anticipate acquisition by public companies will need to comply with Sarbanes-Oxley's requirements on internal controls.

8: Standards, Guidelines, and Codes

BS7799-British Standards Institution

ISO17799-International Standards Organisation

BS7799 is the most influential, globally recognised standard for information security management. Part 1 contains guidance and explanatory information. Part 2 provides a model that can be used by businesses to set up and run an effective Information Security Management System.

BS7799 is divided into ten main sections covering security policy, organisational security, asset classification and control, personnel security, physical and environmental security, communications and operations management, access control, system development and maintenance, business continuity management, compliance with relevant national and international laws, professional standards, and any processes mandated by the Information Security Management System.

Part 1 was released as ISO17799 and Part 2 is due for conversion to an ISO standard over the next few years.



BSI IT Security Baselines

Bundesamt für Sicherheit in der Informationstechnik (BSI) is a German organisation tasked with producing standards for IT security. They have an English version of the BSI Baselines that are designed to:

- Help solve common security problems rapidly
- Raise the security level of IT systems and
- Simplify the creation of IT security policies.

COBIT

The Control Objectives for IT (COBIT) were designed to act as a control framework and a supporting toolset. COBIT has a range of products including a Management Guide, Control Objectives and related support material. COBIT is aimed at audit professionals but provides a strong framework for larger organisations.

GASSP

The Generally Accepted System Security Principles (GASSP) were assembled by the Computer Security Institute to meet US Government needs. They are based on multiple sources, including OECD Guidelines and BS 7799.

GMITS

Guidelines for the Management of IT Security (GMITS) also known as ISO/IEC TR 13335 1-4 were designed to provide comprehensive guidance on information security management.

Information Technology Infrastructure Library (ITIL)

ITIL was assembled by the Central Computer & Telecommunications Agency (CCTA). It provides a foundation for the management of IT infrastructure and for the management of information security. It describes best practices in information security management and related practices. The CCTA is an executive agency of the UK Office of Public Service.

International Accounting Standards/International Financial Reporting Standards

Set by the independent International Accounting Standards Board, the European Union has legislated that all 7,000 EU-listed companies must use these standards by 1st January 2005.

The DTI may extend these requirements to private companies. Compliance requirements will differ from sector to sector, but will be more stringent for financial services. The legislation could necessitate dual reporting, according to the old standards and the new. Companies will, in effect, be running two accounting systems. Yet to be fully endorsed by Brussels, many major European banks may adopt the standards early to tie in with the US which has similar fair value accounting.

The Combined Code and the Turnbull Report (UK)

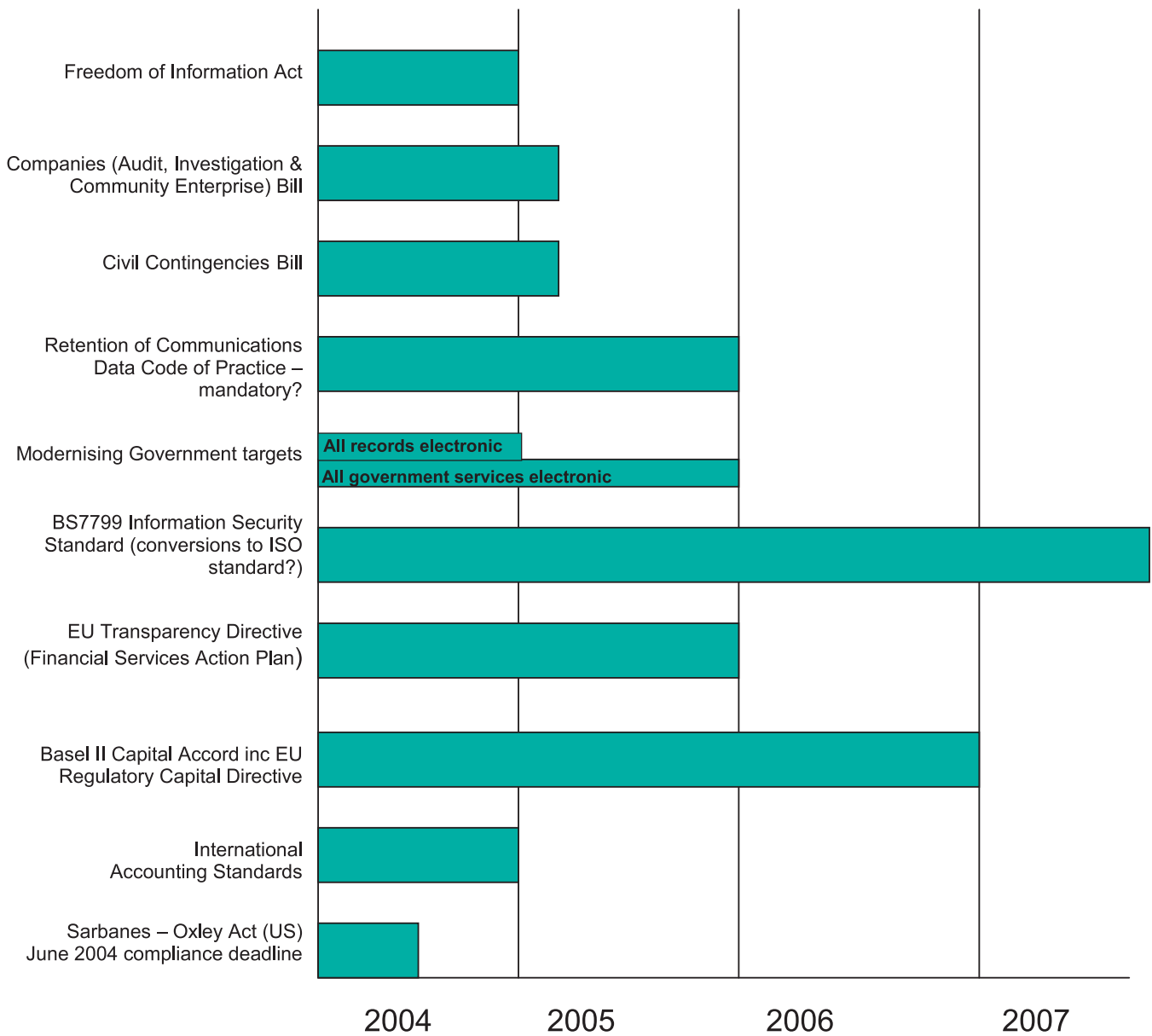
The Combined Code requires companies to annually review "all controls, including financial, operational, compliance and risk management." The Turnbull Report explicitly requires boards, on an ongoing basis, to identify, assess and deal with significant risks in all areas, including information and information technology.

Public Records Office (PRO) Guidelines

The National Archives (PRO) provides advice and guidance to records managers across central government. This covers the entire life cycle of public records, in whatever format, from creation through to destruction or transfer to the National Archives.



In the Modernising Government White Paper, all government organisations were set a target to manage their records electronically by 2004. This is a demanding task and the National Archives is now working to ensure it is met. The amount of paper currently held by central government is larger than ever and needs to be properly managed.



Source: InTechnology, April 2004



Conclusion

Compliance with data protection legislation is not an option. Big or small, public or private, organisations, their directors and senior managers are all bound by common law and a raft of rules and regulations. There are no grey areas. No excuses. Anyone with responsibility for managing data, from the backroom to the boardroom, has a duty to know what the law requires and what their organisation needs to do to comply. To hide behind the fog of confusion that has descended on some areas of data law is not an option, either. Just ask Humberside Police or the power company regulator.

The best advice from leading lawyers who specialise in this increasingly complex area of the law is simple. Protect your data physically and electronically. Put strict procedures in place to control access to that data. And tightly audit any access or alteration to that data.

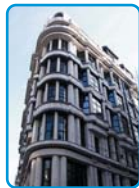
Disclaimer

Customers/clients are responsible for ensuring their own compliance with legal requirements. It is the customer/client's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer/client's business and any actions the customer/client may need to take in order to comply with such laws. InTechnology plc does not provide legal advice or represent or warrant that its services, products or advice whether provided implicitly or explicitly, will ensure that the customer/client is in compliance with any law.



Head Office
Nidderdale House
Beckwith Knowle
Harrogate
HG3 1SA

T: +44 (0)1423 850000
F: +44 (0)1423 877565



London Office
1 Threadneedle Street
London
EC2R 8AW

T: +44 (0)20 7786 3400
F: +44 (0)20 7786 3444



Reading Office
Building 1320
Arlington Business Park
Theale, Reading
RG7 4SA

T: +44 (0) 1189 711 511
F: +44 (0) 1189 711 522

W e b : www.intechnology.co.uk

E m a i l : info@intechnology.co.uk

