

# White Paper



## EU Compliance and Regulations

for the IT Professional

...data loss is now a legal issue  
and IT professionals need to be  
aware of their responsibilities

Nigel Stanley

This paper is sponsored by

**SOPHOS**

## Contents

---

<b>Executive summary</b>	<b>1</b>
<b>Objectives of this paper</b>	<b>2</b>
<b>Introduction to European Compliance issues</b>	<b>3</b>
<b>Summary of relevant Acts and Regulations</b>	<b>5</b>
EU Data Retention Directive 2006/24/EC	5
Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995	6
EU Capital Requirements Directive/Basel II Accord	7
Payment Card Industry Data Security Standards (PCI DSS)	8
The Rules Governing Medicinal Products in the European Union and Commission Directives 91/356/EEC, 2003/94/EC, and 91/412/EEC	9
MiFID - The Markets in Financial Instruments Directive	10
Statutory Audit and the Company Reporting Directives (“EuroSox”)	11
Data Protection Act 1984, amended 1988 (UK)	12
Freedom of Information Act (UK)	13
Regulation of Investigatory Powers Act 2000 (RIP or RIPA) (UK)	14
Federal Data Protection Act (November 2006) (Germany)	15
Freedom of Information Act (2005) (Germany)	16
Data Protection Act (2004) (France)	17
Law on Access to Administrative Documents (1978/2005) (France)	18
Control of Insurance Undertakings (1995) (Belgium)	19
Law of Privacy Protection (1998) (Belgium)	20
Money Laundering and Finance of Terrorism Law (1993) (Belgium)	21
Supervision of the Financial Sector Law (2003) (Belgium)	21
Consumer Credit Law (1992) (Belgium)	21
Personal Data Protection Act (2000) (Netherlands)	22
Protection of persons with regard to the Processing of Personal Data (2002 and 2007) (Luxemburg)	23
Personal Data Protection Code (2004) (Italy)	24
Civil Code section 2214 and 2220 (Italy)	25
Protection of Personal Data (1999) (Spain)	26
Commercial Code (Spain)	27
Personal Data Act (1999) (Finland)	28
Personal Data Act (1998) (Sweden)	29
Accounting Act SFS 1999:1078 (Sweden)	30
Public Records Act SFS 1990:782 (Sweden)	31
<b>EU Compliance—Summary Comparison Table</b>	<b>32</b>
<b>Other significant legislation and regulations</b>	<b>34</b>
<b>Strategies for managing information technology compliance</b>	<b>35</b>



## Executive summary

---

The protection of data as it rests, transacts or journeys through computer systems is seen as a major component of good corporate hygiene. As well as protecting organisations from reputational risk and damaging losses, failure to protect this data can now result in both corporate and personal criminal prosecutions.

The growth of compliance requirements over the past few years has sometimes been seen as a US-based phenomenon as regulations are implemented to address various corporate failures and scandals over the past decade or so. In fact, compliance, rules and regulations to protect data stored by EU-based organisations can be just as onerous as those originating from the US.

This paper highlights key directives and legislation as it affects the member states of the EU.

Data loss prevention technologies are now seen as crucial tools to help address regulatory and compliance requirements. These technologies include data encryption, device control, application control and content inspection, which are now all being deployed by organisations that realise the consequences of unintended data loss.

A data loss incident should no longer be seen as an unfortunate accident; now it will be accompanied by significant reputational risk and the possibility of legal action against the organisation or, even, executives personally.

Clearly, and quite rightly, data loss is now a legal issue and IT professionals need to be aware of their responsibilities.

## Objectives of this paper

---

This paper highlights key directives and legislation within the European Union that have an impact on IT security practitioners, especially those responsible for the safe storage of data using data loss prevention technologies.

EU legislation is vast and constantly changing. This paper is not designed to be an exhaustive review of every law and directive applicable across the EU and is not to be construed as legal advice. Where appropriate, national legislation has been highlighted as it applies to the larger members of the EU.

By reading this paper, IT security practitioners will gain an awareness of legal factors that affect them today. It is strongly advised that any organisation requiring further explanations or details of appropriate legislation consult qualified legal practitioners.

## Introduction to European Compliance issues

The EU, or European Union, currently comprises 27 member states. It was established following the Maastricht treaty in 1993, which renewed the union originally called the European Economic Community or EEC. The EU generates approximately 30% of worldwide GDP and has around 500 million citizens.

The EU has developed a system of laws that apply to the movement of goods and people and the creation of a single trading entity. Each member state is subject to both EU and their own locally created national laws. There are countries that form part of Europe geographically but do not have membership of the EU, for example Switzerland. These countries are therefore not subject to EU-based legislation and have not been considered for inclusion in this paper.

As part of its remit, the EU has created business-related compliance and regulatory requirements, including laws that cover the safe keeping and management of data in computer systems. Failure to comply with these laws can result in criminal proceedings and prosecutions, so any organisation operating in the EU needs to take such laws as seriously as those developed by individual nation states.

### European Union compliance structure

When considering EU law it is important to understand the structure of the EU and how laws are enacted.

The EU Council represents national governments and is a council of ministers run by a 6-month rotating presidency. National ministers attend meetings as appropriate to their portfolio. The European Parliament is elected every five years by citizens of the member states. Members of the European Parliament have geographically-based constituencies that are generally larger than those for members of a national parliament.

The European Commission acts as a civil service and drafts new laws, which are passed to the European Parliament for discussion and enactment. The EU is based on a rule of law, which is laid down in a series of treaties and directives. These then become a collective legislative act of the EU, which are then enacted in member state laws. If a member state fails to enact a suitable law then action can be taken against that state in the European Courts of Justice, which is the judicial institution of the Community.

### The business benefits of compliance

Aside from the obvious dangers of non-compliance, which can result in all-too-public prosecutions, what are the tangible business benefits of adhering to regulatory compliance and rules?

Running any type of organisation can be complex and time consuming, and pressures exist every day to generate more profits by marketing and selling goods. IT is a business enabler and, as such, needs to be present to help an organisation make money, save time or save money. If an IT system fails to meet one of these objectives then its role, broadly, needs to be reconsidered. In the past, IT security was placed a long way down the list of priorities and it is only in the past few years of internet enablement that the sheer scale of data security violations has been acknowledged.

In the days of IT before the proliferation of the PC, data leaks were unheard of outside the scope of targeted espionage as the systems needed to read stolen data were so specialised. Now anyone can read terabytes of corporate data at home on their own PC.

An organisation's reputation is now a vital part of its marketing mix and, as such, needs to be protected as much as any other core company property. In the past, scares such as contaminated products could be dealt with relatively quickly by removing products from shop shelves. Now, data leaks are far more personal as millions of confidential customer records can be lost in seconds. Such a personal affront will create a lot of disharmony in a customer base, and needs to be prevented as a matter of urgency.

The costs of recovering from a data loss incident have been well publicised in a number of reports. Disclosure rules now exist in some US states, so that if personal data has been leaked then the organisation concerned is legally obliged to inform those potentially affected. There are ongoing discussions across the EU, both nationally and at a European level, to determine if such legislation should be implemented in this region.

Adherence to compliance requirements can assist an organisation trying to achieve funding or a possible sale. During a due diligence process non-compliance will rapidly be uncovered leading to discussions concerning the overall

## Introduction to European Compliance issues

---

management of the business and the hunt for additional problem areas. The knock-on effect to corporate valuations and exit multiples can have a direct, profound affect on the principals.

### Preventing data leaks

Data can leak from an organisation via two routes; the incompetent and non-malicious and the competent and malicious. The former occurs when data is accidentally emailed, copied, discarded or otherwise incompetently lost. The latter occurs when deliberate data theft is carried out by a suitably trained and motivated individual.

There are a number of solutions that can be deployed to help prevent data loss:

- Content inspection tools can monitor flows of data in real time to determine if sensitive data is at risk of leakage. Using intelligent rules, content is scanned and, coupled with data origin and data destination information, decisions are made dynamically to establish if data is at risk of being compromised.

- Data encryption is the process of taking everyday readable data and turning it into unreadable gibberish to anyone that does not have legitimate access to it. If data is encrypted and the decryption keys suitably protected then data leaks will not violate any current EU-based legislation or regulation. After all it is only gibberish that has been leaked, not clear text data.
- Application control can monitor a network and detect if inappropriate software is being installed or configuration changes are being made that could help data to leak.
- Device control protects against unauthorised use of removable media, such as USB memory sticks, and can enforce a range of policies from preventing use through to allowing basic read-only access to data.

It is only by the intelligent planning and deployment of these solutions that an organisation can help protect themselves from inadvertent data loss and falling foul of legal and compliance issues.

## Summary of relevant Acts and Regulations

EU Data Retention Directive 2006/24/EC		
<b>Geographic coverage</b> EU	<b>Industries/sectors affected</b> Telecoms	<b>Scope of coverage</b> Data relating to electronic communications

### Summary

The Data Retention Directive was created in 2006 and covers the retention of data generated in connection with public electronic communications. Member states are required to store users' telecommunications data for between 6 and 24 months. This will include data such as IP addresses, time and duration of telephone calls and text messages sent or received. Courts need to approve an order before data access can be granted.

Countries that have implemented the directive, or laws similar to it, include Italy and Denmark. Other countries have legislation or regulations at various stages of discussion, approval or adoption. The UK has implemented a voluntary agreement with providers that is capable of being supported in law if the Home Secretary believes that providers are not cooperating. In the UK, access to this data is subject to the Regulation of Investigatory Powers Act 2000 (RIPA). The sensitive nature of the data being collected has led to significant privacy concerns amongst many European citizens.

### Non-compliance penalties

Will vary across nation states.

### Implications for IT security

As the storage of this data has been mandated by law or a voluntary agreement it must be stored safely and securely. The sensitive nature of the data could cause political issues if it was leaked. Data loss prevention technologies have a significant part to play in securing this data.

## Summary of relevant Acts and Regulations

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995		
<b>Geographic coverage</b> EU	<b>Industries/sectors affected</b> All	<b>Scope of coverage</b> Personal data

### Summary

As part of the development of the EU, this legislation has been put in place to harmonise data protection laws across the EU. The law focuses on seven key principles concerning the use of and access to personal data. Member states of the EU have generally implemented their own local data protection laws that enshrine the principles of Directive 95/46/EC; for example the UK has implemented the Data Protection Act, Germany has The Federal Data Protection Act (Bundesdatenschutzgesetz) and the Netherlands has the Personal Data Protection Act (Wet bescherming persoonsgegevens).

### Non-compliance penalties

Each nation member can impose their own penalties. These generally comprise of fines imposed by courts.

### Implications for IT security

Any organisation holding personal data subject to this directive must ensure that the information is protected according to seven principles:

- The principle of openness
- The principle of individual participation
- The principle of collection limitation
- The principle of data quality
- The principle of finality
- The principle of security
- The principle of accountability

These principles rely on good, overall system security including the use of data loss prevention solutions to ensure that data is protected both at rest at in motion.

## Summary of relevant Acts and Regulations

EU Capital Requirements Directive/Basel II Accord		
<b>Geographic coverage</b> International	<b>Industries/sectors affected</b> Banking and Finance	<b>Scope of coverage</b> Internationally-active banks with assets greater than \$250 billion or foreign exposures greater than \$10 b

### Summary

Basel II is designed to create an international standard to be used across banking organisations when creating regulations concerning the amount of capital that banks need to set aside to guard against operational risks.

The accord is designed to prevent international financial problems being created by collapsed banks, and sets rules on the amount banks need to keep in reserve based on their exposure. Basel II is based on the concept of three pillars that encompass how banks can prepare for credit risks, interact with regulators and provide responsible disclosure.

In July 2009, and in light of the worldwide financial crisis, the Basel Committee on Banking Supervision approved measures to strengthen a number of rules and to enhance the three pillars of the Basel II framework. Banks and supervisors were expected to begin implementing the Pillar 2 guidance from July 2009 onwards. The new Pillar 1 capital requirements and Pillar 3 disclosures need to be implemented by the end of 2010. Basel II has been implemented in the EU as part of the Capital Requirements Directives. In December 2009 the Committee announced a package of proposals to further strengthen banking resilience.

### Non-compliance penalties

Non-compliance can result in institutions having to reserve greater amounts of capital to cover their risk exposure, resulting in less favourable pricing in capital markets.

### Implications for IT security

Operational risk forms the heart of Basel II. An institution therefore needs to protect its data with the utmost integrity—be it data at rest, in motion or during transactions. Data loss prevention forms a mainstay of this requirement.

## Summary of relevant Acts and Regulations

Payment Card Industry Data Security Standards (PCI DSS)		
<b>Geographic coverage</b> Global	<b>Industries/sectors affected</b> All	<b>Scope of coverage</b> Any that process card payments

### Summary

The use of payment cards has increased massively with the popularity of online purchasing. PCI DSS was introduced by the PCI Standards Council, which was founded by the major payment card brands in order to enhance the security of payment accounts.

At the foundation of the PCI DSS are 12 requirements that specify how payment data should be managed:

- Install and maintain a firewall configuration to protect cardholder data.
- Do not use vendor-supplied defaults for system passwords and other security parameters.
- Protect stored cardholder data.
- Encrypt transmission of cardholder data across open, public networks.
- Use and regularly update anti-virus software.
- Develop and maintain secure systems and applications.
- Restrict access to cardholder data by business need-to-know.
- Assign a unique ID to each person with computer access.
- Restrict physical access to cardholder data.
- Track and monitor all access to network resources and cardholder data.
- Regularly test security systems and processes.
- Maintain a policy that addresses information security.

PCI DSS only applies if the payment card primary account number is stored by the organisation. PCI DSS is managed by the payment card industry, which conduct audits and checks dependent on the volume of card transactions. Smaller volume retailers are expected to self-audit/self-certify that their systems adhere to the PCI DSS requirements. Version 1.2 of PCI DSS was released in October 2008 and further clarified the requirements on card processing organisations.

### Non-compliance penalties

Fines and withdrawal of payment card facilities.

### Implications for IT security

PCI DSS is very much an IT-focused requirement, with some very specific requirements on the safe keeping of payment card data. The 12 principles highlighted by PCI DSS comprise a valid health check and best practice checklist in their own right. Data loss prevention plays a vital part in PCI DSS and by having in place a robust and well-managed data encryption system a number of PCI DSS requirements can be addressed immediately.

## Summary of relevant Acts and Regulations

The Rules Governing Medicinal Products in the European Union and Commission Directives 91/356/EEC, 2003/94/EC, and 91/412/EEC		
<b>Geographic coverage</b> EU	<b>Industries/sectors affected</b> Pharmaceuticals	<b>Scope of coverage</b> Computers used in the manufacturing process

### Summary

The EU has high standards of pharmaceutical manufacturing. In an effort to maintain these standards, rules have been introduced to ensure that approved manufacturers maintain appropriate standards. This good manufacturing practice, known as GMP, as been codified in two directives that have been adopted by the European Commission. Annex 11 of this regulation determines best practice use of computing in good manufacturing practice.

### Non-compliance penalties

Fines imposed by the EU.

### Implications for IT security

This regulation insists that good computing practice be implemented for proper control of the manufacturing process. This ranges from the best principles of systems development through to the implementation of system security and safeguards. Data can only be entered or updated by approved people and any changes are to be recorded. Systems are to be fully backed up to prevent data loss. Data must be protected against inappropriate changes and adequately secured. Data loss prevention is mentioned directly, as Part 13 of annexe 11 states that "Data should be secured by physical or electronic means against wilful or accidental damage".

## Summary of relevant Acts and Regulations

MiFID - The Markets in Financial Instruments Directive		
<b>Geographic coverage</b> EU	<b>Industries/sectors affected</b> Banking and Finance	<b>Scope of coverage</b> Companies and banks trading in financial instruments and businesses that deal in advisory services

### Summary

The directive affects the way in which some share trades are undertaken. Instead of using exchanges, banks are able to deal "off-book"; buying and selling shares through customers directly. This is seen to be easier than using a share exchange. It is an update to the Investment Services Directive and is referred to in some places as ISD 2. The original Investment Services Directive was not successful.

### Non-compliance penalties

MiFID is monitored by local authorities who are responsible for the regulation of financial transactions (for example the Financial Services Authority in the UK). Non-compliance will be investigated and, if appropriate, fines will be imposed by these regulators.

### Implications for IT security

Businesses will need to prove that they are able to provide 'best execution' on any deals they are conducting. This will need to take into account cost, speed, pricing and venue and any records created will need to be stored for a minimum of 5 years. There will be an increase in algorithmic trading using automatic systems to determine the best trade venues, which will need to provide a clear audit trail.

From a security perspective it will be vital that these trades are protected during the transaction phase and that records created are stored securely, using data loss technologies such as encryption, for the minimum 5 year period.

## Summary of relevant Acts and Regulations

Statutory Audit and the Company Reporting Directives (“EuroSox”)		
<b>Geographic coverage</b> EU—must be implemented into local laws by EU member states by 2010.	<b>Industries/sectors affected</b> All	<b>Scope of coverage</b> Public companies

### Summary

Two European directives were issued by the European Union Council of Ministers aiming to create more transparency and public confidence in the operations of companies operating within the EU. The Statutory Audit Directive is designed to strengthen the standards and public accountability of the audit profession and the Company Reporting Directive aims to enhance confidence in financial statements and annual reports from European companies. As an example of a national implementation the provisions of the Statutory Audit Directive were introduced into UK law through the Companies Act 2006,

### Non-compliance penalties

EuroSox will be incorporated into local national company laws; therefore penalties will vary from member state to member state.

### Implications for IT security

EuroSox will demand that IT maintains accurate, dependable records with full audit trails of any data changes. Management will expect accurate and dependable reports created from within IT systems. IT systems will need to be secured to meet auditor approval and data must be protected from unauthorised access. Data loss prevention technologies will have a key part to play in securing data subject to EuroSox.

## Summary of relevant Acts and Regulations

Data Protection Act 1984, amended 1988 (UK)		
<b>Geographic coverage</b> UK	<b>Industries/sectors affected</b> All	<b>Scope of coverage</b> Any organisation that collects personal data

### Summary

The UK Data Protection Act imposes legal obligations on anyone processing personal data to ensure there is good practice and management of that data. In part 1 of the Act there are 8 enforceable principles of good personal information handling.

Data must be:

- Accurate and up to date.
- Fairly and lawfully processed.
- Secured.
- Not allowed to leave the UK unless the destination countries have similar legislation.
- Processed in line with a person's rights.
- Only kept for as long as necessary.
- Processed for limited purposes.
- Adequate, relevant and not excessive.

Part 2 of the act gives individuals rights to find out what personal information is held about them on computers and most paper records.

### Non-compliance penalties

The UK Information Commissioner's Office (ICO) has legal powers to ensure that organisations comply with the requirements of the Data Protection Act. A data controller who persistently breaches the Act and has been served with an enforcement notice can be prosecuted for failing to comply with a notice. This offence carries a maximum penalty of a £5,000 fine in the magistrates' court and an unlimited fine in the Crown Court. In November 2009 the ICO responded to a consultation paper from the UK Ministry of Justice by calling for an increase in these penalties and the ability for courts to sentence offenders to a custodial punishment.

### Implications for IT security

IT security is not mentioned explicitly in this act, but as computer systems will be used to store this data it is vital that these remain secure at all times. Data encryption forms a vital part of the secure storage of this data as, once encrypted, it will address the secure requirement as listed above. Other data leak prevention technologies could be employed to help prevent either intentional or unintentional data loss or, maybe, data being sent out of the UK.

## Summary of relevant Acts and Regulations

Freedom of Information Act (UK)		
<b>Geographic coverage</b> UK (Scottish public authorities are subject to the Freedom of Information (Scotland) Act 2002)	<b>Industries/sectors affected</b> Government bodies, local authorities and companies owned by the government	<b>Scope of coverage</b> Information held by authorities, excluding personal data

### Summary

The Freedom of Information Act allows access to recorded information such as notes from meetings, research reports and emails held by public authorities. Under the Act any individual can make a request for information and have the necessary data sent to them. Any refusal to supply the information needs to be justified in writing to the applicant, making the reasons for the refusal clear.

### Non-compliance penalties

The Information Commissioner can serve an enforcement notice on a body that fails to provide information. Failure to comply with an enforcement notice may result in the Commissioner referring the matter to the High Court. The High Court can deal with the public authority as if it had committed contempt of court. A public authority may appeal against an enforcement notice to the Information Tribunal.

### Implications for IT security

Data that is subject to the Freedom of Information Act can be resident in a variety of forms throughout an organisation. This could be in the form of emails, word processor documents, spreadsheets or written notes. Any of this data can be secured using data loss prevention technologies such as data encryption. It is imperative that decryption keys be made available so that data can be retrieved in original form from whatever source.

## Summary of relevant Acts and Regulations

Regulation of Investigatory Powers Act 2000 (RIP or RIPA) (UK)		
<b>Geographic coverage</b> UK	<b>Industries/sectors affected</b> All	<b>Scope of coverage</b> All electronic data

### Summary

RIPA allows government organisations to access an individual's electronic communications. This can range from access to Internet Service Provider records through to telephone and email data. ISP records can be demanded from service providers who are under a legal obligation to provide them. Part III of the act allows certain government agencies to demand the cryptographic key to be supplied if the actual decrypted data was not available.

### Non-compliance penalties

Failure to provide a cryptographic key can result in a 2 year jail term.

### Implications for IT security

A demand to access data under RIPA must be adhered to by those receiving the request. If data encryption has been poorly implemented and the decryption key lost then there would be significant implications for the manager of that encryption system.

Efficient and effective key management is a vital part of any data loss prevention deployment.

## Summary of relevant Acts and Regulations

Federal Data Protection Act (November 2006) (Germany)		
<b>Geographic coverage</b> Germany	<b>Industries/sectors affected</b> Public bodies of the Federation and the Länder. Private organisations and businesses	<b>Scope of coverage</b> Private data held by these organisations

### Summary

This is the implementation of EU Directive 95/46/EC in Germany and covers the protection of data held by organisations, in a similar way to the UK Data Protection Act. The act, formally called Bundesdatenschutzgesetz (BDSG), adheres to the seven basic principles of EU Directive 95/46/EC in the protection of data relating to individuals or data that allows an individual to be identified.

The 16 Länder have their own data protection regulations that cover local public bodies. These local regulations are similar in spirit to the Federal Data Protection Act.

In July 2009, German legislature passed a number of amendments to the act to strengthen its powers. Most notably there was a new requirement introduced to provide notification of data breaches in a similar way to the United States. These were effective as from 1<sup>st</sup> September 2009.

### Non-compliance penalties

Fines imposed by the Federal Commissioner for Data Protection and Freedom of Information. Maximum fine is now EURO 50,000 for ordinary offences rising to over EURO 300,000 for more serious offences.

### Implications for IT security

Good data security is a key aspect of this legislation and the onus is on the data-keeping body to ensure that data is held in a secure and reliable way. Data loss prevention is a key technology that will help with adherence to this act.

## Summary of relevant Acts and Regulations

Freedom of Information Act (2005) (Germany)		
<b>Geographic coverage</b> Germany	<b>Industries/sectors affected</b> Government and public bodies	<b>Scope of coverage</b> Information held by authorities (excluding personal data)

### Summary

Citizens in Germany can request information from Government bodies irrespective of whether the individual requesting has a legal interest in gaining access to these documents. There must be minimal delay in providing the information and a maximum time limit of 2 months is given to service the most complex enquiries.

Information can be withheld on the basis of security, defence, tax-related issues or for the protection of trade secrets.

A number of Länder have their own similar laws.

### Non-compliance penalties

Fines imposed by the Federal Commissioner for Data Protection and Freedom of Information.

### Implications for IT security

As for similar legislation across the EU, requests for information can touch on a large amount of data sources, both electronic and paper-based. Good corporate data hygiene is therefore paramount to ensure data is held safely and securely. Data encryption has a large part to play in the safe retention of data, but government departments need to ensure foolproof key management so that data is recoverable in response to requests.

## Summary of relevant Acts and Regulations

Data Protection Act (2004) (France)		
<b>Geographic coverage</b> France	<b>Industries/sectors affected</b> All	<b>Scope of coverage</b> Any organisation that collects personal data

### Summary

This is the implementation of EU Directive 95/46/EU in France and follows the same broad protection requirements of similar legislation in the EU. Enforcement is undertaken by CNIL, the National Commission for Data Protection. The law enables an individual to find out what data is being held about them on payment of a small fee.

### Non-compliance penalties

Fines up to EURO 300,000.

### Implications for IT security

As with the other data protection acts in the EU, data needs to be stored safely and securely, as well as kept to a minimum. Data loss prevention technologies have a significant part to play in securing this data.

## Summary of relevant Acts and Regulations

Law on Access to Administrative Documents (1978/2005) (France)		
<b>Geographic coverage</b> France	<b>Industries/sectors affected</b> Government and public bodies	<b>Scope of coverage</b> Information held by authorities (excluding certain data relating to national security issues etc.)

### Summary

This law gives anyone a right to access the full range of files, reports, minutes, orders, instructions and other related documents created or held by public bodies. These bodies must respond to a request within 1 month. The law stems from an original Article in the 1789 Declaration of the Rights of Man.

Certain documents relating to personal privacy and national security issues are specifically excluded from this range of accessible information. In 2005 an amendment was made to, amongst other changes, allow access to data in electronic form.

The law is overseen by The Commission d'accès aux documents administratifs (CADA)

### Non-compliance penalties

None—the CADA can only mediate and issue recommendations.

### Implications for IT security

As for similar legislation across the EU, requests for information can touch on a large amount of data sources, both electronic and paper based. Good corporate data hygiene is therefore paramount to ensure data is held safely and securely. Data encryption has a large part to play in the safe retention of data, but government departments need to ensure foolproof key management so that data is recoverable in response to requests.

## Summary of relevant Acts and Regulations

Control of Insurance Undertakings (1995) (Belgium)		
<b>Geographic coverage</b> Belgium	<b>Industries/sectors affected</b> Insurance	<b>Scope of coverage</b> Documents relating to contracts

### Summary

This law requires that documents relating to contracts be stored for a mandatory period determined by the Insurance Control Office (OCI).

### Non-compliance penalties

Various fines and/or imprisonment.

### Implications for IT security

Many insurance companies have significant IT systems in support of the business. Therefore many of these documents will be held electronically across multiple repositories, each of which will need to be secured. Data loss prevention technologies have a significant part to play in managing this data, especially data encryption that can be used to protect documents for the mandatory storage period and ensure they are not tampered with.

## Summary of relevant Acts and Regulations

Law of Privacy Protection (1998) (Belgium)		
<b>Geographic coverage</b> Belgium	<b>Industries/sectors affected</b> All	<b>Scope of coverage</b> Any organisation that collects any information relating to an identified or identifiable person

### Summary

This law follows the broad principles of other privacy and data protection laws in the EU. Prior to 1992, only medical data was covered by data protection laws in Belgium. EU Directive 95/46/EC was implemented in Belgium in 1998 and comprehensively modified the protection of personal data. The law is supervised by the Commission for the Protection of Privacy.

### Non-compliance penalties

Various fines, the publishing of judgements in newspapers and/or the forced erasing of data.

### Implications for IT security

As with the other data protection acts in the EU, data needs to be stored safely and securely, as well as kept to a minimum. Data loss prevention technologies have a significant part to play in securing this data.

## Summary of relevant Acts and Regulations

Money Laundering and Finance of Terrorism Law (1993) (Belgium)		
Supervision of the Financial Sector Law (2003) (Belgium)		
Consumer Credit Law (1992) (Belgium)		
<b>Geographic coverage</b> Belgium	<b>Industries/sectors affected</b> Banking	<b>Scope of coverage</b> Documents and transaction records

### Summary

A number of laws cover the storage of data across the banking sector in Belgium. The Money Laundering and Finance of Terrorism Law requires that a copy of a client's identity documents must be stored for a period not less than 5 years after the relationship with that client has terminated. In a similar fashion the Supervision of the Financial Sector Law requires that data relating to financial transactions needs to be kept for a period of 5 years after their execution. The Consumer Credit Law has a range of data retention periods from 15 days through to 10 years depending on the type of transactional data.

### Non-compliance penalties

Various fines and/or imprisonment.

### Implications for IT security

As volumes of documents and transactions will often be very high in a banking environment the various data retention periods add additional complexity. Even so, good information security will ensure that document and transactional integrity is retained, with encryption being a primary tool alongside content inspection solutions used to monitor how and where data is being used.

## Summary of relevant Acts and Regulations

Personal Data Protection Act (2000) (Netherlands)		
<b>Geographic coverage</b> Netherlands	<b>Industries/sectors affected</b> All	<b>Scope of coverage</b> Any organisation that collects any information relating to an identified or identifiable person. Certain data categories are exempt.

### Summary

In the Netherlands the Personal Data Protection Act (Wet Bescherming Persoonsgegevens, or the 'WBP') was enacted in September 2001 and is the Dutch implementation of EU Directive 95/46/EC. The WBP incorporates previous Dutch legislation including the Personal Data Files Act. Following the enactment of the WBP, subsequent legislation has provided exemptions for certain categories of data. The act is supervised by the Data Protection Authority (College Bescherming Persoonsgegevens or CBP).

### Non-compliance penalties

Fines with possible imprisonment for "deliberate" offences.

### Implications for IT security

As with the other data protection acts in the EU, data needs to be stored safely and securely, as well as kept to a minimum. Data loss prevention technologies have a significant part to play in securing this data.

## Summary of relevant Acts and Regulations

Protection of persons with regard to the Processing of Personal Data (2002 and 2007) (Luxemburg)		
<b>Geographic coverage</b> Luxemburg	<b>Industries/sectors affected</b> All	<b>Scope of coverage</b> Any organisation that collects any information relating to an identified or identifiable person

### Summary

EU Directive 95/46/EC was implemented in Luxemburg in 2002. A new data protection authority was created—Commission Nationale pour la Protection des Données or CNPD. The CNPD is responsible for the control and compliance of all those that process personal data in Luxemburg.

A number of reforms to this act were introduced in 2007 to further clarify the law in areas such as employee monitoring, data subject consent and processing of health-related data.

### Non-compliance penalties

Administrative sanctions include the publishing of judgements in newspapers, bans on those that process data contrary to the law and the destruction of data.

### Implications for IT security

The destruction of data obtained in contravention of this act could have implications for other data stored in an organisation, especially if data has been allowed to merge with other record sets. This could mean the loss of more than the data covered under this law. As with the other data protection acts in the EU, data needs to be stored safely and securely, as well as kept to a minimum. Data loss prevention technologies have a significant part to play in securing this data.

## Summary of relevant Acts and Regulations

Personal Data Protection Code (2004) (Italy)		
<b>Geographic coverage</b> Italy	<b>Industries/sectors affected</b> All	<b>Scope of coverage</b> Any organisation that collects any information relating to an identified or identifiable person. Includes deceased people.

### Summary

EU Directive 95/46/EC was implemented in Italy in 1996 but the Italian Data Protection Code, introduced in 2004, brought together all laws and regulations that covered data protection requirements under a single piece of legislation. Supervised by the Italian Data Protection Commission.

### Non-compliance penalties

Fines and the publishing of judgements in newspapers.

### Implications for IT security

As with the other data protection acts in the EU, data needs to be stored safely and securely, as well as kept to a minimum. Data loss prevention technologies have a significant part to play in securing this data.

## Summary of relevant Acts and Regulations

Civil Code section 2214 and 2220 (Italy)		
<b>Geographic coverage</b> Italy	<b>Industries/sectors affected</b> All	<b>Scope of coverage</b> All accounting records, emails, faxes, invoices and other business records

### Summary

The Italian Civil Code, sections 2214 and 2220, requires that businesses store all their business related documentation, including emails, in a format that can be made accessible. Digital storage is permitted, as long as the digital copy matches the original and can be readily accessed.

Other similar legislation includes regulation 16190 of the Italian National Commission for the Listed Companies and Stock Exchange that requires financial promoters to keep 5 years of data. The Italian Financial Code law 58/1998 requires financial intermediaries to keep 5 years of data in a similar fashion.

### Non-compliance penalties

None that are specific, but it may influence the course of investigations and the company's rights if access to documents by a judicial authority is denied.

### Implications for IT security

As with the other data protection acts in the EU, data needs to be stored safely and securely, as well as kept to a minimum. Proving that data has not been altered may require the use of audit trails or digital signing technologies. Data loss prevention technologies have a significant part to play in securing this data.

## Summary of relevant Acts and Regulations

Protection of Personal Data (1999) (Spain)		
<b>Geographic coverage</b> Spain	<b>Industries/sectors affected</b> All	<b>Scope of coverage</b> Any organisation that collects any information relating to an identified or identifiable person.

### Summary

Data protection is enshrined under article 18.4 of the Spanish constitution. It was further protected under extra legislation introduced in 1992 and 1993 with the Spanish Data Protection Agency being formed in March 1993. Organic law on the Protection of Personal Data 15/1999 implemented EU Directive 95/46/EC into Spanish law.

### Non-compliance penalties

Fines with possible imprisonment under the Spanish Criminal Code 1995.

### Implications for IT security

As with the other data protection acts in the EU, data needs to be stored safely and securely, as well as kept to a minimum. Data loss prevention technologies have a significant part to play in securing this data.

## Summary of relevant Acts and Regulations

---

Commercial Code (Spain)		
<b>Geographic coverage</b> Spain	<b>Industries/sectors affected</b> All	<b>Scope of coverage</b> All accounting and other business records

### Summary

The Spanish Commercial Code requires that all businesses keep their business-related documents for a period of 6 years from the last accounting book entry. A similar tax law places a requirement to keep tax related documentation for up to 4 years. There are no specific laws related to the archiving and retrieval of email-based data.

### Non-compliance penalties

None specific but there may be an increase in tax liabilities that are levied for those businesses that do not comply.

### Implications for IT security

Even though the non-compliance penalties are not specific it is in the best interest of any organisation to adhere to such a requirement as it demonstrates good corporate management. Data encryption has a key part to play in keeping this data secure.

---

## Summary of relevant Acts and Regulations

Personal Data Act (1999) (Finland)		
<b>Geographic coverage</b> Finland	<b>Industries/sectors affected</b> All	<b>Scope of coverage</b> Any organisation that collects any information relating to an identified or identifiable person. Indirectly covers the deceased if their sensitive data may affect living relatives

### Summary

EU Directive 95/46/EC was introduced in 1995, the year that Finland joined the EU. As a result Finnish data protection laws were revised in 1999. The new act—Personal Data Act 1999—encompassed broader rights and freedoms of individuals as regards their personal data. The Act is managed by the Data Protection Ombudsman.

### Non-compliance penalties

Fines with possible imprisonment of up to 1 year under the Finnish Criminal Code 1995.

### Implications for IT security

As with the other data protection acts in the EU, data needs to be stored safely and securely, as well as kept to a minimum. Data loss prevention technologies have a significant part to play in securing this data.

## Summary of relevant Acts and Regulations

---

Personal Data Act (1998) (Sweden)		
<b>Geographic coverage</b> Sweden	<b>Industries/sectors affected</b> All	<b>Scope of coverage</b> Any organisation that collects any information relating to an identified or identifiable person

### Summary

Sweden introduced a data protection act in 1973 that regulated the automatic processing of data files that contained personal data. As this act was outdated by advances in technology, EU Directive 95/46/EC was introduced with relative speed as the Personal Data Act 1998. In some instances the Data Act 1973 does still apply, as the legislation has not been fully repealed. The act is supervised by the Data Protection Board.

---

### Non-compliance penalties

Fines with possible imprisonment.

---

### Implications for IT security

As with the other data protection acts in the EU, data needs to be stored safely and securely, as well as kept to a minimum. Data loss prevention technologies have a significant part to play in securing this data.

---

## Summary of relevant Acts and Regulations

Accounting Act SFS 1999:1078 (Sweden)		
<b>Geographic coverage</b> Sweden	<b>Industries/sectors affected</b> All	<b>Scope of coverage</b> All companies

### Summary

Under the Swedish Accounting Act all companies, irrespective of their size, must archive their accounting information. This includes all forms of documents or technically-readable media. Documents received from other parties must be stored in their original form, including emails. The documents must be easily accessible for a period of 10 years.

### Non-compliance penalties

Fines with possible imprisonment.

### Implications for IT security

In this case failure to protect documents and make them easily accessible could result in a prison sentence. Clearly data loss prevention technologies will play a key part in keeping this data safe and secure.

## Summary of relevant Acts and Regulations

---

Public Records Act SFS 1990:782 (Sweden)		
<b>Geographic coverage</b> Sweden	<b>Industries/sectors affected</b> Government and public bodies	<b>Scope of coverage</b> Public authorities and other bodies controlled by municipal bodies

### Summary

Under this act all public authorities or other entities that are controlled by a municipal body must archive all documentation and records they receive, process or create. This includes all incoming and most outgoing emails. These records are to be retained for the purposes of research and the right to access public documents.

### Non-compliance penalties

None specific but the act is supervised by the Swedish National Archives.

### Implications for IT security

As with the other public information data protection acts in the EU, data needs to be stored safely and securely. Data loss prevention technologies have a significant part to play in securing this data.

---

## EU Compliance—Summary Comparison Table

Act	Geographic coverage	Industries and sectors affected	Scope of coverage notes
EU Data Retention Directive 2006/24/EC	EU	Telecoms	Data relating to electronic communications
Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995	EU	All	Personal data
Capital Requirements Directive/Basel II Accord	International	Banking and Finance	Internationally-active banks with assets greater than \$250 billion or foreign exposures greater than \$10 billion
Payment Card Industry Data Security Standards (PCI DSS)	International	All	Any that process card payments
The Rules Governing Medicinal Products in the European Union and Commission Directives 91/356/EEC, 2003/94/EC, and 91/412/EEC	EU	Pharmaceutical	Computers used in the drug manufacturing process
MiFID - The Markets in Financial Instruments Directive	EU	Banking and Finance	Companies and banks trading in financial instruments and businesses that deal in advisory services
Statutory Audit and the Company Reporting Directives (EuroSox)	EU - must be implemented into local laws by EU member states by 2010.	All	Public companies
Data Protection Act 1984, amended 1988	UK	All	Any organisation that collects personal data
Freedom of Information Act	UK (Scottish public authorities are subject to the Freedom of Information (Scotland) Act 2002)	Government bodies, local authorities and companies owned by the government	Information held by authorities, excluding personal data
Regulation of Investigatory Powers Act 2000 (RIP or RIPA)	UK	All	All electronic data
Federal Data Protection Act (November 2006)	Germany	Public bodies of the Federation and the Länder. Private organisations and businesses	Private data held by these organisations
Freedom of Information Act (2005)	Germany	Government and public bodies	Information held by authorities (excluding personal data)
Data Protection Act (2004)	France	All	Any organisation that collects personal data
Law on Access to Administrative Documents (1978/2005)	France	Government and public bodies	Information held by authorities (excluding certain data relating to national security issues etc.)
Control of Insurance Undertakings (1995)	Belgium	Insurance	Documents relating to contracts
Law of Privacy Protection (1998)	Belgium	All	Any organisation that collects any information relating to an identified or identifiable person

## Summary of relevant Acts and Regulations

Act	Geographic coverage	Industries and sectors affected	Scope of coverage notes
Money Laundering and Finance of Terrorism Law (1993) Supervision of the Financial Sector Law (2003) Consumer Credit Law (1992)	Belgium	Banking	Documents and transaction records
Personal Data Protection Act (2000)	Netherlands	All	Any organisation that collects any information relating to an identified or identifiable person. Certain data categories are exempt.
Protection of persons with regard to the Processing of Personal Data (2002 and 2007)	Luxemburg	All	Any organisation that collects any information relating to an identified or identifiable person
Personal Data Protection Code (2004)	Italy	All	Any organisation that collects any information relating to an identified or identifiable person. Includes deceased people
Civil Code section 2214 and 2220	Italy	All	All accounting records, emails, faxes, invoices and other business records
Protection of Personal Data (1999)	Spain	All	Any organisation that collects any information relating to an identified or identifiable person.
Commercial Code	Spain	All	All accounting and other business records
Personal Data Act (1999)	Finland	All	Any organisation that collects any information relating to an identified or identifiable person. Indirectly covers the deceased if their sensitive data may affect living relatives
Personal Data Act (1998)	Sweden	All	Any organisation that collects any information relating to an identified or identifiable person
Accounting Act SFS 1999:1078	Sweden	All	All companies
Public records Act SFS 1990:782	Sweden	Government and public bodies	Public authorities and other bodies controlled by municipal bodies

## Other significant legislation and regulations

---

The following legislation and regulations may be of interest to those investigating IT compliance requirements in the EU but detailed coverage is not included in this paper:

- Sarbanes-Oxley Act of 2002 (SOX). US legislation that only covers EU companies that have a presence in the United States.
- Health Insurance Portability and Accountability Act of 1996 (HIPPA). US legislation that applies to healthcare providers based in the United States.
- The Gramm-Leach-Bliley Act (Financial Modernization Act of 1999). US legislation that covers the protection of financial institutions' private customer data.
- USA Patriot Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001). US legislation that covers the use of surveillance by government agencies and the requirement of business to report computer-based crime.
- The Turnbull Guidance. The Turnbull Guidance sets out best practices on internal control for UK-listed companies. The US Securities and Exchange Commission has permitted use of the Turnbull Guidance as a suitable framework for complying with US requirements to report on internal controls over financial reporting, as set out in Section 404 of the Sarbanes-Oxley Act 2002 and related SEC rules. Limited direct relevance to EU-based IT professionals.
- California Data Security Breach Notification Law Cal. Civ. Code 1798.82 and 1798.29. This law, enacted in 2002, requires that if personal data security has been breached then those individuals possibly affected must be notified of this breach. This law is seen by many to be the model breach notification legislation. EU legislators are considering a similar law in the EU and individual nation states, such as Germany, have already implemented a similar law.
- Money Laundering Regulations 2003. UK legislation that places obligations on financial professionals such as accountants and auditors to report money laundering and keep appropriate records.
- The Companies Act 1985 (Investment Companies and Accounting and Audit Amendments) Regulations 2005. This UK Act changes the financial reporting requirements for some companies, notably smaller businesses. Limited direct relevance to EU-based IT professionals.
- International Financial Reporting Standards (IFRS). A set of standards and a framework for the preparation of accounts. Limited direct relevance to EU-based IT professionals.
- Royal Decree on Medical Files 1999. In Belgium medical records must be kept in a hospital for a minimum of 30 years. If these are in an electronic form then it will be relevant to EU-based IT professionals.
- Care Net Protocol and Belgium National Service for Medical and Disability Insurance. Both of these require data to be stored from 3–10 years. If these are in an electronic form then it will be relevant to EU-based IT professionals.

## Strategies for managing information technology compliance

---

Information technology can be notoriously complex and often sees business managers chased away from getting involved with decisions related to technology. Whilst this may be appropriate in very narrow technical decisions it is important that business understands IT and how it is benefiting the business.

From a compliance perspective it is very easy for the business to be frightened by talk of liabilities, whilst technicians appear to spend budgets with limited care for the overall business benefit. When considering IT compliance, it is imperative that a strategic approach is taken based on clear, rational thinking. Many businesses have rushed into a technical solution that was sold as solving compliance issues only for them to quickly realise the limitations of the product.

Poorly implemented data encryption projects are notorious for causing significant trouble to the business. Tactical encryption, maybe at the departmental level, may appear to be a perfect solution for the first few months. Problems then start to occur as users leave or move on, taking with them, or forgetting, decryption keys. Soon the department is faced with stores of data that cannot be recovered, which, in itself, can create legal problems, especially if the organisation is subject to an investigation and associated discovery. Poor encryption key management is at the centre of very many bad encryption implementations.

A data leak prevention project needs to be planned with suitable care and diligence. Implemented badly, data will still go missing whilst legitimate data transfers are prevented, causing dismay to business users. Data encryption forms the backbone of a strategic data leak prevention strategy as it gives the reassurance that any data that does go missing will be unreadable.

Bloor Research actively advocates the use of both data leak prevention and data encryption technologies to produce what we term Enterprise Data Protection. By implementing an Enterprise Data Protection strategy organisations are a significant way down the route of achieving compliance across many legislative areas.

### Further Information

Further information is available from <http://www.BloorResearch.com/update/1077>

## Bloor Research overview

---

Bloor Research is one of Europe's leading IT research, analysis and consultancy organisations. We explain how to bring greater Agility to corporate IT systems through the effective governance, management and leverage of Information. We have built a reputation for 'telling the right story' with independent, intelligent, well-articulated communications content and publications on all aspects of the ICT industry. We believe the objective of telling the right story is to:

- Describe the technology in context to its business value and the other systems and processes it interacts with.
- Understand how new and innovative technologies fit in with existing ICT investments.
- Look at the whole market and explain all the solutions available and how they can be more effectively evaluated.
- Filter "noise" and make it easier to find the additional information or news that supports both investment and implementation.
- Ensure all our content is available through the most appropriate channel.

Founded in 1989, we have spent over two decades distributing research and analysis to IT user and vendor organisations throughout the world via online subscriptions, tailored research services, events and consultancy projects. We are committed to turning our knowledge into business value for you.

## About the author

---

### Nigel Stanley Practice Leader—Security

Nigel Stanley is a specialist in business technology and IT security and now heads up Bloor's IT Security practice.

IT security comprehensively covers the whole remit of protecting and defending business or organisational systems and data from unwelcome attacks or intrusions. This large area includes protection from the outer edges of the security domain such as handheld devices through to the network perimeter, inside threats and local defences. It looks at the ever-growing threats, many of them new and innovative. It includes use of firewalls, data loss prevention, data encryption, anti-malware, database protection, identity management, intrusion detection/prevention, content management/filtering and security policies and standards.

For a number of years Nigel was technical director of a leading UK Microsoft partner where he led a team of consultants and engineers providing secure business IT solutions. This included data warehouses, client server applications and intelligent web based solutions. Many of these solutions required additional security due to their sensitive nature. From 1995 until 2003 Nigel was a Microsoft regional director, an advisory role to Microsoft Corporation in Redmond, which was in recognition of his expertise in Microsoft technologies and software development tools.

Nigel had previously worked for Microsoft as a systems engineer and product manager specialising in databases and developer technologies. He was active throughout Europe as a leading expert on database design and implementation.

He has written three books on database and development technologies including Microsoft .NET. He is working on a number of business-led IT assignments and is an executive board member of a number of privately held companies including Incoming Thought Limited, a partner company to Bloor Research that specialises in security consultancy and education.

Nigel is a member of the Institution of Engineering and Technology, the British Computer Society and the Institute of Directors.



## Copyright & disclaimer

---

This document is copyright © 2010 Bloor Research. No part of this publication may be reproduced by any method whatsoever without the prior consent of Bloor Research.

Due to the nature of this material, numerous hardware and software products have been mentioned by name. In the majority, if not all, of the cases, these product names are claimed as trademarks by the companies that manufacture the products. It is not Bloor Research's intent to claim these names or trademarks as our own. Likewise, company logos, graphics or screen shots have been reproduced with the consent of the owner and are subject to that owner's copyright.

Whilst every care has been taken in the preparation of this document to ensure that the information is correct, the publishers cannot accept responsibility for any errors or omissions.



2nd Floor,  
145-157 St John Street  
LONDON,  
EC1V 4PY, United Kingdom

Tel: +44 (0)207 043 9750  
Fax: +44 (0)207 043 9748  
Web: [www.BloorResearch.com](http://www.BloorResearch.com)  
email: [info@BloorResearch.com](mailto:info@BloorResearch.com)