

# IT compliance and IT security

## Part 3: How are risks addressed in Europe?

---

*This article is the 3rd in a series by Dr Jörg Hladjk, Associate at Hunton & Williams, and provides an overview of the European policy on IT security, outlines the main legal instruments and provides practical guidance for IT security policies*

---

This is the final part in a series of articles about the interrelationship of data protection and IT security. (For previous parts, see “IT compliance and IT security - Part 1: Why is it necessary to comply with legal requirements?,” *Privacy & Data Protection*, Volume 7, Issue 4, pp. 3-5, and “IT compliance and IT security - Part 2,” *Privacy & Data Protection*, Volume 7, Issue 5, pp. 11-13).

This article will first provide an overview of the current European policy on IT security. It will then consider the main European legal instruments in the area. These include practical measures of risk management and IT security from a business point of view, the importance of self-regulation and tools such as common IT security standards, and practical guidance which can help Data Protection Officers and Chief Information Officers draft appropriate IT security policies and establish procedures that are based on sound legal definitions.

### European policy on IT security

European policy recognises that networks and IT systems have become an essential factor for organisations with regard to economic development. The security of networks and IT systems, in particular their availability, is considered to be of increasing concern to organisations, not least because of system complexity, accidents, mistakes and attacks that may have consequences for physical infrastructures which deliver services critical to the organisation and its customers.

The growing number of security breaches has already caused substantial financial damage, undermined customer confidence and been detrimental to the development of e-commerce. At the same time, IT security has moved to the forefront of regulation in the European Union to address potential risks associated with the use of IT and to facilitate specific requirements with regard to relevant legislation.

IT security has long been within the scope of the European legal framework starting with the Council Decision of 1992 in the field of security of information systems. The INFOSEC program of the European Commission resulted in the IT Security Evaluation Criteria (‘ITSEC’) and the IT Security Manual (‘ITSEM’) on the implementation of the evaluation criteria.

The Council Resolution of 2002 on a common approach and specific actions in the area of network and information security imposes a number of obligations on the Member States and the European Commission. For example, Member States have to promote best practices and usage of internationally recognised standards, including the Common Criteria Standard (ISO 17799). For the Commission, the resolution imposes requirements such as facilitating awareness and best practices and proposing measures to promote the Common Criteria Standard (ISO 15408).

A further significant policy initiative has been the establishment of the European Network Information Security Agency (ENISA) following the adoption of Regulation No. 460/2004 on 10th March, 2004. ENISA is a European Community agency. Such agencies are not provided for in the European Treaties. Instead, each one is set up by an individual piece of legislation that specifies the task of that particular agency.

ENISA’s main objective is to enhance the capability of the Community, Member States and the business community, to prevent, address and respond to network and IT security problems.

From a legal viewpoint, specific regulatory action has already been taken both at the European level and at Member State level. Standardisation has been developed in Europe within the European standardisation organisations, the European Telecommunications Standards Institute (‘ETSI’) and the European Committee for Standardisation/Information Society Standardisation System (‘CEN/ISSS’), as well as through international cooperation with ISO or

Member State initiatives. These standards assume legal significance as mandated by law in order to give effect to a particular Directive.

## European regulatory framework

In May 2007, the ad-hoc Working Group on Regulatory Aspects of Network and Information Security ('RANIS') of ENISA issued a report that provides an overview of European regulatory activities in the area of network and IT security.

The inventory on legal instruments provided in the report covers the following areas: network and information security, attacks against information systems, corporate governance/IT governance, data authentication and security; data protection and data retention; provision of electronic communications networks and services; intellectual property rights and the protection of technical mechanisms designed to prevent copying and counterfeiting; as well as security and financial services.

This article focuses on some main legal instruments mentioned in the report and highlights provisions which are crucial with regard to practical measures of risk management and IT security.

## Network and information security

Even though the ENISA Regulation is not addressed to businesses directly, it provides for interesting definitions which can help businesses draft appropriate IT security policies and establish procedures that are based on sound legal definitions. According to the Regulation:

- “network and information security means the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data and the related services offered by or accessible via these networks and systems”, Article 4(c);

- “risk means a function of the probability that a vulnerability in the system affects authentication or the availability, authenticity, integrity or confidentiality of the data processed or transferred and the severity of that effect, consequential to the intentional or non-intentional use of such a vulnerability”, Article 4(h);
- “risk assessment means a scientific and technologically based process consisting of four steps, threats identification, threat characterisation, exposure assessment and risk characterisation”, Article 4(i); and
- “risk management means the process, distinct from risk assessment, of weighing policy alternatives in consultation with interested parties, considering risk and other legitimate factors, and, if need be, selecting appropriate prevention and control options”, Article 4(j).

The interaction of these definitions with other existing legal instruments (such as the Data Protection Directive 1995/46/EC) has not yet been addressed in case law or literature. However, these definitions provide useful guidance on a European level for organisations drafting risk management and IT security procedures. It should also be noted that in case of any legal proceedings, European courts may refer to European instruments in order to interpret the European business policies in question.

## Attacks against information systems

Another legal instrument to be mentioned when looking for legal guidance in terms of business IT security is the Framework Decision of 2005 on attacks against information systems.

Framework Decisions are used to align the laws and regulations of Member States. They are binding on the Member States as to the result to be achieved, but leave the choice of form and methods to the national authorities. The 2005 Framework Decision ensures that attacks against information systems are sanctioned in all Member States by effective, propor-

tionate and dissuasive criminal penalties. It improves and encourages judicial co-operation by removing potential obstacles. It includes the following acts as criminal offences:

- illegal access to information systems (the intentional access without right to the whole or any part of an information system), Article 2;
- illegal system interference (the intentional serious hindering or interruption of the functioning of an information system by inputting, transmitting, damaging, deleting, deteriorating, altering, suppressing or rendering inaccessible computer data), Article 3; or
- illegal data interference (intentional deletion, damaging, deterioration, alteration, suppression or rendering inaccessible of computer data on an information system), Article 4.

In each case, the criminal act must be intentional. Instigating, aiding, abetting or attempting to commit any of the above offences is subject to punishment.

The Decision defines an information system as: “any device or group of inter-connected devices that perform automatic processing of computer data, and the computer data stored, processed, recovered or transmitted by them for the purposes of their operation, use, protection and maintenance,” Article 1(a).

It further states that computer data can be: “any representation of facts, information or concepts in a form suitable for processing in an information system, including a program suitable for causing an information system to perform a function,” Article 1(b).

The above descriptions of acts that constitute criminal offences may be used by businesses for risk management policies and guidelines in order to set clear categories and descriptions with regard to security breaches.

In addition, the definitions provided in the Decision may provide for starting points to describe the businesses' IT

(Continued on page 12)

(Continued from page 11)

systems and information or data that is processed on these systems.

## Data protection and data security

According to Article 17(1) of Directive 95/46/EC, Member States have to provide that a data controller must implement: “appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.”

For example, in Germany, Article 17(1) has been implemented in a very detailed way. According to Section 9 of the Federal Data Protection Act, companies processing personal data either on their own behalf or on behalf of others must take the technical and organisational measures necessary to ensure the implementation of the provisions of the Act, in particular the requirements set out in the Annex to the Act.

Measures are required only if the effort involved is reasonable in relation to the required level of protection. According to the Annex, measures suited to the type of personal data or data categories to be protected have to be implemented:

- “to prevent unauthorised persons from gaining access to data processing systems with which personal data are processed or used (access control);”
- “to prevent data processing systems from being used without authorisation (access control);”
- “to ensure that persons entitled to use a data processing system have access only to the data to which they have a right of access, and that personal data cannot be read, copied, modified or removed with-

out authorisation in the course of processing or use and after storage (access control);”

- “to ensure that personal data cannot be read, copied, modified or removed without authorisation during electronic transmission or transport, and that it is possible to check and establish to which bodies the transfer of personal data by means of data transmission facilities is envisaged (transmission control);”

—  
**“Personal data of customers are a business asset that needs appropriate security protection to avoid security breaches”**  
 —

- “to ensure that it is possible to check and establish whether and by whom personal data have been input into data processing systems, modified or removed (input control);”
- “to ensure that, in the case of commissioned processing of personal data, the data are processed strictly in accordance with the instructions of the principal (job control);”
- “to ensure that personal data are protected from accidental destruction or loss (availability control); and”
- “to ensure that data collected for different purposes can be processed separately.”

Article 4(1) of Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector contains similar requirements for providers of publicly available electronic communications services.

The detailed measures provided in national law implementing the requirements of Article 17 of Directive 95/46/EC and Directive 2002/58/EC have to be taken seriously in order to avoid any risk in terms of non-compliance.

This is particularly important in the context of setting up appropriate risk management, security and business continuity programs which are supposed to apply in different European Member States. Since the Member States have implemented the requirements of Article 17 differently by means of comprehensive (secondary) legislation (for example, Italy, Latvia, Poland and Spain) or detailed guidance by data protection authorities for that area exists (for example, Belgium, Luxembourg and The Netherlands), European IT security compliance projects have to consider these differences to avoid compliance risks for local entities in these countries.

Personal data of customers are a business asset that needs appropriate security protection to avoid security breaches that can have an impact on the business image in general or its financial performance.

## Self-regulation and security policy

In addition to legal requirements, IT security can be addressed through frameworks set up by businesses themselves. These frameworks include policies and agreements that set out the conditions for IT security within an organisation.

Measures such as internal policy drafting and mapping, audit and control of enforcement are essential for supporting a security framework. In general, any approach to IT security includes the detection and recognition of a threat and the risks it poses through an appropriate threat analysis and risk assessment, a strategy on a security plan and subsequent implementation, and an audit of the implemented security measures.

On a practical level, IT security can be assured by supporting policies through appropriate international standards such as ISO 17799. In fact, some national data protection authorities explicitly recommend in their legal guidance the use of these types of standards (for example, Ireland and the United Kingdom).

ISO 17799 gives recommendations for IT security management for use by those who are responsible for initiating, implementing or maintaining

security in their organisations. It is intended to provide a common basis for developing security standards and effective security management practice. From a legal standpoint, the elements of a security policy have to be modified to the type and corporate goal of an organisation.

## The IT security policy

Typical elements of a security policy may include at least the following:

- **Scope:** The scope of the IT security policy needs to be defined clearly. This allows additional content to be included over and above what is defined in, for example, ISO 17799.
- **Purpose:** The purpose will define the status of the document, in particular to whom the policy applies. This section will normally allow a business to link the IT security policies to other critical policies on topics such as data protection, HR and accounting. These may have interfaces to the IT security policy. This section can also state the formal review process under which the IT policy will be reviewed.
- **Definition:** The definition of security section should outline a well-defined security concept for the organisation. The security concept should be clear and concise and convey to the readers the intention of the policy, for example, ensuring the confidentiality, integrity and availability of data and resources through the use of effective and established security processes and procedures. The definition should address why the security policy is implemented, and what the corresponding mission entails, according to the mission and the business goals of the business.
- **Responsibility:** The security organisation section should define the persons responsible for design, implementation and review of IT security policies. The business should decide how the IT security policy should be communicated internally and externally.
- **Inventory:** In the asset inventories section, the business should prepare and maintain formal inventories of all system software, hardware, networking and application software used to

process information and personal data.

- **Human resource:** The personnel security section needs to reference the HR policy. In general, this should contain two elements. Firstly, the need to recruit suitably experienced staff, who are qualified for all roles related to the maintenance of IT systems. Secondly, there should be a requirement to ensure that a formal HR process is established to monitor the performance and skills of staff processing critical information or data. For example, the business could identify staff responsibilities for internal controls and IT security.
- **Management:** In the communications and operations management section, the security of the network parameters and the operation of the business network and central IT facilities should be defined and described.
- **Access control:** In the access control section of the policy, procedures in line with access to IT systems should be defined.
- **Development:** The systems development and maintenance section should outline the procedures for system development and maintenance oriented at common standards for IT security.
- **Enforcement:** The policy should identify how it will be enforced and how a security breach or misconduct is handled. This requirement is necessary in order to ensure that incidents are handled in an appropriate manner while the security policy remains binding across the organisation.

## Conclusion

In Europe, risk management in IT security is a business process that should be linked and aligned to the corporate mission and strategy. It should constitute a recurring process, based on the participation and awareness of the whole enterprise.

Further, risk management has to consider the existing European legal framework on IT security specifying the operational environment of the business. The existing European legal instruments do not all have businesses

as direct addresses, but they provide for valuable input and practical guidance that can assist in the drafting of appropriate IT security policies and the establishment of procedures that are based on sound legal definitions.

In addition, full incorporation and implementation of all sub-processes such as evaluation and audit of IT security are crucial to successful IT security projects.

---

**Jörg Hladjk**  
Hunton & Williams  
jhladjk@hunton.com

---