



The Security Division of EMC

White paper

The Relationship Between ISO 27002 and the EU Data Protection Directive



ISO/IEC 27002 is a practical guideline for developing security standards.

RSA Foreword

The regulatory landscape for Information Security in Europe has grown ever more complex in recent years. As organisations, both public and private, recognise the inherent value of their information, and as the safety and reliability of our electronic communications become ever more central to the ways in which we interact with each other, business and public bodies, regulators have moved to ensure that those who collect, use and store this data do so in a manner which effectively protects it.

The International community responded most recently in 2005 by developing and standardising a “best practices” Information Security Framework in the form of ISO27002.

In the summer of 2008, RSA commissioned international legal firm and experts in this area, Field Fisher Waterhouse, to review current data protection legislation, arising from the enactment of the EU Data Protection Directive in the EU’s 27 member states, in the context of ISO27002, to help identify how these regulations and best practices interrelate. This white paper, along with the RSA Compliance Navigator, found at www.rsa.com//node.aspx?id=2763 are the results of this work. We hope you find them useful in assisting your regulatory compliance efforts.

ISO/IEC 27002

ISO/IEC 27002 is the current International Standard for public and private sector organisations to establish guidelines and general principles for initiating, implementing, maintaining and improving information security management.

Information and information systems are vitally important business assets which are susceptible to security threats from a wide variety of sources, including computer-assisted fraud, sabotage, espionage, vandalism, fire and flood. As a result, defining, maintaining and improving information security is an essential component for organisations to maintain competitiveness, cash flow, profitability, commercial image and legal compliance.

ISO/IEC 27002 serves as a practical guideline for all organisations to develop security standards and effective security management practices and to build and maintain confidence in organisational activities.

It is Field Fisher Waterhouse LLP’s considered opinion that the proper formulation and implementation of an information security management framework which follows the guidelines set in ISO/IEC 27002 will help organisations to properly comply with Article 17 of the EU Data Protection Directive (‘the Directive’).

The Data Protection Directive and Article 17

The Directive is a legal instrument which protects the fundamental rights and freedoms of natural persons, in particular their right to privacy, with respect to the processing of personal data. It sets minimum standards for the protection of this data which must be adopted by EC member states through implementation of national laws.

As can be seen from the text below, Article 17 of the Directive provides that organisations must implement ‘appropriate technical and organisational measures’ to protect against unlawful or accidental damage or destruction to personal data and that such security measures must be appropriate to the risks facing the data.

Article 17

1. Member States shall provide that the 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.

Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

2. The Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organisational measures governing the processing to be carried out, and must ensure compliance with those measures.
3. The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that:
 - the processor shall act only on instructions from the controller,
 - the obligations set out in paragraph 1, as defined by the law of the Member States in which the processor is established, shall also be incumbent on the processor.
4. For the purposes of keeping proofs, the parts of the contract or the legal act relating to data protection and the requirements relating to the measures referred to in paragraph 1 shall be in writing or in another equivalent form.

It is up to member states to interpret and implement the provisions of the Directive. As can be seen from the supporting table of national laws, Italy, Austria and Spain have taken a highly prescriptive approach to security through their interpretation and implementation of Article 17, whilst some countries, such as Luxembourg, France, Hungary and Greece have merely interpreted and repeated the content of Article 17 in their interpretation and implementation.

In between both these interpretations, countries such as the United Kingdom, Ireland and Lithuania have adopted a 'half-way house' approach.

As a result, for the purposes of adopting best practice, a data controller should look to the totality of national laws implemented around Europe, because collectively, they provide an overall best practice approach to implementation of the ISO/IEC 27002 International Standard.

Implications of Compliance with Article 17

The Directive is structured around key principles and the obligation to comply with these principles rests with the 'data controller' – in many instances this will be an organisation, which will have the power to control the manner and processing of the personal data.

It follows that if an organisation implements and maintains effective policies to comply with its obligations under Article 17, compliance with other obligations under the Directive, including the key principles, will also follow.

For example, one of the key principles requires data to be 'accurate and, where necessary, kept up to date', ensuring inaccurate or incomplete data is 'erased or rectified':

Article 6

1. Member States shall provide that personal data must be:
 - (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified.

It follows that data which is properly protected under an effective security framework, as required under Article 17, is increasingly likely to satisfy this requirement, limiting the possibility of compromised or erroneous data having to be removed.

Implementing and maintaining effective policies to comply with Article 17 obligations can prepare the way to compliance with other obligations under the Directive, including the key principles.

Similarly, another principle under Article 6 requires personal data to be:

- (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.

Clearly, secured data which has not been compromised by accidental or unlawful means, will allow for the efficient identification of individuals and the prompt identification and removal of this data when it is no longer required.

Finally, Article 25 of the Directive, which concerns the transfer of personal data to 'third countries' states:

1. The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.

For these purposes, a 'third country' refers to a country situated outside the European Economic Area. Compliance with ISO/IEC 27002 and Article 17, through implementation of an appropriate security framework, would limit infringement of Article 25, where for example data is accidentally transferred across a transborder network to a country where an 'adequate level of protection' is not provided for.

Conclusion

The implementation of a considered information security framework which ensures compliance with ISO/IEC 27002 and therefore Article 17 of the Directive will function as an enabler for all organisations, helping to achieve business aims whilst reducing the security and data protection risks which can undermine an organisation's information assets.

About Field Fisher Waterhouse

Field Fisher Waterhouse LLP is a full-service European law firm with offices in Brussels, Hamburg, Paris and London. With more than 120 partners, over 220 other lawyers and nearly 300 support staff, we assist a wide range of international clients, advising across a full range of legal issues. Our main areas of practice are IP and technology (including a distinct data protection team), corporate and commercial, banking and finance, regulatory and real estate. We also have particular expertise in competition & EU law, dispute resolution, employment, personal injury, public sector and tax.



Appendix. The RSA Compliance Navigator

Transposition of Article 17 of the Data Protection Directive into the law of EU Member States

The following pages contain detail regarding the application of Article 17 to the EU countries, arranged alphabetically.

Article 17

1. Member States shall provide that the 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.

Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

2. The Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organisational measures governing the processing to be carried out, and must ensure compliance with those measures.

3. The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that:

- the processor shall act only on instructions from the controller,
- the obligations set out in paragraph 1, as defined by the law of the Member States in which the processor is established, shall also be incumbent on the processor.

4. For the purposes of keeping proofs, the parts of the contract or the legal act relating to data protection and the requirements relating to the measures referred to in paragraph 1 shall be in writing or in another equivalent form.

Jurisdiction: Austria

Relevant provision transposing Article 17

Federal Act concerning the Protection of Personal Data (Datenschutzgesetz 2000)

Section 11

Paragraph 1

Irrespective of contractual obligations, all processors have the following obligations when using data for a controller:

- (1) to use data only according to the instructions of the controller; in particular, the transmission of the data used is prohibited unless so instructed by the controller;
- (2) to take all required safety measures pursuant to section 14; in particular to employ only operatives who have committed themselves to confidentiality vis-à-vis the processor or are under a statutory obligation of confidentiality;
- (3) to enlist another processor only with the permission of the controller and therefore to inform the controller of this intended enlistment of another processor in such a timely fashion that the controller has the possibility to object;
- (4) insofar as this is possible given the nature of the service processing – to create in agreement with the controller the necessary technical and organisational requirements for the fulfilment of the controller's obligation to grant the right of information, rectification and erasure;
- (5) to hand over to the controller after the end of the service processing all results of processing and documentation containing data or to keep or destroy them on his request;
- (6) to make available to the controller all information necessary to control the compliance with the obligations according to sub-paras 1 to 5.

Paragraph 2

Agreements between the controller and the processor concerning the details of the obligations according to para 1 shall be laid down in writing to perpetuate the evidence.

Section 14

Paragraph 1

Measures to ensure data security shall be taken by all organisational units of a controller or processor that use data. Depending on the kind of data used as well as the extent and purpose of the use and considering the state of technical possibilities and economic justifiability it shall be ensured that the data are protected against accidental or intentional destruction or loss, that they are properly used and are not accessible to unauthorised persons.

Paragraph 2

In particular, the following measures are to be taken insofar as this is necessary with regard to the last sentence of para. 1:

1. The distribution of functions between the organisational units as well as the operatives regarding the use of data shall be laid down expressly,
2. The use of data must be tied to valid orders of the authorised organisational units or operatives,
3. every operative is to be instructed about his duties according to this Federal Act and the internal data protection regulations, including data security regulations,
4. The right of access to the premises of the data controller or processor is to be regulated,

Austria (continued)

5. The right of access to data and programs is to be regulated as well as the protection of storage media against access and use by unauthorised persons,
6. The right to operate the data processing equipment is to be laid down and every device is to be secured against unauthorised operation by taking precautions for the machines and programs used,
7. Logs shall be kept in order that the processing steps that were actually performed, in particular modifications, consultations and transmissions can be traced to the extent necessary with regard to their permissibility,
8. A documentation shall be kept on the measures taken pursuant to sub-paras. 1 to 7 to facilitate control and conservation of evidence.

These measures must, taking into account the technological state of the art and the cost incurred in their execution, safeguard a level of data protection appropriate with regard to the risks arising from the use and the type of data to be protected.

Paragraph 3

Unregistered transmissions from data applications subject to an obligation to grant information pursuant to sect. 26 shall be logged in such a manner that the right of information can be granted to the subject pursuant to sect. 26. Transmissions provided for in the standard ordinance (sect. 17 para. 2 lit. 6) and the model ordinance (sect. 19 para. 2) do not require logging.

Paragraph 4

Logs and documentation data may not be used for purposes that are incompatible with the purpose of the collection – viz., monitoring the legitimacy of the use of the logged and documented data files. In particular, any further use for the purpose of supervising the data subjects whose data is contained in the logged data files, as well as for the purpose of monitoring the persons who have accessed the logged data files, or for any purpose other than checking access rights shall be considered incompatible, unless the data is used for the purpose of preventing or prosecuting a crime according to sect. 278a StGB (criminal organisation) or a crime punishable with a maximum sentence of more than five years imprisonment.

Paragraph 5

Unless expressly provided for otherwise by law, logs and documentation data shall be kept for three years. Deviations from this rule shall be permitted to the same extent that the logged or documented data files may legitimately be erased earlier or kept longer.

Paragraph 6

Data security regulations are to be issued and kept available in such a manner that the operatives can inform themselves about the regulations to which they are subject at any time.

Section 15 Confidentiality of Data

Paragraph 1

Controllers, processors and their operatives – these being the employees and persons comparable to employees – shall keep data from uses of data confidential that have been entrusted or made

accessible to them solely for professional reasons, without prejudice to other professional obligations of confidentiality, unless a legitimate reason exists for the transmission of the entrusted or accessed data (confidentiality of data).

Paragraph 2

Operatives shall transmit data only if expressly ordered to do so by their employer. controllers and processors shall oblige their operatives by contract, insofar as they are not already obliged by law, to transmit data from uses of data only if so ordered and to adhere to the confidentiality of data even after the end of their professional relationship with the controller or processor.

Austria (continued)

Paragraph 3

Controllers and processors may only issue orders for the transmission of data if this is permitted pursuant to the provisions of this Federal Act. They shall inform the operatives affected by these orders about the transmission orders in force and about the consequences of a violation of data confidentiality.

Paragraph 4

Without prejudice to the constitutional right to issue instructions, a refusal to follow an order to transmit data on the grounds that it violates the provisions of this Federal Act shall not be to the operatives detriment.

Jurisdiction: Belgium

Relevant provision transposing Article 17

Belgian Law of 8 December 1992 on Privacy in relation to the Processing of Personal Data as modified by the law of 11 December 1998 implementing Directive 95/46/EC and the law of 26 February 2003

Art. 16

Paragraph 1

If the processing is consigned to a processor, the controller or his representative in Belgium, if such is the case, shall:

- (1) choose a processor providing sufficient guarantees in respect of the technical and organisational measures governing the processing to be carried out;
- (2) supervise the compliance with these measures, in particular by laying them down in contractual stipulations;
- (3) lay down in the contract the responsibility of the processor in respect to the controller;
- (4) agree with the processor that the processor only acts on behalf of the controller and that the processor is bound by the same obligations as by which the controller is bound pursuant to paragraph 3;
- (5) lay down in writing or on electronic carrier the elements of the contract with regard to the protection of data and the requirements with regard to the measures referred to in paragraph 3;

Paragraph 2

The controller or, if such is the case, his representative in Belgium, shall:

- (1) watch carefully that the data are updated, that inaccurate, incomplete and irrelevant data, as well as data that have been obtained or further processed in violation of the Articles 4-8, are corrected or erased;
- (2) take care that the access to the data and possibilities of processing for the persons who are acting under his authority, are limited to what is necessary for the fulfilment of their duties or for the requirements of the service;
- (3) notify all persons acting under his authority about the provisions of this law and its implementing decrees, as well as about all relevant provisions in respect of the protection of the privacy with regard to the processing of personal data;
- (4) ascertain that the programmes for the automatic processing of personal data are in accordance with the statements in the notification referred to in Article 17 and that no unlawful use is made thereof.

Paragraph 3

Any person acting under the authority of the controller or of the processor, as well as the processor himself having access to the personal data, may only process them on the instructions of the controller, except for the case of an obligation imposed by or by virtue of a law, decree or ordinance.

Belgium (continued)

Paragraph 4

In order to guarantee the security of personal data the controller or, if such is the case, his representative in Belgium, as well as the processor shall take the appropriate technical and organisational measures that are necessary for the protection of personal data against accidental or unauthorised destruction, accidental loss, as well as against alteration of, access to and any other unauthorised processing of personal data.

These measures shall ensure an appropriate level of security taking into account the state of the art in this field and the cost of implementing the measures on the one hand, and the nature of the data to be protected and the potential risks on the other hand.

On the advice of the Commission for the protection of privacy the King may promulgate appropriate standards in the matter of informatics security for all or certain categories of processing.

Jurisdiction: Bulgaria

Relevant provision transposing Article 17

Law for the protection of Personal Data (2001)

Article 23

Paragraph 1

The personal data administrator must implement appropriate technical and organisational measures to protect the data against accidental or unlawful destruction, or against accidental loss, unauthorised access, alteration or dissemination, and against other unlawful forms of processing.

Paragraph 2

The administrator shall implement special protection measures where processing involves the transmission of data over an electronic network.

Paragraph 3

Measures referred to in paragraph (1) and paragraph (2) shall take into account state-of-the-art technology and ensure a level of security corresponding to the risks involved in processing, and the nature of the data to be protected.

Paragraph 4

The measures referred to in paragraph (1) and paragraph (2) shall be determined in an instruction issued by the personal data administrator.

Paragraph 5

The Commission shall specify the minimum level of technical and organisational measures, as well as the admissible type of protection in a regulation. Such regulation shall be published in the State Gazette.

Article 24

Paragraph 1

Administrators may process data on their own or through assignment to data processors. When this is needed for organisational reasons, the processing may be assigned to more than one data processor with a view to, inter alia, to delimitate their specific tasks.

Bulgaria (continued)

Paragraph 2

Where the data processing is not performed by the administrator, the latter shall designate the data processor and provide sufficient data protection guarantees.

Paragraph 3 (repealed)

Paragraph 4

The relationship between the administrator and the personal data processor must be governed by a piece of legislation, a written contract or another act of the administrator defining the scope of duties assigned by the administrator to the data processor.

Paragraph 5

The administrator shall be jointly and severally liable for any damages caused to any third party resulting from any action or failure to act on behalf of the data processor.

Paragraph 6

The personal data processor or any person acting under the guidance of the administrator or of the processor who has access to personal data may process them only on instructions from the administrator, unless otherwise provided for by law.

Article 25

Paragraph 1

Upon the achievement of the purpose of personal data processing, the personal data administrator must:

- (1) either destroy the data, or
- (2) having given prior notification to the Commission, transfer them to another administrator provided that such transfer is provided for in a law and the purposes of processing are identical.

Paragraph 2

Upon the achievement of the intended purposes of personal data processing, the personal data administrator shall store data only in the cases laid down by law.

Paragraph 3

In cases where, having achieved the purpose of personal data processing, the administrator wishes to store the personal data processed as anonymous data for historical, statistical or research purposes, it must inform the Commission thereof.

Paragraph 4

The Commission for Personal Data Protection may prohibit the storage of data for the purposes under Paragraph 3 if the administrator has failed to provide sufficient protection of the anonymous storage of the data processed.

Paragraph 5

The decision of the Commission under Paragraph 4 shall be subject to appeal before the Supreme Administrative Court. Where the Supreme Administrative Court fails to grant an appeal against the decision of the Commission, the personal data administrator shall destroy the data.

Jurisdiction: Cyprus

Relevant provision transposing Article 17

The Processing of Personal Data (Protection of Individuals) Law (138/2001)

Section 10

Subsection 1

The processing of data is confidential. It shall be carried out only by persons acting under the instructions from the controller.

Subsection 2

For carrying out the processing, the controller must select persons who possess appropriate qualifications and who provide sufficient guarantees as regards technical knowledge and personal integrity for the observance of confidentiality.

Subsection 3

The controller must take the appropriate organizational and technical measures for the security of data and their protection against accidental or unlawful destruction, accidental loss, alteration, unauthorised dissemination or access and any other form of unlawful processing. Such measures shall ensure a level of security which is appropriate to the risks involved in the processing and the nature of the data processed.

The Commissioner gives, from time to time, directions with regard to the degree of security of the data and to the measures of protection required to be taken for every category of data, taking also into account technological developments.

Subsection 4

If processing is performed by the processor, the assignment for the processing must be made in writing. The assignment must provide that the processor shall perform the processing only upon instructions from the controller and that the remaining obligations set out in this section shall also lie on the processor.

Jurisdiction: Czech Republic

Relevant provision transposing Article 17

Personal Data Protection Act 101 of April 4, 2000 on the Protection of Personal Data and on Amendment to Some Acts

Article 6

Where authorization does not follow from a legal regulation, the controller must conclude with the processor an agreement on personal data processing. The agreement must be made in writing. In particular, the agreement shall explicitly stipulate the scope, purpose and period of time for which it is concluded and must contain guarantees by the processor related to technical and organisational securing of the protection of personal data.

Article 13

- (1) The controller and the processor shall be obliged to adopt measures preventing unauthorised or accidental access to personal data, their alteration, destruction or loss, unauthorised transmission, other unauthorised processing, as well as other misuse of personal data. This obligation shall remain valid after terminating personal data processing.
- (2) The controller or the processor shall be obliged to develop and to document the technical-organisational measures adopted and implemented to ensure the personal data protection in accordance with the law and other legal regulations.
- (3) In the framework of measures pursuant to paragraph (1), the controller or the processor perform a risk assessment concerning

Czech Republic (continued)

- (a) the carrying out of instructions for personal data processing by persons who have immediate access to the personal data,
 - (b) prevention of unauthorized persons' access to personal data and means for their processing,
 - (c) prevention of unauthorized reading, creating, copying, transferring, modifying or deleting of records containing personal data, and
 - (d) measures enabling to determine and verify to whom the personal data were transferred.
- (4) In the area of automatic processing of personal data, the controller or processor shall, in the framework of measures under paragraph 1, be obliged to
- (a) ensure that the systems for automatic processing of personal data are used only by authorized persons,
 - (b) ensure that the natural persons authorized to use systems for automatic processing of personal data have access only to the personal data corresponding to their authorization, and this on the basis of specific user authorizations established exclusively for these persons,
 - (c) make electronic records enabling to identify and verify when, by whom and for what reason the personal data were recorded or otherwise processed, and
 - (d) prevent any unauthorized access to data carriers.

Jurisdiction: Denmark

Relevant provision transposing Article 17

Act on Processing of Personal Data (Act No. 429 of 31 May 2000)

Title IV Security, Chapter 11,

Section 41

Subsection 1

Individuals, companies etc. performing work for the controller or the processor and who have access to data may process these only on instructions from the controller unless otherwise provided by law or regulations.

Subsection 2

The instruction mentioned in subsection (1) may not restrict journalistic freedom or impede the production of an artistic or literary product.

Subsection 3

The controller shall implement appropriate technical and organizational security measures to protect data against accidental or unlawful destruction, loss or alteration and against unauthorized disclosure, abuse or other processing in violation of the provisions laid down in this Act. The same shall apply to processors.

Subsection 4

As regards data which are processed for the public administration and which are of special interest to foreign powers, measures shall be taken to ensure that they can be disposed of or destroyed in the event of war or similar conditions.

Subsection 5

The Minister of Justice may lay down more detailed rules concerning the security measures mentioned in subsection (3).

Section 42

Denmark (continued)

Subsection 1

Where a controller leaves the processing of data to a processor, the controller shall make sure that the processor is in a position to implement the technical and organizational security measures mentioned in section 41 (3) to (5), and shall ensure compliance with those measures.

Subsection 2

The carrying out of processing by way of a processor must be governed by a written contract between the parties. This contract must stipulate that the processor shall act only on instructions from the controller and that the rules laid down in section 41 (3) to (5) shall also apply to processing by way of a processor. If the processor is established in a different Member State, the contract must stipulate that the provisions on security measures laid down by the law in the Member State in which the processor is established shall also be incumbent on the processor.

Jurisdiction: Estonia

Relevant provision transposing Article 17

Personal Data Protection Act (12 February 2003)

Section 18

Personal data processing requirements

In the processing of personal data, chief processors and authorised processors are required to:

- (1) promptly erase or block personal data unnecessary for the given purposes unless otherwise prescribed by law;
- (2) ensure that personal data are correct and, if necessary for the given purposes, up to date;
- (3) block incomplete and inaccurate personal data and immediately take the necessary measures for the amendment or rectification of the data;
- (4) store inaccurate data with a notation concerning their period of use together with accurate data;
- (5) block personal data which are contested on the basis of accuracy until the accuracy of the data is verified or the accurate data are determined.

Section 19

Organisational, physical and IT security measures to protect personal data

Subsection 1

In order to protect personal data, chief processors and authorised processors are required to take organisational, physical and IT security measures:

- (1) as regards the integrity of the data, against accidental or intentional unauthorised alteration of data;
- (2) as regards the availability of the data, against accidental loss and intentional destruction and against prevention of access to the data for entitled persons;
- (3) as regards the confidentiality of the data, against unauthorised processing.

Subsection 2

In the processing of personal data, chief processors and authorised processors are required to:

- (1) prevent the access of unauthorised persons to equipment used for processing personal data;
- (2) avoid unauthorised reading, copying and alteration in the data processing system and unauthorised removal of data media;

Estonia (continued)

- (3) prevent the unauthorised recording, alteration or erasure of personal data and ensure that it be subsequently possible to determine when, by whom and which personal data were recorded, altered or erased;
- (4) ensure that every user of a data processing system only has access to personal data permitted to be processed by him or her and to the data processing permitted for him or her;
- (5) ensure the existence of information on the transmission of personal data regarding when, to whom and which personal data were transmitted and the unaltered storage of such data;
- (6) ensure that unauthorised reading, copying, alteration or erasure of personal data is not carried out in the transmission of the personal data by data communication equipment and in the transportation of data media;
- (7) organise the work of enterprises, agencies and associations in a manner that allows compliance with data protection requirements.

Subsection 3

Chief processors and authorised processors are required to maintain records on the devices and software which are under the supervision thereof and used in the processing of personal data and they shall document the following information:

- (1) the name, type and location of the device and the name of the manufacturer of the device;
- (2) the name and version and the name and details of the manufacturer of the software and the location of the documents of the software.

Jurisdiction: Finland

Relevant provision transposing Article 17

Personal Data Act (523/1999)

Chapter 7 – Data Security and storage of personal data

Section 32 – Data Security

Paragraph 1

The controller shall carry out the technical and organisational measures necessary for securing personal data against unauthorised access, against accidental or unlawful destruction, manipulation, disclosure and transfer and against other unlawful processing. The techniques available, the associated costs, the quality, quantity and age of the data, as well as the significance of the processing to the protection of privacy shall be taken into account when carrying out the measures.

Paragraph 2

Anyone who as an independent trader or business operates on the behalf of the controller shall, before starting the processing of data, provide the controller with appropriate commitments and other adequate guarantees of the security of the data as provided in paragraph (1).

Section 33 – Secrecy obligation

Anyone who has gained knowledge of the characteristics, personal circumstances or economic situation of another person while carrying out measures relating to data processing shall not disclose the data to a third person against the provisions of this Act.

Section 34 – Destruction of a personal data file

If a personal data file is no longer necessary for the operations of the controller, it shall be destroyed, unless specific provisions have been issued by an Act or by lower-level regulation on the continued storage of the data contained therein or the file is transferred to be archived in accordance with section 35.

Jurisdiction: France

Relevant provision transposing Article 17

Act No 78-17 on Data Processing, Data Files and Individual Liberties (6 January 1978) (Amended by Act of 6 August 2004)

Article 34

Paragraph 1

The data controller shall take all useful precautions, with regard to the nature of the data and the risks of the processing, to preserve the security of the data and, in particular, prevent their alteration and damage, or access by non-authorized third parties.

Paragraph 2

Decrees taken upon an opinion of the ‘Commission nationale de l’informatique et des libertés’ may determine the technical requirements that the processing mentioned in sub-section (2) [processing necessary for the protection of human life with the impossibility of obtaining consent] and sub-section (6) [processing necessary to medicine and administration of care] of Section II of Article 8 should meet.

Jurisdiction: Germany

Relevant provision transposing Article 17

Federal Data Protection Act (15 November 2006)

Section 5 – Confidentiality

Persons employed in data processing shall not collect, process or use personal data without authorisation (confidentiality). On taking up their duties such persons, in so far as they work for private bodies, shall be required to give an undertaking to maintain such confidentiality. This undertaking shall continue to be valid after termination of their activity.

Section 9 – Technical and Organisational Measures

Public and private bodies processing personal data either on their own behalf or on behalf of others shall take the technical and organisational measures necessary to ensure the implementation of the provisions of this Act, in particular the requirements set out in the annex to this Act. Measures shall be required only if the effort involved is reasonable in relation to the desired level of protection.

Annex 9

Where personal data are processed or used automatically, the internal organisation of authorities or enterprises is to be arranged in such a way that it meets the specific requirements of data protection. In particular, measures suited to the type of personal data or data categories to be protected shall be taken:

- (1) to prevent unauthorised persons from gaining access to data processing systems with which personal data are processed or used (access control)
- (2) to prevent data processing systems from being used without authorisation (access control)
- (3) 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 without authorisation in the course of processing or use and after storage (access control)
- (4) 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)

Germany (continued)

- (5) 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)
- (6) 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)
- (7) to ensure that personal data are protected from accidental destruction or loss (availability control)
- (8) to ensure that data collected for different purposes can be processed separately.

Jurisdiction: Greece

Relevant provision transposing Article 17

Law 2472/1997 on the Protection of Individuals with regard to the Processing of Personal Data

Article 10(3)

The Controller is obliged to take the appropriate organisational and technical measures for the security of the data and their protection against accidental or unlawful destruction, accidental loss, alteration, illegal disclosures to the public or access and any other form of unlawful processing. All the security precautions should ensure a security level commensurate with the risks arising from the processing itself and the nature of the data being processed. Without prejudice to other provisions, the Authority, in accordance to Article 19 (1) (k) will offer instructions and issue regulations in reference to the security level of the data and of the computer and information infrastructure, the security measures required for each category and processing of the data, as well as the use of technology for the enhancement of privacy.

Jurisdiction: Hungary

Relevant provision transposing Article 17

Act LXIII of 1992 on the Protection of Personal Data and Public Access to Data of Public Interest

Article 10 – Data Security

Paragraph 1

The data controller and, within its scope of activities the technical data processor, shall ensure data security and shall take all technical and organisational measures and elaborate the rules of procedure necessary to enforce compliance with this Act and other rules pertaining to data protection and confidentiality.

Paragraph 2

Data shall be protected in particular against unauthorised access, alteration, transfer, making public, deletion or destruction, as well as against accidental destruction or damage. If personal data are transferred via a network or other information technology equipment, the data controller, technical data processor and the operator of the telecommunications or information technology equipment shall take special protective measures to ensure the technical protection of personal data.

Jurisdiction: Ireland

Relevant provision transposing Article 17

Consolidated version of Data Protection Acts 1988 and 2003

Section 2

Subsection 1

A data controller shall, as respects personal data kept by him or her, comply with the following provisions....

(d) appropriate security measures shall be taken against unauthorised access to, or unauthorised alteration, disclosure or destruction of, the data, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Subsection 2

A data processor shall, as respects personal data processed by him, comply with paragraph (d) of subsection (1) of this section.

Section 2C

Subsection 1

In determining appropriate security measures for the purposes of section 2(1)(d) of this Act, in particular (but without prejudice to the generality of that provision), where the processing involves the transmission of data over a network, a data controller –

- (a) may have regard to the state of technological development and the cost of implementing the measures, and
- (b) shall ensure that the measures provide a level of security appropriate to
 - (i) the harm that might result from unauthorised or unlawful processing, accidental or unlawful destruction or accidental loss of, or damage to, the data concerned, and
 - (ii) the nature of the data concerned.

Subsection 2

A data controller or data processor shall take all reasonable steps to ensure that –

- (a) persons employed by him or her, and
- (b) other persons at the place of work concerned, are aware of and comply with the relevant security measures aforesaid.

Subsection 3

Where processing of personal data is carried out by a data processor on behalf of a data controller, the data controller shall:

- (a) ensure that the processing is carried out in pursuance of a contract in writing or in another equivalent form between the data controller and the data processor and that the contract provides that the data processor carries out the processing only on and subject to the instructions of the data controller and that the data processor complies with obligations equivalent to those imposed on the data controller by section 2(1)(d) of this Act,
- (b) ensure that the data processor provides sufficient guarantees in respect of the technical security measures, and organisational measures, governing the processing, and
- (c) take reasonable steps to ensure compliance with those measures.

Jurisdiction: Italy

Relevant provision transposing Article 17

Personal Data Protection Code Legislative Decree no. 196 of 30 June 2003

Section 31

Personal data undergoing processing shall be kept and controlled, also in consideration of technological innovations, of their nature and the specific features of the processing, in such a way as to minimise, by means of suitable preventative security measures, the risk of their destruction or loss, whether by accident or not, of unauthorized access to the data or of processing operations that are either unlawful or inconsistent with the purposes for which the data have been collected.

Section 32

Paragraph 1

The provider of a publicly available electronic communications service shall take suitable technical and organisational measures under Section 31 that are adequate in the light of the existing risk, in order to safeguard security of its services and integrity of traffic data, location data and electronic communications against any form of unauthorised utilisation or access.

Paragraph 2

Whenever security of service or personal data makes it necessary to also take measures applying to the network, the provider of a publicly available electronic communications service shall take those measures jointly with the provider of the public communications network. Failing an agreement between said providers, the dispute shall be settled, at the instance of either provider, by the Authority for Communications Safeguards in pursuance of the arrangements set out in the legislation in force.

Paragraph 3

In case of a particular risk of a breach of network security, the provider of a publicly available electronic communications service shall inform subscribers and, if possible, users concerning said risk and, when the risk lies outside the scope of the measures to be taken by said provider pursuant to paragraphs 1 and 2, of all the possible remedies including an indication of the likely costs involved. This information shall be also provided to the Garante and the Authority for Communications Safeguards.

Section 33

Within the framework of the more general security requirements referred to in Section 31, or else provided for by specific regulations, data controllers shall be required in any case to adopt the minimum security measures pursuant either to this Chapter or to Section 58(3) in order to ensure a minimum level of personal data protection.

Section 34

Paragraph 1

Processing personal data by electronic means shall only be allowed if the minimum security measures referred to below are adopted in accordance with the arrangements laid down in the technical specifications as per Annex B:

- a) computerised authentication,
- b) implementation of authentication credentials management procedures,
- c) use of an authorisation system,
- d) regular update of the specifications concerning scope of the processing operations that may be performed by the individual entities in charge of managing and/or maintaining electronic means,
- e) protection of electronic means and data against unlawful data processing operations, unauthorised access and specific software,

Italy (continued)

- f) implementation of procedures for safekeeping backup copies and restoring data and system availability,
- g) keeping an up-to-date security policy document,
- h) implementation of encryption techniques or identification codes for specific processing operations performed by health care bodies in respect of data disclosing health and sex life.

Section 35

Paragraph 1

Processing personal data without electronic means shall only be allowed if the minimum security measures referred to below are adopted in accordance with the arrangements laid down in the technical specifications as per Annex B:

- a) regular update of the specifications concerning scope of the processing operations that may be performed by the individual entities in charge of the processing and/or by the individual organisational departments,
- b) implementing procedures such as to ensure safekeeping of records and documents committed to the entities in charge of the processing for the latter to discharge the relevant tasks,
- c) implementing procedures to keep certain records in restricted-access filing systems and regulating access mechanisms with a view to enabling identification of the entities in charge of the processing.

Section 36

Paragraph 1

The technical specifications as per Annex B concerning the minimum measures referred to in this Chapter shall be regularly updated by a decree of the Minister of Justice issued in agreement with the Minister for Innovation and Technologies by having regard to both technical developments and the experience gathered in this sector.

Annex B

Processing by Electronic Means

The following technical arrangements to be implemented by the data controller, data processor — if nominated — and person(s) in charge of the processing whenever data are processed by electronic means:

Computerised Authentication System

1. Persons in charge of the processing shall be allowed to process personal data by electronic means if they are provided with authentication credentials such as to successfully complete an authentication procedure relating either to a specific processing operation or to a set of processing operations.
2. Authentication credentials shall consist in an ID code for the person in charge of the processing as associated with a secret password that shall only be known to the latter person; alternatively, they shall consist in an authentication device that shall be used and held exclusively by the person in charge of the processing and may be associated with either an ID code or a password, or else in a biometric feature that relates to the person in charge of the processing and may be associated with either an ID code or a password.
3. One or more authentication credentials shall be assigned to or associated with each person in charge of the processing.
4. The instructions provided to the persons in charge of the processing shall lay down the obligation to take such precautions as may be necessary to ensure that the confidential component(s) in the credentials are kept secret and that the devices used and held exclusively by persons in charge of the processing are kept with due care.
5. Where provided for by the relevant authentication system, a password shall consist of at least eight characters; if this is not allowed by the electronic equipment, a password shall consist of the maximum permitted number of characters. It shall not contain any item that can be easily related to the person in charge of the processing and shall be modified by the latter when it is first used as well as at least every six months thereafter. If sensitive or judicial

Italy (continued)

data are processed, the password shall be modified at least every three months.

6. An ID code, if used, may not be assigned to another person in charge of the processing even at a different time.
7. Authentication credentials shall be de-activated if they have not been used for at least six months, except for those that have been authorised exclusively for technical management purposes.
8. Authentication credentials shall be also de-activated if the person in charge of the processing is disqualified from accessing personal data.
9. The persons in charge of the processing shall be instructed to the effect that electronic equipment should not be left unattended and made accessible during processing sessions.
10. Where data and electronic equipment may only be accessed by using the confidential component(s) of the authentication credential, appropriate instructions shall be given in advance, in writing, to clearly specify the mechanisms by which the data controller can ensure that data or electronic equipment are available in case the person in charge of the processing is either absent or unavailable for a long time and it is indispensable to carry out certain activities without further delay exclusively for purposes related to system operationality and security. In this case, copies of the credentials shall be kept in such a way as to ensure their confidentiality by specifying, in writing, the entities in charge of keeping such credentials. Said entities shall have to inform the person in charge of the processing, without delay, as to the activities carried out.
11. The provisions concerning the authentication system referred to above as well as those concerning the authorisation system shall not apply to the processing of personal data that are intended for dissemination.

Authorisation System

12. Where authorisation profiles with different scope have been set out for the persons in charge of the processing, an authorisation system shall be used.
13. Authorisation profiles for each person or homogeneous set of persons in charge of the processing shall be set out and configured prior to start of the processing in such a way as to only enable access to the data that are necessary to perform processing operations.
14. It shall be regularly verified, at least at yearly intervals, that the prerequisites for retaining the relevant authorisation profiles still apply.

Other Security Measures

15. Within the framework of the regular update — to be performed at least at yearly intervals — of the specifications concerning the scope of the processing operations that are entrusted to the individual persons in charge of the processing as well as to the technicians responsible for management and/or maintenance of electronic equipment, the list of the persons in charge of the processing may also be drawn up by homogeneous categories of task and corresponding authorisation profile.
16. Personal data shall be protected against the risk of intrusion and the effects of programmes as per Section 615-quinquies of the Criminal Code by implementing suitable electronic means to be updated at least every six months.
17. The regular update of computer programmes as aimed at preventing vulnerability and removing flaws of electronic means shall be carried out at least annually. If sensitive or judicial data are processed, such update shall be carried out at least every six months.
18. Organisational and technical instructions shall be issued such as to require at least weekly data back-ups.

Security Policy Document

19. By 31 March of each year, the controller of processing operations concerning sensitive and/or judicial data shall draw up, also by the agency of the data processor, if nominated, a security policy document containing appropriate information with regard to:

Italy (continued)

- 19.1 the list of processing operations concerning personal data,
- 19.2 the distribution of tasks and responsibilities among the departments/divisions in charge of processing data,
- 19.3 an analysis of the risks applying to the data,
- 19.4 the measures to be taken in order to ensure data integrity and availability as well as protection of areas and premises insofar as they are relevant for the purpose of keeping and accessing such data,
- 19.5 a description of the criteria and mechanisms to restore data availability following destruction and/or damage as per point 23 below,
- 19.6 a schedule of training activities concerning the persons in charge of the processing with a view to informing them on the risks applying to the data, the measures that are available to prevent harmful events, the most important features of personal data protection legislation in connection with the relevant activities, the resulting liability and the arrangements to get updated information on the minimum security measures adopted by the data controller. Said training activities shall be planned as of the start of the employment relationship as well as in connection with changes in the task(s) discharged and/or the implementation of new, significant means that are relevant to the processing of personal data,
- 19.7 a description of the criteria to be implemented in order to ensure adoption of the minimum security measures whenever processing operations concerning personal data are externalised in accordance with the Code,
- 19.8 as for the personal data disclosing health and sex life referred to under point 24, the specification of the criteria to be implemented in order to either encrypt such data or keep them separate from other personal data concerning the same data subject.

Additional Measures Applying to Processing of Sensitive or Judicial Data

20. Sensitive or judicial data shall be protected against unauthorised access as per Section 615-ter of the Criminal Code by implementing suitable electronic means.
21. Organisational and technical instructions shall be issued with regard to keeping and using the removable media on which the data are stored in order to prevent unauthorised access and processing.
22. The removable media containing sensitive or judicial data shall be destroyed or made unusable if they are not used; alternatively, they may be re-used by other persons in charge of the processing, who are not authorised to process the same data, if the information previously contained in them is not intelligible and cannot be re-constructed by any technical means.
23. If either the data or electronic means have been damaged, suitable measures shall be adopted to ensure that data access is restored within a specific deadline, which must be compatible with data subjects' rights and not in excess of seven days.
24. Health care bodies and professionals shall process data disclosing health and sex life as contained in lists, registers or data banks in accordance with the mechanisms referred to in Section 22(6) of the Code also in order to ensure that said data are processed separately from the other personal data allowing data subjects to be identified directly. Data concerning genetic identity shall only be processed in protected premises that may only be accessed by such persons in charge of the processing and entities as have been specifically authorised to access them. Containers equipped with locks or equivalent devices shall have to be used in order to remove the data outside the premises reserved for their processing; the data shall have to be encrypted for the purpose of electronically transferring them.

Safeguards and Protections

25. Where a data controller adopts minimum security measures by committing the relevant tasks to external entities, prior to implementing such measures he or she shall require the installing technician(s) to supply a written description of the activities performed by which it is certified that they are compliant with the provisions set out in these technical specifications.

Italy (continued)

26. The circumstance that the security policy document has been drawn up and/or updated shall be referred to in the management report that the data controller may be required to submit together with the relevant balance sheet.

Processing Without Electronic Means

The following technical arrangements to be implemented by the data controller, data processor — if nominated — and person(s) in charge of the processing whenever data are processed without electronic means:

27. The persons in charge of the processing shall be instructed in writing with regard to controlling and keeping, throughout the steps required to perform processing operations, records and documents containing personal data. Within the framework of the regular update — to be performed at least at yearly intervals — of the specifications concerning the scope of the processing operations that are entrusted to the individual persons in charge of the processing, the list of the persons in charge of the processing may also be drawn up by homogeneous categories of task and corresponding authorisation profile.
28. If records and documents containing sensitive or judicial personal data are entrusted to the persons in charge of the processing for the latter to discharge the relevant tasks, said records and documents shall be kept and controlled by the persons in charge of the processing until they are returned so as to prevent unauthorised entities from accessing them; they shall be returned once the relevant tasks have been discharged.
29. Access to archives containing sensitive or judicial data shall be controlled. The persons authorised to access said archives for whatever purpose after closing time shall be identified and registered. If an archive is not equipped with electronic devices for access control or is not placed under the surveillance of security staff, the persons accessing said archive shall have to be authorised in advance.

Jurisdiction: Latvia

Relevant provision transposing Article 17

Personal Data Protection Law as amended December 2006

Section 14

Paragraph 1

A system administrator may entrust personal data processing to a personal data processor provided a written contract is entered into between them.

Paragraph 2

A personal data processor may process personal data entrusted to him or her only within the amount determined in the contract and in conformity with the purposes provided for therein and in accordance with the instructions of the system administrator if they are not in conflict with regulatory enactments.

Paragraph 3

Prior to commencing personal data processing, a personal data processor shall perform safety measures determined by the system administrator for the protection of the system in accordance with the requirements of this Law.

Section 25

Paragraph 1

A system administrator and personal data processor have a duty to use the necessary technical and organisational measures in order to protect personal data and to prevent their illegal processing.

Latvia (continued)

Paragraph 2

A system administrator shall control the form of personal data entered in the personal data processing system and the time of recording and is responsible for the actions of persons who carry out personal data processing.

Section 26

Paragraph 1

The mandatory technical and organisational requirements for the protection of personal data processing systems shall be determined by the Cabinet.

Paragraph 2

Every year State and local government institutions shall submit to the Data State Inspectorate a personal data processing system internal audit findings (also a system risk analysis) and a report regarding measures performed in the field of information security.

Paragraph 3

The Data State Inspectorate in accrediting a person who wishes to perform systems audits in State and local government personal data processing systems shall perform the following in relation to external systems auditors:

- 1) initial accreditation;
- 2) repeated accreditation;
- 3) accreditation for the renewal of activities;
- 4) extension of the time period of the accreditation; and
- 5) issuing of duplicates of accreditation certificates.

Paragraph 4

For the performance of each of the activities referred to in Paragraph three of this Section, a State fee shall be paid according to the procedures and in the amount specified by the Cabinet.

Section 27

Paragraph 1

Natural persons involved in personal data processing shall make a commitment in writing to preserve and not, in an unlawful manner, disclose personal data. Such persons have a duty not to disclose the personal data even after termination of legal employment or other contractually specified relations.

Paragraph 2

A system administrator is obliged to record the persons referred to in Paragraph one of this Section.

Paragraph 3

When processing personal data, a processor of the personal data shall comply with the instructions of the system administrator.

Jurisdiction: Lithuania

Relevant provision transposing Article 17

Law on Legal Protection of Personal Data

Article 24

Paragraph 1

The data controller and data processor must implement appropriate organizational and technical measures intended for the protection of personal data against any accidental or unlawful destruction, alteration, disclosure as well as against any other unlawful processing. These measures must ensure a level of security appropriate to the nature of the data to be protected and the risks represented by the processing and must be specified in a written document or its equivalent (data processing regulations approved by the data controller, a contract concluded by the data controller and the data processor etc).

Paragraph 2

The data controller shall himself process personal data and/ or shall authorize the data processor to do so. If the data controller authorizes the data processor to process personal data, he must choose a processor providing guarantees in respect of adequate technical and organizational data protection measures and ensuring compliance with those measures.

Paragraph 3

When authorizing the data processor to process personal data, the data controller shall stipulate that personal data must be processed only on instructions from the data controller.

Paragraph 4

The relations between the data controller and the data processor who is not the data controller shall be regulated by a written contract except where such relations are provided for by laws or other legal acts.

Paragraph 5

The employees of the data controller, the data processor and their representatives who are processing personal data must keep confidentiality of personal data if these personal data are not intended for public disclosure. This obligation shall continue after leaving the public services, transfer to another position or upon termination of employment or contractual relations.

Jurisdiction: Luxembourg

Relevant provision transposing Article 17

Data Protection Act (2 August 2002 as amended)

Section 22

The controller must implement all appropriate technical and organisational measures to ensure the protection of the data he processes against accidental or unlawful destruction or accidental loss, falsification, unauthorised dissemination or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing².

Jurisdiction: Malta

Relevant provision transposing Article 17

Data Protection Act

Article 25

Paragraph 1

Any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data may only process personal data in accordance with instructions from the controller unless the person is otherwise required to do so by law.

Paragraph 2

The carrying out of processing by way of a processor is to be governed by a contract or other legally binding instrument in a written or in an equivalent form binding the processor to the controller and stipulating in particular that the processor:

- (a) shall act only on instructions from the controller;
- (b) shall take those measures referred to in article 26(1).

Article 26

Paragraph 1

The controller shall implement appropriate technical and organisational measures to protect the personal data that is processed against accidental destruction or loss or unlawful forms of processing thereby providing an adequate level of security that gives regard to the:

- (a) technical possibilities available;
- (b) cost of implementing the security measures;
- (c) special risks that exist in the processing of personal data;
- (d) sensitivity of the personal data being processed.

Paragraph 2

If the controller engages a processor, the controller shall ensure that the processor:

- (a) can implement the security measures that must be taken;
- (b) actually takes the measures so identified by the controller.

Jurisdiction: The Netherlands

Relevant provision transposing Article 17

Personal Data Protection Act of 6 July 2000, containing rules regarding the protection of personal data (Dutch Personal Data Protection Act) as amended

Article 13

The responsible party shall implement appropriate technical and organizational measures to secure personal data against loss or against any form of unlawful processing. These measures shall guarantee an appropriate level of security, taking into account the state of the art and the costs of implementation, and having regard to the risks associated with the processing and the nature of the data to be protected. These measures shall also aim at preventing unnecessary collection and further processing of personal data.

Article 14

Paragraph 1

Where responsible parties have personal data processed for the purposes by a processor, these responsible parties shall make sure that the processor provides adequate guarantees concerning the technical and organizational security measures for the processing to be carried out. The responsible parties shall make sure that these measures are complied with.

Paragraph 2

The carrying out of processing by a processor shall be governed by an agreement or another legal act whereby an obligation is created between the processor and the responsible party.

Paragraph 3

The responsible party shall make sure that the processor:

- (a) processes the personal data in accordance with Article 12(l) and
- (b) complies with the obligations incumbent upon the responsible party under Article 13.

Paragraph 4

Where the processor is established in another country of the European Union, the responsible party shall make sure that the processor complies with the laws of that other country, notwithstanding the provisions of (3) (b).

Paragraph 5

With a view to the keeping of proof, the parties of the agreement or legal act relating to personal data protection and the security measures referred to in Article 13, shall be set down in writing or in another equivalent form.

Jurisdiction: Poland

Relevant provision transposing Article 17

Act of 29 August 1997 on the Protection of Personal Data

Article 31

Paragraph 1

The controller may authorise another subject to carry out the processing of personal data pursuant to a contract concluded in writing.

Paragraph 2

The subject, referred to in paragraph 1 above, may process the data solely within the scope and for the purpose determined in the contract.

Paragraph 3

The subject, referred to in paragraph 1, prior to processing the data shall be obliged to provide security measures protecting the data filing system, as defined in Article 36-39, and to meet the requirements specified in the provisions referred to in Article 39a. With regard to the observance of these provisions the data subject shall bear the liability as the controller.

Paragraph 4

In cases referred to in paragraphs 1 to 3, the liability for compliance with the provisions hereof shall remain with the controller, whereas the contracting party shall not be exempted from the liability in case the data are processed in a way incompatible with the contract.

Paragraph 5

The provisions of Articles 14 – 19 shall apply respectively to supervision over ensuring the compliance of data processing conducted by the subject referred to in paragraph 1 with the provisions on the protection of personal data.

Article 36

Paragraph 1

The controller shall be obliged to implement technical and organisational measures to protect the personal data being processed, appropriate to the risks and category of data being protected, and in particular to protect data against their unauthorised disclosure, takeover by an unauthorised person, processing with the violation of the Act, any change, loss, damage or destruction.

Paragraph 2

The controller shall keep the documentation describing the way of data processing and measures referred to in paragraph 1.

Paragraph 3

The controller shall appoint an administrator of information security who supervises the compliance with security principles referred to in paragraph 1, unless the controller performs these activities by himself.

Jurisdiction: Portugal

Relevant provision transposing Article 17

Data Protection Act (26 October 1998 no. 67)

Article 14 – Security of Processing

Paragraph 1

The 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. Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

Paragraph 2

Where processing is carried out on his behalf the controller must choose a processor providing sufficient guarantees in respect of the technical security measures and organisational measures governing the processing to be carried out, and must ensure compliance with those measures.

Paragraph 3

The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that the processor shall act only on instructions from the controller and that the obligations referred to in 1 shall also be incumbent on the processor.

Paragraph 4

Proof of the will to negotiate, the contract or the legal act relating to data protection and the requirements relating to the measures referred to in 1 shall be in writing in a supporting document legally certified as affording proof.

Article 15 – Special Security Measures

Paragraph 1

The controllers of the data referred to in Articles 7 (2) and Article 8 shall take appropriate measures to:

- a) prevent unauthorised persons from entering the premises used for processing such data (control of entry to the premises);
- b) prevent data media from being read, copied, altered or removed by unauthorised persons (control of data media);
- c) prevent unauthorised input and unauthorised obtaining of knowledge, alteration or elimination of personal data input (control of input);
- d) prevent automatic data processing systems from being used by unauthorised persons by means of data transmission premises (control of use);
- e) guarantee that authorised persons may only access data covered by the authorisation (control of access);
- f) guarantee the checking of the bodies to whom personal data may be transmitted by means of data transmission premises (control of transmission);
- g) guarantee that it is possible to check a posteriori, in a period appropriate to the nature of the processing, the establishment in the regulations applicable to each sector of which personal data are input, when and by whom (control of input);
- h) in transmitting personal data and in transporting the respective media, prevent unauthorised reading, copying, alteration or elimination of data (control of transport).

Portugal (continued)

Paragraph 2

Taking account of the nature of the bodies responsible for processing and the type of premises in which it is carried out, the CNPD may waive the existence of certain security measures, subject to guaranteeing respect for the fundamental rights, freedoms and guarantees of the data subjects.

Paragraph 3

The systems must guarantee logical separation between data relating to health and sex life, including genetic data, and other personal data.

Paragraph 4

Where circulation over a network of the data referred to in articles 7 and 8 may jeopardise the fundamental rights, freedoms and guarantees of their data subjects the CNPD may determine that transmission must be encoded.

Article 16 – Processing by a processor

Any person acting under the authority of the controller or the processor, including the processor himself, who has access to personal data must not process them except on instructions from the controller, unless he is required to do so by law.

Article 17 – Professional secrecy

Paragraph 1

Controllers and persons who obtain knowledge of the personal data processed in carrying out their functions shall be bound by professional secrecy, even after their functions have ended.

Paragraph 2

Members of the CNPD shall be subject to the same obligation, even after their mandate has ended.

Paragraph 3

The provision in the previous numbers shall not exclude the duty to supply the obligatory information according to the law, except when it is contained in filing systems organised for statistical purposes.

Paragraph 4

Officers, agents or staff who act as consultants for the CNPD or its members shall be subject to the same obligation of professional secrecy.

Jurisdiction: Romania

Relevant provision transposing Article 17

Law no. 677/2001 for the Protection of Persons concerning the Processing of Personal Data and Free Circulation of Such Data

Article 19 – Confidentiality of data processing

Any person who acts under authority of the controller or of the processor, including the processor, and who has access to personal data, may not process them unless on the controller's specific instructions, except when the above-mentioned person acts on a legal obligation basis.

Article 20

Paragraph 1

It is the controller's obligation to apply the adequate technical and organisational measures in order to protect the data against accidental or unlawful destruction, loss, alteration, disclosure or unauthorised access, notably if the respective data are committed to the IT net, as against any other form of illegal processing.

Paragraph 2

These measures must ensure, depending on the costs and the processing means employed, adequate security against processing hazards, considering the nature of the data that must be protected. The minimum security requirements shall be elaborated by the supervisory authority and shall be periodically upgraded, according to the technical progress and the accumulated experience.

Paragraph 3

When appointing a processor, the controller has the obligation to nominate a person who presents enough guarantees regarding technical security and the organisational measures concerning the data to be processed. The controller shall also supervise that the nominated person complies with these measures.

Paragraph 4

The supervisory authority may decide, in individual cases, that the controller should adopt additional security measures, except such measures as might affect the guaranteed security of telecommunication services.

Paragraph 5

Data processing performed by an appointed processor shall be initiated following a written contract which should necessarily contain the following:

- (a) the obligation of the empowered person to act only while strictly following instructions received from the controller;
- (b) the fact that the accomplishment of the obligations set out in paragraph (1) also applies to the processor.

Jurisdiction: Slovakia

Relevant provision transposing Article 17

Act on Protection of Personal Data as amended (3 July 2002 no. 428)

Section 15

Paragraph 1

The controller and the processor shall be responsible for security of personal data by protecting them against accidental or unlawful damage or destruction, accidental loss, alteration, unauthorized access and making available, as well as against any other unauthorized forms of processing. For this purpose he shall take due technical, organisational and personal measures adequate to the manner of processing, while he shall take into account above all

- (a) the existing technical means
- (b) the extent of possible risk that could violate security or functionality of the filing system
- (c) confidentiality and importance of the processed personal data.

Paragraph 2

The controller and the processor shall take the measures under Paragraph 1 in the form of a security project of the filing system (hereinafter the ‘Security Project’) and they shall provide its development if

- (a) special categories of personal data under Section 8 are processed in the filing system and the filing system is interconnected with a publicly accessible computer network or it is operated in a computer network interconnected with a publicly accessible computer network
- (b) special categories of personal data under Section 8 are processed in the filing system; in such case the controller and the processor shall only document the taken technical, organisational and personal measures in the extent stipulated by Section 16 Paragraph 3 subparagraph (c) and paragraph 6; or
- (c) the filing system is used for safeguarding the public interest under Section 1 Paragraph 1; the provision of Section 16 shall not apply to development of the Security Project only provided that an obligation to elaborate a Security Project pursuant to a special Act [Act no. 215/2004 Coll] simultaneously applies to the respect case.

Paragraph 3

Upon request of the Office the controller and the processor shall prove the extent and contents of the taken technical, organisational and personal measures under Paragraph 1 or 2.

Paragraph 4

If the subject of the inspection is constituted by the filing systems under Paragraph 2, the Office shall be entitled to request the controller or the processor for submittal or an evaluation report on the outcome of an audit of the filing system’s security (hereinafter the “evaluation report”), provided that there are serious doubts about its security or about practical implementation of the measures referred to in the Security Project. The controller or the processor shall submit the evaluation report, not older than two years, to the Office without undue delay, otherwise he shall provide performance of an audit of the filing system’s security at his own expense and submit an evaluation report within three months from the day of the obligation’s imposition.

Paragraph 5

The audit of the filing system’s security may only be performed by an external, professionally qualified legal or natural person, who did not participate in development of the Security Project of the respective filing system and there are no doubts about its impartiality.

Slovakia (continued)

Section 16

Security Project

Paragraph 1

The Security Project shall define the extent and manner of the technical, organisational and personal measure necessary for elimination and minimizing of the threats and risks affecting the filing system from the viewpoint of impairing its security, reliability and functionality.

Paragraph 2

The Security Project shall be developed in accordance with the basic rules of filing system's security, the issued security standards, legal regulations and international treaties binding for the Slovak Republic.

Paragraph 3

The Security Project shall include above all

- a) a security policy,
- b) analysis of the filing system's security,
- c) security directives.

Paragraph 4

The security policy shall specify the basic security objectives that must be achieved for protection of the filing system against violation of its security and it shall contain above all

- a) specification of the basic security objectives and the minimum required security measures,
- b) specification of the technical, organisational and personal measures for ensuring protection of personal data in the filing system and the manner of their use,
- c) definition of the filing system's environment and its relation to the possible security violation,
- d) definition of the limits determining residual risks.

Paragraph 5

Analysis of the filing system's security shall mean a detailed analysis of the state of the filing system's security containing above all

- a) qualitative risk analysis, within of which the threats affecting individual items of the filing system capable of violating its security or functionality are identified; the result of the qualitative risk analysis shall be a list of threats that could endanger confidentiality, integrity and availability of the processed personal data, while it shall also state the extent of the possible risk, proposals of the measures eliminating or minimizing the affect of the risk and a list of the remaining risks,
- b) use of security standards and determination of other methods and means of the protection of personal data; evaluation of conformity of the proposed security measures with the applied security standards, methods and means shall constitute a part of the analysis of the filing system's security.

Paragraph 6

Security directives shall specify and apply the conclusions resulting from the Security Project to the concrete conditions of the operated filing system and they shall include above all

- a) description of the technical, organisational and personal measures defined in the Security Project and their use in concrete conditions,

Slovakia (continued)

- b) the scope of powers and description of the permitted activities of individual entitled persons, the manner of the identification and authentication in accessing the filing system,
- c) the scope of liability of entitled persons and of the personal data protection official (Section 19),
- d) the manner, form and periodicity of performance of the inspection activities focused on observation of the filing system's security,
- e) procedures during breakdowns, failures and other extraordinary situations including preventive measures for restricting the occurrence of extraordinary situations and possibilities of an effective restoration of the state before the breakdown.

Section 17

The controller or the processor shall be obliged to advise the entitled persons on the rights and obligations stipulated by this Act and on the liability for their breach. The controller or the processor shall advise on the above before giving the first instruction to the entitled person to perform any processing operation with the personal data. The entitled person shall confirm the advice by his signature; the controller or the processor shall make a written record of the advice.

Section 18

Paragraph 1

The controller and the processor shall be obliged to maintain secrecy about the personal data which they process. The obligation to maintain secrecy also applies after termination of the processing. The obligation to maintain secrecy shall not apply to them if pursuant to a special Act it is necessary for fulfilment of the tasks of the law enforcement agencies; this shall not affect provisions of special Acts³.

Paragraph 2

The entitled person shall be obliged to maintain secrecy about the personal data which he comes across; he must not use them even for his personal needs and he must not make them public, provide them or make them available to anybody without consent of the controller.

Paragraph 3

The obligation to maintain secrecy under Paragraph 2 shall also apply to other natural persons, who come across the personal data at the controller's or processor's place within the framework of their activities (e.g. maintenance and service of the technical means).

Paragraph 4

The obligation to maintain secrecy under Paragraph 2 shall also apply after termination of the function of the entitled person or after termination of his employment relationship or similar labour relation, as well as the civil service employment relationship or the relation under Paragraph 3.

Paragraph 5

Paragraphs 1 to 4 and the obligation to maintain secrecy imposed on controllers, processors and entitled persons pursuant to special regulations shall not apply in respect of the Office in the course of fulfilment of its task (Sections 38 to 44).⁴

³ E.g. Section 40 of the Act of the National Council of the Slovak Republic No. 566/1992 Coll. on National Bank of Slovakia, as amended by the Act No. 149/2001 Coll.

⁴ E.g. Section 6 Paragraph 1 of the Act No. 150/2001 Coll. on Tax Authorities and on Changing and Amending of the act No. 440/2000 Coll. on Reports of Financial Control, Section 14 of the Act No. 330/2000 Coll. on Security Exchange, Section 134 of the Act No. 566/2001 Coll. on Securities and Investment Services and on Changing and Amending of Some Acts (Securities Act), Sections 91 to 93 of the Act No. 483/2001 Coll. on Banks and on Changing and Amending of Some Acts, Section 24 of the Act No.

Jurisdiction: Slovenia

Relevant provision transposing Article 17

Personal Data Protection Act 2004

Article 24

Paragraph 1

Security of personal data comprises organisational, technical and logical-technical procedures and measures to protect personal data, and to prevent accidental or deliberate unauthorised destruction, modification or loss of data, and unauthorised processing of such data:

- (1) by processing premises, equipment and systems software, including input-output units;
- (2) by protecting software applications used to process personal data;
- (3) by preventing unauthorised access to personal data during transmission thereof, including transmission via telecommunications means and networks;
- (4) by ensuring effective methods of blocking, destruction, deletion or anonymisation of personal data;
- (5) by enabling subsequent determination of when individual personal data were entered into a filing system, used or otherwise processed, and who did so, for the period covered by statutory protection of the rights of an individual due to unauthorised supply or processing of personal data.

Paragraph 2

In cases of processing of personal data accessible over telecommunications means or network, the hardware, systems software and software applications must ensure that the processing of personal data in filing systems is within the limits of authorisations of the data recipient.

Paragraph 3

The procedures and measures to protect personal data must be adequate in view of the risk posed by processing and the nature of the specific personal data being processed.

Paragraph 4

Functionaries, employees and other individuals performing work or tasks at persons that process personal data shall be bound to protect the secrecy of personal data with which they become familiar in performing their functions, work and tasks. The duty to protect the secrecy of personal data shall also be binding on them after termination of their function, work or tasks, or the performance of contractual processing services.

Article 25

Paragraph 1

Data controllers and data processors shall be bound to ensure the protection of personal data in the manner set out in Article 24 of this Act.

Paragraph 2

Data controllers shall prescribe in their internal acts the procedures and measures for security of personal data and shall define the persons responsible for individual filing systems and the persons who, due to the nature of their work, shall process individual personal data.

24/1991 Coll. on Insurance Business, as amended, Section 81 e) and Section 240 Paragraph 5 of the Act No. 311/2001 Coll. Labour Code, Section 53 Paragraph 1 Subparagraph e) of the Act No. 312/2001 Coll. on Civil Service and on Changing and Amending of Some Acts, Section 9 Paragraph 2 Subparagraph b) of the Act No. 313/2001 Coll. on Public Service, section 8 of the Act No. 367/2000 Coll., Section 80 of the Act of the National Council of the Slovak Republic No. 171/1993., as amended, Section 15 Paragraphs 2 and 3 of the Act of the National Council of the Slovak Republic No. 38/1993 Coll. on Organisation of the Constitutional Court of the Slovak Republic, on Proceedings before It and on Status of Its Judges.

Jurisdiction: Spain

Relevant provision transposing Article 17

Organic Law 15/1999 of 13 December on the Protection of Personal Data

Article 9

Paragraph 1

The controller of, where applicable, the processor shall adopt the technical and organisational measures necessary to ensure the security of the personal data and prevent their alteration, loss, unauthorised processing or access, having regard to the state of the art, the nature of the data stored and the risks to which they are exposed by virtue of human action or the physical or natural environment.

Paragraph 2

No personal data shall be recorded in files which do not meet the conditions laid down by rules regarding their integrity and security, as well as the rules governing the processing centres, premises, equipment, systems and programs.

Paragraph 3

Rules shall be laid down governing the requirements and conditions to be met by the files and the persons involved in the data processing referred to in Article 7 of this Law.

Royal Decree 1720/2007 of 21 December which approves the regulation implementing Organic Law 15/1999 of 13 December on the Protection of Personal Data

Title VIII: Regarding security measures in the processing of personal data

Chapter 1: General Provisions

Article 79

Data controllers and data processors shall implement the security measures pursuant to the provisions of this Title, whatever may be the system of processing.

Article 80

There are three levels of applicable security measures for files and processing: basic, medium and high.

Article 81

1. All files or processing of personal data shall adopt the basic-level security measures.
2. The following files or processing of personal data shall also implement medium-level security measures, in addition to the basic-level security measures:
 - a) Those relating to criminal or administrative offences;
 - b) Those whose operation is subject to Article 29 of Organic Law 15/1999, of 13 December;
 - c) Those controlled by the tax administrations and relating to the exercise of the powers of taxation;
 - d) Those controlled by financial institutions for purposes related to the provision of financial services;
 - e) Those controlled by the Management Agencies and Common Services of the Social Security and relating to the exercise of their powers. Similarly, those controlled by the Mutual Funds for accidents at work and occupational illness associated with the Social Security;
 - f) Those containing a set of personal data that provide a definition of the characteristics or identity of citizens and which permit the evaluation of specific aspects of their identity or behaviour.

Spain (continued)

3. The following files or processing of personal data shall also implement high-level security measures, in addition to the basic- and medium-level measures:
 - a) Those referring to data on ideology, trade union membership, religion, beliefs, racial origin, health or sex life;
 - b) Those containing or referring to data collected for security forces without the consent of the data subjects;
 - c) Those concerning data arising from acts of gender-based violence.
4. As well as the basic- and medium-level security measures, the high-level security measure contained in Article 103 hereof shall be applied to files controlled by operators providing electronic communications services to the public or that exploit public electronic communications networks with regard to traffic and location data.
5. The implementation of basic-level security measure shall be sufficient for files or processing of data on ideology, trade union membership, religion, beliefs, racial origin, health or sex life if:
 - a) The data are used for the sole purpose of carrying out a monetary transfer to organisations to which the data subjects are associated or are members of;
 - b) Regarding non-automated files or processing that incidentally contain such data that have no relation with its purpose.
6. Basic-level security measures may also be implemented in the files or processing that contain data relating to health, referring exclusively to the degree of disability or the simple declaration of the condition of disability of the data subject, for the purpose of fulfilling public duties.
7. The measures included in each of the aforesaid levels are the minimum that can be applied, without prejudice to the current specific regulations or legal provisions that may be applicable in each case or those adopted on the initiative of the data controller.
8. For the purposes of facilitating compliance with the provisions herein, when an information system has files or processing that, depending on their specific purpose or use, or on the nature of the data they contain, require the application of a level of security measures different to that of the main system, they may be separated from the latter, with the relevant level of security measures being applicable in each case and whenever the relevant data and users with access to them can be delimited, and this is recorded in the security document.

Article 82

1. When the data controller provides access to the data, to the supports that contain them or to the resources of the information system that processes them, for a data processor providing his services on the premises of the data controller this shall be recorded in the security document of the latter. The staff of the data processor shall commit themselves to the fulfilment of the security measures set out therein.
2. If the service is provided by the data processor on his own premises, outside those of the data controller, he shall draw up a security document under the terms required by Article 88 hereof or complete that already drafted, if appropriate, identifying the filing system or processing and the data controller and including the security measures that are to be implemented in relation to such processing.
3. In any case, access to the data by the data processor shall be subject to the security measures set out herein.

Article 83

The data controller shall adopt the adequate measures to limit access of staff to personal data, to the supports that contain them or to the resources of the information system, for the execution of tasks that do not involve the processing of personal data.

With regard to external personnel, the service provision contract shall expressly record the prohibition of access to the personal data and the obligation of confidentiality regarding the data that personnel may become aware of due to provision of the service.

Spain (continued)

Article 84

The authorisations in this Title that are attributed to the data controller may be delegated to the persons designated for this purpose. The security document shall record the persons able to grant such authorisations as well as those who are delegated. Under no circumstances shall such delegation imply a delegation of the liability corresponding to the data controller.

Article 85

The applicable security measures for the access to personal data through communications networks, whether public or not, shall guarantee a level of security equivalent to that applicable to local access, pursuant to the criteria established in Article 80.

Article 86

1. When the personal data are stored in portable devices or are processed outside the premises of the data controller or the data processor, the data controller shall necessarily give his prior authorisation, and in any case shall guarantee the level of security relevant to the type of file processed.
2. The authorisation to which the previous paragraph refers shall be recorded in the security document and may be established for a user or for a user profile and shall set out the duration of its validity.

Article 87

1. Temporary filing systems or copies of documents that have been created exclusively for the execution of temporary or auxiliary tasks shall comply with the relevant level of security pursuant to the criteria established in Article 81.
2. All temporary filing systems or working copies thus created shall be erased or destroyed once they are no longer necessary for the purposes for which they were created.

Chapter II: Security Document

Article 88

1. The data controller shall draw up a security document including the technical and organisational measures according to current legislation on security that shall be binding on the personnel with access to the information systems.
2. The security document shall be of general application to all the filing systems or processing, or individual for each filing system or processing. Different security documents may be drawn up grouping filing systems or processing according to the processing system used for their organisation, or bearing in mind the organisational criteria of the data controller. In any case, it shall be considered an internal document of the organisation.
3. The document shall contain, at least, the following aspects:
 - a) Scope of application of the document with detailed specifications of the protected resources;
 - b) Measures, regulations, protocols for action, rules and standards aimed at guaranteeing the level of security required herein;
 - c) Tasks and obligations of the staff in relation to the processing of personal data included in the filing system;
 - d) Structure of the filing systems with personal data and description of the information systems that process them;
 - e) Procedure of notification, management and response to incidents;
 - f) The procedures for making backup copies and recovery of the data in the automated filing systems or processing;
 - g) The measures that shall necessarily be adopted for the transport of the supports or documents, as well as for their destruction, or if appropriate, their re-use.

Spain (continued)

4. In the event of the medium- or high-level security measures provided in this Title being applicable to the filing systems, the security document shall also contain:
 - a) The identification of the data controller(s);
 - b) The monitoring that shall be carried out from time to time to verify fulfilment of that provided therein.
5. In the event of data processing by third parties, the security document shall contain the identification of the files or processing that have been commissioned with express reference to the contract or document regulating the conditions of the commission, as well as the identification of the data controller and the duration of validity of the commission.
6. In those cases where the personal data of a filing system or processing are included and processed exclusively in the systems of the data processor, the data controller shall record this in the security document. When this affects part or all of the filing systems or processing of the data controller, he shall delegate the security document to the data processor, with the exception of that relating to the data contained in his own resources. This fact shall be expressly indicated in the contract executed under Article 12 of Organic Law 15/1999, of 13 December, specifying the affected files or processing.

In this case, reference shall be made to the security document of the data processor for the purpose of fulfilment of that provided herein.

7. The security document shall be kept up-to-date at all times and shall be reviewed whenever any material changes are made to the information system, the processing system used, its organisation, the contents of the information included in the filing systems or processing or, if appropriate, as a result of the periodic monitoring. In any case, a change shall be deemed material when it may have repercussions on the fulfilment of the implemented security measures.
8. The content of the security document shall be adapted, at all times, to the current provisions of the security of personal data.

Chapter III: Security Measures Applicable to Automated Filing Systems and Processing

Section One: Basic-level security measures

Article 89

1. The functions and obligations of each of the users or profiles of users with access to the personal data and to the information systems shall be clearly defined and documented in the security document.

The monitoring functions or authorisations delegated by the data controller of the filing system or processing shall also be defined.
2. The data controller shall adopt the necessary measures so that the staff members understand the security regulations that affect the performance of their functions as well as the consequences that may arise in the event of non-performance.

Article 90

There shall be a procedure for notification and management of incidents that affect personal data and a register established for recording the type of incident, the moment it occurred, or if appropriate, was detected, the person making the notification, to whom it was communicated, the effect arising from it and the corrective measures applied.

Article 91

1. The users shall only have access to those resources required for the performance of their functions.
2. The data controller shall ensure there is an updated list of users and user profiles, and the authorised accesses for each one.

Spain (continued)

3. The data controller shall establish mechanisms to avoid a user being able to access resources with rights other than those authorised.
4. Only staff members authorised in the security document shall grant, alter or annul the access authorised to resources, pursuant to the criteria established by the data controller.
5. Should personnel not pertaining to the data controller have access to the resources they shall be subject to the same security conditions and obligations as the internal personnel.

Article 92

1. The supports and documents containing personal data shall permit identification of the type of information they contain, allow an inventory to be taken and shall only be accessible by the personnel authorised in the security document.

An exception to these obligations shall be made when the physical characteristics of the support makes their fulfilment impossible, a record justifying this fact being made in the security document

2. The departure of supports and documents containing personal data, including those comprising and/or attached to e-mails, outside the premises under the control of the data controller shall be authorised by the data controller or be duly authorised in the security document.
3. Measures aimed at avoiding the theft, loss or unauthorised access to the information during transport shall be taken in the transfer of documentation.
4. Any document or support containing personal data that is to be discarded shall always be erased or destroyed, by taking measures aimed at avoiding access to the information contained therein or its later recovery.
5. The identification of the supports containing personal data that the organisation deems particularly sensitive may be made using logical labelling systems permitting authorised users of such supports and documents to identify their content, and making identification difficult for anyone else not so authorised.

Article 93

1. The data controller shall take the measures that guarantee the correct identification and authentication of the users.
2. The data controller shall establish a mechanism that permits the unequivocal and personalised identification of any user who tries to access the information system and the verification of his authorisation.
3. When the authentication mechanism is based on the existence of passwords there shall be a procedure of disclosure, distribution and storage guaranteeing their confidentiality and integrity.
4. The security document shall establish the frequency, which under no circumstances shall be less than yearly, with which the passwords shall be changed. Whilst in force, passwords shall be stored in an unintelligible way.

Article 94

1. Protocols for action shall be established for making weekly backup copies, at least, unless data have been updated during that time.
2. Similarly, procedures for the recovery of data shall be established to guarantee at all times their reconstruction to the original state at the moment the loss or destruction occurred.

Manual recording of the data shall only be done when the loss or destruction affects partially automated filing systems or processing, and whenever the existence of documentation allows for the objective to be met to which the previous paragraph refers; a justified record of this fact being made in the security document.

3. The data controller shall ensure verification every six months of the correct definition, operation and application of the procedures for making backup copies and for the recovery of data.

Spain (continued)

4. The tests prior to the implementation or amendment of the information systems the process filing systems with personal data shall not be done with real data, unless the relevant level of security for the processing is ensured and it is recorded in the security document.

If tests are to be done with real data, a backup copy shall be made first.

Section Two. Medium-level security measures

Article 95

The security document shall appoint one or several security officers commissioned with co-ordinating and monitoring the measures defined therein. This appointment may be general for all the filing systems or processing of personal data or specific depending on the information systems used, which shall be clearly recorded in the security document.

Under no circumstances shall this designation imply an exemption of the liability corresponding to the data controller or data processor pursuant to this Regulation.

Article 96

1. At the medium and higher levels the information systems and processing and data storage installations shall be subject, at least every two years, to an internal or external audit that verifies compliance with this Title.

In extraordinary circumstances the audit shall be done whenever substantial amendments to the information system are made that may have repercussions in the fulfilment of the implemented security measures for the purpose of verifying their adaptation, adjustment and efficiency. This audit starts the calculation of the aforesaid two years.

2. The audit report shall report on the adaptation of the measures and monitoring to the Law and its regulations, identifying deficiencies and proposing the necessary corrective or complementary measures. It shall also include the data, facts and observations on which the reports are based and recommendations proposed.
3. The audit reports shall be analysed by the competent security officer, who shall inform the data controller of the conclusions so he may take the adequate corrective measures and they shall be made available to the Spanish Data Protection Agency or, if appropriate, the supervisory authorities of the Autonomous Communities.

Article 97

1. A registration system for the entry of supports shall be established permitting, directly or indirectly, the type of document or support to be known, as well as the date and time, the issuer, the number of documents or supports included in the despatch, the type of information they contain, the method of despatch and the person responsible for receipt, who shall be duly authorised.
2. Similarly, a registration system for the departure of supports shall be provided permitting, directly or indirectly, the type of document or support to be known, as well as the date and time, the recipient, the number of documents or supports included in the despatch, the type of information they contain, the method of despatch and the person responsible for delivery, who shall be duly authorised.

Article 98

The data controller shall establish a mechanism to limit the possibility of repeated attempts of unauthorised access to the information systems.

Article 99

Only the personnel authorised in the security document shall have access to the places housing the physical equipment that supports the information systems.

Spain (continued)

Article 100

1. The register regulated in Article 90 shall also provide the procedures for the recovery of data, indicating the person who executed the process, the data restored and, if appropriate, which data have had to be manually recorded in the recovery process.
2. Authorisation of the data controller shall be necessary for the execution of the data recovery procedures.

Section Three: High-level security measures

Article 101

1. The identification of the supports shall be done using logical labelling systems allowing users with authorised access to such supports and documents to identify their contents, and making identification difficult for everyone else.
2. The distribution of supports containing personal data shall be done encoding such data or using another mechanism that guarantees that such information is not accessible or manipulated during transport.

Similarly, the data contained in portable devices shall be encoded when they are outside the installations of the data controller.

3. The processing of personal data in portable devices that do not permit encoding shall be avoided. Should it be strictly necessary it shall be recorded with the justification in the security document and measures shall be taken bearing in mind the risks of processing in unprotected environments.

Article 102

A backup copy of the data and of their recovery procedures shall be kept in a different place to that housing the computer equipment that processes them, which shall in any case comply with the security measures required herein, or use elements that guarantee the integrity and recovery of the information, so that their recovery is possible.

Article 103

1. For each attempt at access at least the following shall be stored: identification of the user, the date and time it was done, the filing system accessed, the type of access and whether it has been authorised or denied.
2. Should access be authorised, it shall be necessary to store the information allowing the accessed register to be identified.
3. The mechanisms that permit the register of accesses shall be under the direct control of the competent security officer and shall not permit their deactivation or manipulation.
4. The minimum period for storing the registered data shall be two years.
5. The security officer shall review the registered monitoring information at least once a month and shall draft a report of the revisions and the problems detected.
6. The registration of accesses defined herein shall not be necessary when the following circumstances concur:
 - a) The data controller is a natural person;
 - b) The data controller guarantees that only he has access and processes the personal data.

The concurrence of these aforesaid circumstances shall be expressly recorded in the security document.

Article 104

When, pursuant to Article 81.3, the high-level security measures must be implemented, the transfer of personal data through public or wireless electronic communications networks shall be done encoding such data or using any other mechanism that guarantees the information shall not be intelligible or manipulated by third parties.

Spain (continued)

Chapter IV: Security Measures Applicable to Non-automated filing systems and processing

Article 105

1. In addition to the provisions of this Chapter, the provisions of Chapters I and II of this Title shall be applicable to non-automated files relating to:
 - a) Scope
 - b) Levels of security
 - c) The data processor
 - d) Provisions of services without access to personal data
 - e) Delegation of authorisations
 - f) Working procedure outside the premises of the data controller or data processor
 - g) Working copies of documents
 - h) The security document.
2. The provisions established in section one of Chapter III of this Title shall also be applicable relating to:
 - a) Functions and obligations of staff members
 - b) Register of incidents
 - c) Control of access
 - d) Management of supports.

Article 106

The filing of supports or documents shall be done pursuant to the criteria set out in the respective legislation. Such criteria shall guarantee the correct storage of the documents, the location and consultation of the information and allow the exercise of the rights of objection to the processing, access, rectification and erasure.

Should there not be any applicable regulation, the data controller shall establish the criteria and protocols for action that must be followed for the filing.

Article 107

The storage devices for the documents containing personal data shall have mechanisms that hinder opening. When their physical characteristics do not permit such a measure, the data controller shall adopt the measures that prevent access by unauthorised persons.

Article 108

Whilst the documentation containing personal data is not filed in the storage devices established above, due to undergoing revision or processing, whether before or after their filing, the person who is responsible for them shall ensure their safekeeping and prevent at all times their access by unauthorised persons.

Section Two: Medium-level security measures

Article 109

One or several security officers shall be designated under the terms and with the functions set out in Article 95 hereof.

Article 110

The filing systems comprising this section shall be subject to an internal or external audit, at least every two years, which verifies compliance with this Title.

Spain (continued)

Section Three: High-level security measures

Article 111

1. The cupboards, filing cabinets or other elements for storing non-automated files with personal data shall be in areas to which access is protected by entrance doors with locks or another equivalent device. Such areas shall remain closed when access to the documents included in the filing system is not required.
2. If, bearing in mind the characteristics of the premises available to the data controller, it is not possible to comply with that provided above, the data controller shall adopt alternative measures that, duly justified, shall be included in the security document.

Article 112

1. The generation of copies or the reproduction of the documents shall only be done under the control of the personnel authorised in the security document.
2. Copies or reproductions to be discarded shall be destroyed to avoid access to the information contained therein or its later recovery.

Article 113

1. Access to the documentation shall be exclusively limited to the authorised personnel.
2. Mechanisms shall be established to permit identification of access to documents that may be used by multiple users.
3. The access of persons not included above shall be adequately registered pursuant to the procedure established for this purpose in the security document.

Article 114

Whenever there is a physical transfer of the documentation contained in a filing system, measures shall be adopted aimed at preventing access or manipulation of the information being transferred.

Jurisdiction: Sweden

Relevant provision transposing Article 17

Personal Data Act 204/1998

Section 30

A personal data assistance and a person or those persons who work under the assistant's or the controller of personal data's direction may only process personal data in accordance with instructions from the controller of personal data.

There shall be a written contract on the processing by the personal data assistance of personal data on behalf of the controller of personal data. It shall be specifically stipulated in the contract that the personal data assistant may only process personal data in accordance with instructions from the controller of personal data and that the personal data assistant is liable to take those measures referred to in Section 31, first paragraph.

If there are special provisions in a statute or other enactment concerning processing of personal data in public operations as regards matters referred to in the first paragraph, these shall apply instead of that stated in the first paragraph.

Section 31

The controller of personal data shall implement appropriate technical and organisational measures to protect the personal data that is processed. The measures shall provide a level of security that is appropriate having regard to:

- (a) the technical possibilities available;
- (b) what it would cost to implement the measures;
- (c) the special risks that exist with processing of personal data; and
- (d) how sensitive the personal data processed really is.

If the controller of the personal data engages a personal data assistant, the controller of personal data shall ensure for him/herself that the personal data assistant can implement the security measures that must be taken and ensure that the personal data assistant actually takes the measures.

Section 32

The supervisory authority may in an individual case decide on which security measures the controller of personal data shall implement in accordance with section 31.

Jurisdiction: UK

Relevant provision transposing Article 17

Data Protection Act 1998

Schedule 1, Part I, Condition 7:

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Schedule 1, Part II, The Seventh Principle

Paragraph 9

Having regard to the state of technological development and the cost of implementing any measures, the measures must ensure a level of security appropriate to –

- (a) the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage as are mentioned in the seventh principle, and
- (b) the nature of the data to be protected.

Paragraph 10

The data controller shall take reasonable steps to ensure the reliability of any employees of his who have access to the personal data.

Paragraph 11

Where processing of personal data is carried out by a data processor on behalf of a data controller, the data controller must in order to comply with the seventh principle –

- (a) choose a data processor providing sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out, and
- (b) take reasonable steps to ensure compliance with those measures.

Paragraph 12

Where processing of personal data is carried out by a data processor on behalf of a data controller, the data controller is not to be regarded as complying with the seventh principle unless –

- (a) the processing is carried out under a contract –
 - (i) which is made or evidenced in writing, and
 - (ii) under which the data processor is to act only on instructions from the data controller, and
- (b) the contract requires the data processor to comply with obligations equivalent to those imposed on a data controller by the seventh principle.

About RSA

RSA, The Security Division of EMC, is the premier provider of security solutions for business acceleration, helping the world's leading organizations succeed by solving their most complex and sensitive security challenges. RSA's information-centric approach to security guards the integrity and confidentiality of information throughout its lifecycle – no matter where it moves, who accesses it or how it is used.

RSA offers industry-leading solutions in identity assurance & access control, data loss prevention, encryption & key management, compliance & security information management and fraud protection. These solutions bring trust to millions of user identities, the transactions that they perform, and the data that is generated. For more information, please visit www.RSA.com and www.EMC.com.



RSA Security Inc.
RSA Security Ireland Limited
www.rsa.com

The Security Division of EMC

RSA and RSA Security are registered trademarks or trademarks of RSA Security Inc. in the United States and/or other countries. EMC is a registered trademark of EMC Corporation. All other products or services mentioned are trademarks of their respective owners. ©2008 RSA Security Inc. All rights reserved.