Abstract:
The development of computer networks and technology allow organizations to process and transmit tremendous volumes of data, including also large amounts of personal data. However, national and European data protection laws regulate the processing of personal data and impose serious obligations to data controllers for their protection and secure processing. Additionally, the response of the organizations to data protection law provisions and related user interests become determining factors for the acceptance of their business services. The aim of this paper is to propose a security controls selection process to provide data controllers with a framework for selecting appropriate security controls, that will satisfy the privacy protection requirements of the legislation and the security and privacy objectives of the organization.

Key-words: Personal Data Protection; Privacy-Enhancing Technologies; Secure Information and Communication Systems; Security Controls Selection Process; System Auditing Process, Security and Privacy Protection Evaluation.

1. Introduction
Advances in information technology and the Internet have changed the ways in which the communication and exchange of personal data is performed. Vast quantities of personal data are transmitted within seconds across national frontiers and indeed across continents.

Organizations in order to conduct business create, collect, analyze, combine and disseminate personal data. The telecommunication and mobile communication industry, the insurance, direct marketing and health companies are processing an ever-increasing volume of personal data.

Users (data subjects) expect their personal information to be protected and their privacy to be respected by the organizations (data controllers) they conduct business with. On the other hand, data controllers have realized that protecting personal data and addressing privacy issues effectively will become a competitive strategy for both businesses and users.

Privacy protection laws have been enacted in many countries in the last three decades to regulate the processing of personal data. In addition to national data protection laws, several legal instruments related to privacy protection have been adopted at an international level. Among the most influential are the European Union’s Directives 95/46/EC and 97/66/EC, the Council of Europe’s Convention of the Protection of individuals with regard to Automatic Processing of Personal Data, and the OECD’s Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data [3,4].

Therefore, data controllers are obliged to respond to the privacy protection requirements imposed by the above-mentioned legislation. Specifically, these laws impose obligations to data controllers to select an appropriate set of security controls to provide the desired level of protection in relation to personal data. The aim of this paper is to propose a privacy protection model to support data controllers to respond to the requirements of the legislation. This model reflects the auditing practices of the Hellenic Data Protection Authority regarding the compliance of data controllers to Greek and European legal framework.

The paper is organized as follows. In the second section, the privacy protection requirements imposed by the legal framework are analyzed. The third section is devoted to the analysis of the requirements of the security principle. In the fourth section the security control selection model is presented. Finally, the paper is concluded.

2. Privacy Protection Requirements
According to European data protection legislation, data controllers processing personal data should demonstrate that they have implemented an effective approach towards their security arrangements as far as the secure processing of personal data is concerned.

The data protection laws are based on the following principles:

- Principle of lawfulness and fairness: personal data should be gathered by fair and lawful means.
The above principles constitute the privacy protection requirements of the legislation and define a regulatory framework for the protection of personal data.

3. Security Principle Requirements

The main security obligations are outlined in the security principle. This principle states that appropriate technical and organizational security measures should be taken by the data controller for the protection of personal data against accidental or unauthorized destruction or accidental loss as well as against unauthorized access, alteration or dissemination.

According to data protection laws based on the Directive 95/46/EC [3], the obligations of the data controllers regarding the secure processing of personal data are:

1. Establishment of the appropriate security standards and procedures. Data controllers are obliged to be aware of new security techniques and equipment and to periodically assess the security of their information and communication infrastructure and to consider their own security practices in the light of the standards adopted in the industry. The establishment of organizational measures is related to security management and to allocation of resources to security, the identification of roles and responsibilities, the establishment of rules ensuring compliance with the security procedures.

2. Selection of personnel based on their skills and ethics and the provision of appropriate training in security issues: there is a requirement for computer security awareness training for personnel at all levels throughout the organization. Training should focus into making personnel aware of their responsibilities towards security. A third factor affecting personal reliability indicates the establishment of a work environment, which meets health and safety standards.

3. Management of outsourcing contracts and the selection of a processor according to the technical security and organizational measures governing the processing. The security and organizational measures that should be taken by the processor correspond to those implied by the security principle, and are equivalent to those imposed to data controller. Furthermore, the processor is contractually obliged to process personal data only on instructions of the controller and to take the required staff-related precautions. The parts of the contract or the legal act relating to data protection and the requirements relating to the technical and organizational measures should be in writing or in another equivalent form.

4. Whenever personal data are transferred outside Europe, the data controller must consider the security measures taken and the legislation
concerning data protection in the country or territory where the data are transferred.

Therefore, the selection of the appropriate set of security controls to meet the privacy protection requirements imposed by the data protection legislation is of major importance to the data controllers. The appropriate security measures must be selected and implemented so that an acceptable level of privacy is achieved.

4. Security Controls Selection Process

The selection and implementation of an appropriate set of security controls is an accepted way to achieve an adequate level of privacy protection in the organization. The selection of the security controls may be accomplished through the exercise of a risk analysis strategy. However, a number of baseline control manuals are available that can be used to streamline the process. For example the ISO security standard (ISO 17799) constitutes a comprehensive reference document for identifying a set of security controls that will meet the security requirements of the majority of organizations across all functional domains.

Baseline security supports the selection of a set of security controls, which will provide good protection against most threats and under most circumstances. However, baseline manuals provide little guidance on how to determine the set of controls to provide adequate security for the particular business situation or according to legal, regulatory requirements.

Therefore, we propose a model for the selection of an appropriate set of security controls from a baseline manual that will satisfy the legal privacy protection requirements and any particular privacy requirements of the data controller regarding the secure processing of personal data. Our proposed security controls selection model is presented in Fig. 1.

The principle of purpose specification constitutes the axis of the selection model. The first step of the model is to identify the purposes, which require the processing of personal data, according to the activities of the organization. The model steps are repeated for all the identified data purposes of processing.

In the following step, the personal data, whose processing is necessary for the fulfillment of the data processing purposes, are defined. The identification of the personal data is based on the application of the principles of lawfulness and fairness and the principle of minimality.

In the next step, the protection level of the personal data is identified based on the privacy protection requirements imposed by the legislation and the particular privacy requirements deriving from the activities of the organization. The principles of accuracy, anonymity, individual participation and accountability are applied to each processing purpose and the corresponding data so that a specific (detailed) privacy protection requirements set is defined. The concrete privacy protection requirements set includes the law compliant operations that can be performed on personal data, the sources for collecting personal data, the recipients for disclosing personal data, the time period during which processing is necessary and the staff members that are responsible for accountability and compliance.

The next step involves the application of the security principle for the selection of the appropriate security controls from the baseline manual. Security controls are selected from the manual, according to the detailed privacy protection requirements. The computational and communication infrastructure of the organization is taken into consideration in this step so that the security controls selected are in accordance with the existing infrastructure, the procedures in operation and the possible security-related technological solutions.

The technical control requirements of the security principle range from authentication, integrity and access control mechanisms to confidentiality, accountability and digital signature creation and verification. To the organizational control requirements belong among others security and privacy protection planning and strategy, security and privacy policy creation and maintenance and disaster recovery and business continuity planning.

Additionally, the selection of the appropriate security controls is based on the requirements regarding staff selection and security and privacy related training and the possible outsourcing contracts. Finally, possible transfers of personal data outside European Union should be considered.

The following step of the model determines a privacy protection profile for each data processing purpose, which comprises the security controls selected and the privacy protection requirements. Thus, the privacy protection profile defines a set of appropriate privacy and security requirements and objectives. The privacy protection profiles should guide the eventual product selection and evaluation. The model steps are repeated so that a privacy protection profile is determined for all the processing purposes of the data controller.

Finally, the last step refers to a periodical monitoring of the security publications and vulnerability analysis and generally of technological solutions and advances that should be considered so that privacy protection profiles and implementations are adjusted properly.
The purpose of this paper is to propose a security
controls selection process to assist data controllers to
fulfil their, legally imposed, obligations towards the
secure processing of personal data. The process is
based mainly on the privacy protection requirements
of the legislation but takes into consideration the
particular privacy requirements a data controller may
have according to the nature of the business activities.
In the first step of the process, the activities of the
organization are analyzed and the data processing
purposes are identified. In the following step, the
personal data, which are necessary for the fulfillment
of the corresponding processing purposes, are defined.
The protection level of the personal data is determined
detailed privacy protection requirements
and detailed privacy requirements set
the selection of the appropriate security
controls from the baseline manual. The last step of the
model defines a privacy protection profile for each
data processing purpose, which comprises the selected
security controls and the privacy protection
requirements, while technological advances and
solutions are taken into consideration.

References:
p. 124-128.
[2] Institute for Certification of Information
Technology (ICIT), ‘Scheme for self-assessment and
certification of information security against BS 7799’,
1997.
with regard to the processing of personal data and on
the movement of such data and 97/66/EC on the
protection of personal data in telecommunications,
www.eu.int/comm/…/media/dataprot/.
[4] OECD, Guidelines Governing the Protection of
Privacy and Transborder Flows of Personal Data,
[5] Lynette Barnard and Prof. Rossuw von Solms, ‘A
Formalized Approach to the Effective Selection and
Evaluation of Information Security Controls’, J.
Computers & Security, Vol. 19, No. 2, pp. 185-194,
2000.
[6] V. C. Zorkadis, E. Siougle, Ph. Mitleton,
Technical and Legal Reports on Evaluation of Security
and Privacy Protection, Hellenic Data Protection
Privacy Audit Modeling’, Proc. of the 5th World

Fig. 1. Security Controls Selection Process

5. Conclusion
The purpose of this paper is to propose a security
controls selection process to assist data controllers to
fulfil their, legally imposed, obligations towards the
secure processing of personal data. The process is