International Journal of Business and Management Invention
ISSN (Online): 2319 – 8028, ISSN (Print): 2319 – 801X
www.ijbmi.org || Volume 5 Issue 11 || November. 2016 || PP—30-43

Information Security and the Protection of Personal Data in Universities

Asst. Prof. Dr. Türkay Henkoğlu[1], Prof. Dr. Nazan Özenç Uçak[2]
[1](*Department of Management Information Systems / Adnan Menderes University, Turkey)*
[2](*Department Information Management / Hacettepe University, Turkey)*

ABSTRACT: *Increases in the number of computers and the rate of information systems used in today's universities makes viewing universities as information security centers difficult. As a result, such universities are often required to form an information security culture within the framework of university information security policies in which legal arrangements and international standards are considered in conjunction with technical precautions, sharing responsibilities among all units within the university setting. In this study, existing university conditions regarding personal data protection are evaluated; moreover, proposals to meet these deficiencies are made with the intent of providing support in establishing an information security culture. To this end, a survey was conducted in data processing centers of 15 universities in Ankara, and the information security precautions taken by these universities were evaluated.*

The results of this study reveal that risks of data loss were minimized by taking various technical precautions such as the university data processing department (DPD) backing up data; however, overall legal arrangements and precautions taken by university DPDs are insufficient. More specifically, there is no policy regarding the protection of personal data. In addition, when there is destruction of data or data storage systems fail in universities, no report on risk analysis is filed, responsibilities are not shared among university units, and units other than DPDs do not participate in the process of providing information security

Keywords: *Information security, personal data, sensitive data, information security policy*

I. INTRODUCTION

There are numerous uncertainties regarding the degree to which universities are cautious in the protection of electronically saved data, which information policies are implemented, whether the processing of personal data is under proper control, and how the basic rights and freedom of members of the university communities are protected. Considering the protection of personal data, which plays an important role in information assets [2], the protection of privacy is a preferred target even under the condition that this kind of data is captured by malicious individuals. At the core of the problem of personal data protection, there are a variety of aspects including uncontrolled easy and fast copying of the personal data thanks to information technologies, storage of too much information due to increasingly low storage costs, transferring data to increasingly remote locations in a very short time period, unprotected information access by an unlimited number of people, and irremediable results from the moment the process goes out of control.

Limited protection of data secrecy (i.e., ignoring personal rights) can be provided through technical precautions by a university's data processing department (DPD). As emphasized in the justification of the reform package of the European Union (EU) Personal Data Protection Directive [3], to meet the deficiencies of personal data protection, it is necessary to prioritize the improvement of awareness in units that have data processing and storage responsibilities and to develop information security policies for establishing a sound information security culture [4]. Legal arrangements regarding personal data protection is the most important basis of production and application policies on information security. It is not possible to protect information assets by taking technical precautions without any legal basis or by making only legal arrangements [5]. In addition to technical precautions, international standards and legal administrative precautions should include applicable general security elements and protect personal rights. As indicated in the Hong Kong Special Administrative Region (HKSAR) information security report, if information security policies, which are developed by adopting international standards applicable to university units, are conducted with the attendance of all university units and an information policy culture is then established, they will be far more effective in providing information security [6]. The need of interdisciplinary cooperation to provide information security in a versatile way often causes this issue to be deferred and therefore increases risks. In Turkey, there is no standard information security policy that is compatible with legal arrangements in universities. In this study, data on the precautions taken in the scope of information security are collected and evaluated in relation to the protection of data secrecy; however, the findings obtained regarding information security and the proposals presented at the end of the study are created within the framework of personal rights and the protection of an individual's rights regarding his or her own data

II. SECRECY WITHIN THE SCOPE OF LEGAL ARRANGEMENTS AND THE PROTECTION OF PERSONAL RIGHTS

Defined as a Constitutional right that cannot be limited or transferred without an individual's approval or obligatory conditions stated in the legal arrangements, the right for protection of personal data is a fundamental right for the protection of personal rights and is related to the privacy of the individual. For this reason, an illegal sharing of personal data without an individual's approval implies a violation of one's general personal right even if it is for the sake of public interest. The purpose of the protection of personal data is to protect an individual's freedom in making decisions regarding his or her own personal data and protect these data from illegal interventions [7]. Considering legal arrangements regarding data protection and the protection of privacy, the theme is to provide control of an individual's own personal data [8, 9]. Data secrecy is an element of information security regarding the right to demand protection of personal data secrecy [10]. Hence, defining data secrecy as a data owner's ability to control data circulation and the right of an individual's control of his or her own personal data provides a united understanding of secrecy from the fields of law and informatics [11]. Protecting personal data aims to not only maintain data secrecy but also protect personal rights and freedom. In this context, basic principles such as the limited collection and processing of personal data, using it in accordance with its purpose, and taking necessary precautions for protection of these data are adopted [12, 13]. The 20th item of the Constitution indicates that personal data can only be processed under specific conditions of the law or with obvious approval of the owner [14]. Thus, owners of personal data collected and processed in universities are absolute rightful owners. Therefore, administration and all personnel processing these data in universities have responsibilities regarding the processing of such data according to administrative arrangements. Even though basic principles on processing, using, storing, and protecting personal data are not defined in the Turkish Criminal Code (TCC), there are legal arrangements on obtaining, recording, and distributing personal data in illegal ways. For this reason, the TCC should be taken into consideration in all applications of processing and protecting personal data in universities. Moreover, the legal arrangements on revealing the correspondence (i.e., TCC Item 132/3) should be taken into consideration by DPD personnel since specific correspondence tools (e.g., e-mail, SMS, and phone) are not mentioned. Improving the awareness of DPD personnel in regards to legal responsibilities is crucial in implementing the obligations within many different legal arrangements in Turkish Law Codes.

Protection of personal data has been directly or indirectly included in many legal arrangements within Turkish Law (e.g., Constitution, TCC, Law numbered 5651, and Turkish Civil Law)1 to meet the needs of the related fields; however, these legal arrangements do not include necessary preventative precautions for protecting personal rights or personal data. Therefore, it is necessary to inspect the framework of particular standards to then define the legal or technical preventative precautions. The processing, use, storage, and transferring of personal data are also evaluated in the context of the 8th item in the European Convention on Human Rights, and a protection area is formed for the individual (Constitutional Court, 2011). The 90th item of the Constitution expresses that international agreements have statutory effects and statements within these agreements shall be predicated in the conflicts [14].

The main theme of the EU data protection directive is the protection of personal data. Considering this, the focus of the precautions taken for information security is on the protection of personal data; however, in Turkey, precautions for protecting secrecy are primarily what is taken. As mentioned in EU reports on Turkey [18], although the adaptation to the EU process has been kept in the foreground within the necessities of the Personal Data Protection Act (PDPA), protecting basic rights and freedom is taken into consideration as a secondary purpose. Therefore, it is evaluated that establishing information security policies within the framework of basic principles on personal data protection in units of universities is an important first step, along with improving the awareness of the personnel who have personal data processing and storage responsibilities.

III. RESEARCH METHOD

The personal data in this study are evaluated in relation to the real individual. Other elements such as companies or governments noted with the data are excluded from this study. The precautions that should be taken within the framework of a university DPD's information security standards are explicated, as are the legal arrangements against every kind of unauthorized access without the awareness and approval of the data owner. DPDs are the units responsible for providing central database security in which the densest personal data exist in universities and information systems.

1 The given arrangements are incorporated into the 20th and 22nd Items of the TR Constitution 14. T.C. Anayasası *Türkiye Cumhuriyeti Anayasası*. 1982., 132., 135., 136., 138., and 258., Items of Turkish Crime Code 15. TCK *Türk Ceza Kanunu*. 2004., 24. and 25., Items of Turkish Civil Law 16.TMK *Türk Medeni Kanunu*. 2001., and 5 and 6. Items of The Law numbered 5651 17. 5651 Sayılı Kanun *İnternet Ortamında Yapılan Yeyınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun*. 2007..

3.1. Sample and Research Population

The research population consisted of DPD units of 5 public and 10 private universities. No sample is discussed, as the entire population was taken into consideration in this study. One public and two private universities that completed establishing procedures but had still been structuring are not included in this research. Key points regarding information security and personal data in universities are discussed within the scope of Turkish Law and EU Law Regulations.

3.2. Collection of Data

The data for this research were obtained by using interviews and survey techniques; more specifically, university DPDs were asked structured questions. This survey method provides the opportunity to compare and control the data obtained from university DPDs [19]. Surveys were conducted by face-to-face interviews, because by doing so, the possibility of varying respondent comprehension of the questions [20] is taken into consideration, the answer rate is higher than that of a survey conducted by means of mailing, errors can be fixed, deficiencies can be completed, and awareness can be measured more effectively by obtaining more sound information. Directors and deputy directors were asked interview and survey questions since they are responsible for the actual application of information security policies. Results of the interviews and surveys yielded detailed information regarding existing information security policies and applications providing information security in the universities.

The survey questions were prepared to provide insight into the responsibilities for protection and storage of personal data in databases, university information security policies and legal conditions, policies on backups and the destruction of data, risk management, and information security applications. Survey questions prepared for this research included one-choice questions, multiple-choice questions, serial questions, response-defined questions, and open-ended questions. Three pilot studies were conducted in three universities to determine any deficiencies in the survey questions, and the survey questions were then revised according to such feedback. International information security standards, reports published by other institutions in regards to information security controls, the EU Data Protection Directive, and legal arrangements regarding the protection of personal rights were all utilized in preparing the interview and survey questions.

Research questions in the context of this study are as follows:

1. Are the existing legal arrangements adequate for protecting personal rights and freedom regarding the protection of personal data in universities?
2. Are there any written information security policies in the universities? Has any policy been identified for processing and protecting personal data?
3. Have policies been determined for storing data in central databases and computers, processing personal data, and sharing responsibilities between units?
4. How and on which dimensions are precautions taken regarding data protection? Are there any information management strategy and risk management plans?
5. Have responsibilities been determined for data destruction? Has any coordination been provided between units?
6. Has any expert personnel been assigned to provide personal data protection and information security at an adequate level in the university DPD?
7. What are the views of university DPD units on information security and personal data protection?

IV. FINDINGS AND EVALUATION

In accordance with the findings obtained from the research data, the research questions noted above were answered by evaluating personal data backup and destruction policies, information security precautions taken to protect personal data and ensure their compatibility with legal arrangements, responsibilities regarding data protection, and risk conditions on information security. All questions were answered by all respondents (i.e., N = 15).

4.1. Legal Arrangements and Information Security Policies regarding Personal Data Protection in Universities

DPDs responsible for taking technical precautions to provide information security and protection of central databases in which personal data are stored in universities were asked to put forward their views on the adequacy of legal arrangements for personal data protection. Overall, 66.7% of the respondents thought that legal arrangements regarding information security and personal data protection were not adequate; the remaining 33.3% said that they did not have any idea regarding the adequacy of the legal arrangements. From our results, an inadequate amount of time is given to personal data protection in the six universities in which there are too few data DPD processing personnel. Although the disorganization of legal arrangements was

emphasized in the interviews, there are noted deficiencies in examining legal arrangements. Most respondents (90%) had not examined any of the legal documents such as the EU PDPA; thus, showing that respondents have low interest in the legal arrangements on this issue. Taking the findings obtained in this research into consideration, legal arrangements can be described as difficult documents to understand and practice for respondents; however, as Charette expressed [21, 22], it is not possible to prevent information security infractions by taking only technical precautions into account. Preventative precautions regarding personal data protection are only successful via a combined approach using legal and technical capabilities. In the universities, respondents were asked about the responsibilities they have in personal data protection and to describe them within the framework of legal arrangements. Table 1 shows a summary of these responsibilities, with the opportunity to check more than one option provided to the respondents.

Table 1. Responsibilities in the framework of legal arrangements

On which legal arrangements' context do you think you have responsibilities on personal data protection?		
	N	%
TR Constitution	8	53.3
Turkish Crime Code	11	73.3
The Law numbered 5651	12	80
PDPA Draft	8	53.3
EU Data Protection Directive	2	13.3
I do not think that I have responsibility in legal framework	-	-
I have no idea	2	13.3
Out of evaluation	-	-

All respondents expressed that they did not have any information regarding the content of any legal arrangement except for the act numbered 5651. This shows that they are unaware of other legal arrangements on this issue. As shown in the table, 73.3% of the respondents expressed that they also have responsibilities within the scope of the TCC as a secondary priority; furthermore, 86.7% expressed that they did not have any responsibilities in the context of the EU Data Protection Directive and did not have any information regarding this issue. In contrast, the rate of respondents thinking they had responsibilities within the scope of PDPA, which is still a draft law, was the same as the rate of respondents thinking they had responsibilities within the scope of the Constitution. The respondents who thought they had responsibilities within the scope of PDPAD stressed the importance of this draft and noted that this draft can be utilized to fill in the deficient gaps of existing legal arrangements. In addition to the legal arrangements presented in the table, one respondent expressed that he also had responsibilities within the scope of the Right to Information Act and the Electronic Signature Act. Table 2 shows answers provided by directors regarding questions on the existence, content, adequacy, efficiency to the work process of information security, and legal conditions of the respondents in universities.

Table 2. Information security policies on personal data in universities

	Yes		No		No idea		DD	
	N	%	N	%	N	%	N	%
Does the information security policy contain detailed technical and legal precautions?	1	6.7	14	93.3	-	-	-	-
Does the information security policy contain points in personal data protection?	2	13.3	13	86.7	-	-	-	-
Will the existence of information security policy on personal data protection facilitate the definition of work process and responsibility?	15	100	0	-	-	-	-	-

Content analysis was performed on the concerned university websites to detect the existence of any written information security policy; however, no detailed written security policies in which responsibilities are described by university units could be found. Data obtained from university websites showed that the responsibility for information security is only evaluated according to its technical dimensions and undertaken by university DPDs. Information security policies, which are seen on websites belonging to university DPDs, did not include items meeting the needs of personal data protection. Answers provided by respondents regarding the existence of written information security policies (or lack thereof) confirm the preliminary research results regarding the university websites.

In relation to this, respondents were asked whether existing information security policies include legal precautions and points in personal data protection. One of the two respondents stating the existence of an information security policy said that the existing information security policy does not include detailed technical and legal precautions. Respondents overwhelmingly gave "no" answers to the two questions regarding the existence of information security policies including legal precautions (93.3%) and personal data protection

(86.7%); however, none of the policies, except in one university, include detailed technical and legal precautions and are therefore inadequate for personal data protection. Furthermore, a DPD respondent expressed that the existing information security policy is inadequate despite including some points regarding personal data protection, and a new security policy is being prepared and approaching the approval process. All respondents emphasized that information security policies on personal data protection will contribute to defining work processes and responsibilities, stressing the importance of becoming an obligation for determining responsibilities, providing coordination between units, and addressing the known deficiencies.

4.2. Central Storage of Data and Sharing of Responsibilities

To reach information about central supervision and control opportunities of the university DPD unit, respondents were asked whether they know which computers within the university units have personal data. Of the respondents, 64.3% stated that they did not have this information, thus drawing attention to the impossibility of controlling and supervising from only one center (i.e., the DPD) in universities in which the number of computers is very high (e.g., 35,000). This is significant since it indicates problems that newly founded and developing universities may meet after some time. For this reason, even though central supervision and control methods are being practiced in most universities, sharing such responsibilities with the individuals responsible for data processing in university units (or in newly developed structures) should increase the efficiency of the activities. While the computers in which personal data are processed are known in 80% of the foundation universities—and therefore, where control and supervision can be more readily implemented—this rate decreases to 40% in public universities having more computers. DPD respondents with responsibilities for central data storage were asked which university units have data stored in DPD servers; results are shown in Figure 1. Note that the question regarding information stored in DPD servers was answered by all respondents; furthermore, the opportunity to check more than one option was provided.

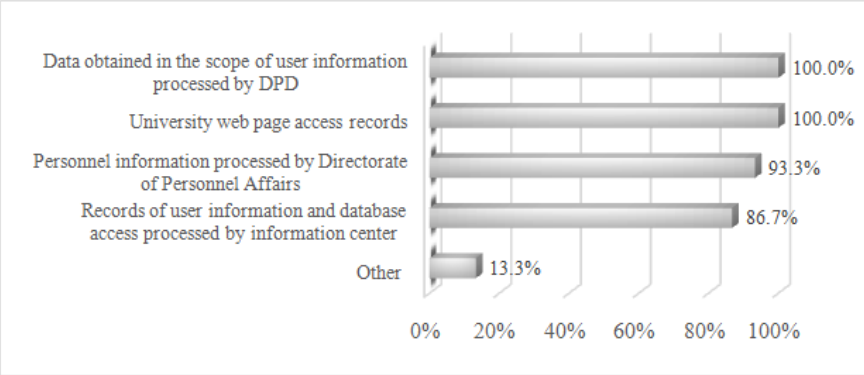

Figure 1. Data centrally stored in servers under the responsibility of DPDs

Overall, the respondents stated that data belonging to the units shown in Figure 1 are stored in servers of university DPDs. In addition, two DPD respondents (i.e., 13.3%) drew attention to keeping important files that include personal data such as scientific research projects, patent studies, and identity sharing systems in central servers of the DPD. In answering this question, the respondents expressed that they think data storage, processing, and sharing of responsibilities are mostly misunderstood, i.e., other units think all responsibilities belong to the DPD. Taking the distribution of data obtained from public and foundation universities into account, there is no difference in taking precautions regarding data protection in safe environments between public and foundation universities.According to data obtained from this research, university DPD units have important responsibilities for providing personal data security processed in electronic forms; however, there are no written policies on how responsibilities regarding these data are shared with other units and how the necessary coordination is achieved. This situation causes units to disagree in terms of data violations and may also negatively impact time management processes, which is one of the most important elements in reaching a solution and results in informatics crimes. For this reason, responsible units for data storage and processing should be defined in information security policies and coordination meetings. Protecting the integrity of personal data processed in universities is seen as the most difficult element among information security precautions. Considering personnel deficiencies in DPD units, it is difficult for them to develop their own solutions for university units. Six respondents defined DPD personnel as an inner threat since they have unlimited access rights, thus showing that concerns regarding this issue are not frivolous. Applicable solutions exist, e.g., maintaining data processing records such that individuals responsible for processing the data and the corresponding media on which data are recorded can control and give enough access and process authority to only concerned personnel within the units. Other examples include periodically updating personal information

of the personnel, comparative analysis, non-deniability, and use of identity confirmation methods Furthermore, it is important to inform DPD personnel to not reveal information that they obtain due to their duties that should be kept secret according to the 258th item of the TCC [15]. Defining and recording the tasks that university units want the DPD to perform through a "data processing help center" will facilitate retrospective follow-up. In addition, if necessary system improvements are made in EU legal norms, data can be stored in a cryptographic way, data owners can access their information at any time, and thus a control mechanism can be created.

Use of an Electronic Records Management System (ERMS) has become increasingly widespread with the use of information technologies within universities. A preliminary condition of ERMS usage is using an electronic signature in an expedient and safe way. According to Public Certification Center records, 40% of universities involved in research have active electronic certificates [23]; however, according to data obtained in the research, nothing is done by DPDs in rearranging signature authorities within the technical facilities or taking additional precautions after the departure of the personnel. With basic responsibilities assigned to university DPDs and other concerned units using the system, giving authorization to access the system by these units can meet the aforementioned deficiencies and contribute to implementing preventative precautions.

4.3. Information Security Precautions for Personal Data Protection

Table 3 presents findings regarding the efficiency of information security precautions taken in the universities to protect secrecy and personal rights; methods were applied with an aim of protecting information assets, technical and administrative precautions, and applications of security supervision. All questions presented in Table 3 were answered by all respondents (i.e., N = 15).

Table 3. Efficiency of information security and security supervision

	Yes		No		Partially	
	N	%	N	%	N	%
Is "cryptography" method used for information security?	5	33.3	10	66.7	-	-
Is "hash" value calculated for the integrity of personal data?	5	33.3	10	66.7	-	-
Do the information security precautions protect the secrecy of data?	14	93.3	1	6.7	-	-
Do the information security precautions protect the personal rights and freedom of the individuals?	14	93.3	1	6.7	-	-
Are the login records in the computers, in which personal data is processed or stored, being kept?	12	80.0	2	13.3	1	6.7
Are the computers having personal information being marked by appropriate labels and warning messages?	1	6.7	14	93.3	-	-
Are the security supervisions being made on the computers having personal information?	7	46.7	8	53.3	-	-

Overall, 66.7% of the respondents who answered questions regarding cryptography and hash value calculation methods expressed that they do not use these methods. Currently, limited protection is provided via the encryption given by the database system in 33.3% of university data processing centers. All respondents stated that they have opportunities to store files containing personal data via encryption; however, a preliminary study should be carried out by each unit to realize this situation because university units do not classify and separate personal data on electronic data storage media. Protecting the secrecy of data is important even if personal data are captured by malicious individuals. Therefore, databases and personal data on server computers should be protected by implementing as many technical precautions as possible including cryptography.

All respondents, except for two, expressed that login records in computers in which personal data are processed are maintained; however, these records are not analyzable since they are not kept centrally, especially in the universities with too many computers. An examination of records such as login records can only be made when an informatics crime is committed. Furthermore, it is only possible to perform these examinations and supervisions, which will be performed only by a DPD, in some particular units. Providing this kind of supervision, especially in academic units where domain structures are not used, can be perceived as too much intervention." For this reason, increasing personnel awareness is important, i.e., creating consciousness around this issue by means of warnings via e-mail, posters, and notes; holding meetings, etc., can be effective in decreasing existing risks. Usage of such warning notes to increase data security awareness exists only in one university. Four respondents defended the idea that this cannot be applied to universities where there is no domain structure, i.e., there are too many computers and various systems. Providing regular communication between data processing personnel working in university units and DPDs to overcome this obstacle can contribute to the application of current security precautions in universities in a shorter period of time and in a standardized way. Fulfilling the responsibilities of the ULAKBİM Acceptable Use Policy (AUP)—which has been approved by senior management in 66.6% of the universities, but whose content is not known by university units through responsible personnel for information processing—will be useful. Possible risk levels and security precautions can differ according to the situation, i.e., the storing, transferring, and processing of information. Therefore, the situation should be taken into consideration to determine the information security precautions that

should be applied. In this context, the respondents were asked to describe what technical and administrative precautions are taken regarding personal data protection. All respondents answering this question (i.e., with N = 15) gave the answer that basic technical precautions (e.g., IDS/IPS, firewall, antivirus, and access authorization) are taken by DPDs. In addition, technical precautions are supported by quality management system standards and user training in two universities. Overall, 93.3% of the respondents thought that these precautions protect the secrecy of data and personal rights and freedom of individuals; however, 40% stated that they do not have enough information regarding personal rights and freedom to answer the question regarding the protection of personal rights and freedom of individuals. Furthermore, no application of administrative precautions taken for information security was mentioned. As in the findings obtained in the preliminary study carried out on the university websites, the lack of administrative precautions was observed during the research, as well. Limited protection of data secrecy (by ignoring personality rights) can be provided through the technical precautions taken by DPDs. This approach causes a failure in associating the protection of personality rights, to which Whitman and Mattord have drawn attention, with the protection of data secrecy [24].

While approximately half of the respondents (i.e., 46.7%) indicated that computers with personal data are supervised, these supervisions are performed by a DPD unit in a limited and mostly occasional way on information systems. The information given by the respondents in the research shows that results similar to those obtained in the supervisions made in various institutions2 by the Presidency State Supervisory Council (SSC) can be achieved (SSC, 2013). Supervision of information security and personal data protection in universities and other public foundations is important; furthermore, standardizing these supervisions is critical. For that reason, in the universities, information security supervision should be made by considering international standards, legal arrangements, and universal information security and information security policies created within the framework of basic principles on personal data protection. As suggested in SSC reports [25], developing security test standards in universities and/or making regular inner supervisions in the framework of detailed information security policies, which will be developed in universities, will contribute to meeting critical deficits and creating awareness.

4.4. Precautions in the Context of Responsibilities of Personal Data Protection

Table 4 presents findings regarding system security tests for providing information security in universities, the compatibility of the precautions on the security of information assets with legal arrangements, sharing responsibilities on personal data protection, personnel assignments on information security provision, sensitivity of university senior management on information security provision, and classification of personal data in central data storage media. All questions in Table 4 were answered by all respondents (i.e., N = 15).

Table 4. Sharing responsibilities in personal data protection in universities

	Yes		No		Partially		No idea	
	N	%	N	%	N	%	N	%
Are system security tests conducted?	10	66.7	5	33.3	-	-	-	-
Are personal and sensitive data used while conducting system security tests?	2	13.3	13	86.7	-	-	-	-
Is it stated obviously that on the scope of which legal arrangements information assets are protected?	3	20.0	12	80.0	-	-	-	-
Are there any specifically assigned personnel on information security?	6	40.0	9	60.0	-	-	-	-
Do you think that information security issue is given importance in senior management levels?	11	73.3	3	20.0	-	-	1	6.7
Is the responsibility for information security shared by all units of the university?	7	46.7	7	46.7	-	-	1	6.7
Are the responsibilities for personal data protection clearly described in the terms of references of the university personnel's duty?	3	20	11	73.3	-	-	1	6.7
Is the "responsible person for informatics" of the university units determined in writing?	5	33.3	10	66.7	-	-	-	-
Is there an "informatics commission" founded with the aim of arranging informatics activities in the university?	6	40.0	9	60.0	-	-	-	-
Are the personal data classified and stored in separate physical environment from the other data?	6	40.0	9	60.0	-	-	-	-
Are the computers with personal data kept on different virtual networks?	10	66.7	5	33.3	-	-	-	-

[2]These studies were conducted in the context of "National and International Situation Evaluation on Personal Data Protection and Supervision Studies Carried out on Information Security and Personal Data Protection" in the Ministry of Justice, Ministry of Health, General Directorate of Civil Registration and Nationality, Revenue Administration, Social Security Institution, and General Directorate of Land Registry and Cadastre.

Are the hardware requirements in providing information security met by the management quickly?	11	73.3	2	13.3	2	13.3	-	-

Security tests of information systems and databases were conducted under the responsibility of the DPD in 66.7% of universities. The respondents stated that these security tests are conducted primarily on access authorization by personnel who either design or manage the systems. Note that these tests are not conducted in a planned and regular way, but are generally conducted depending on system or configuration changes. There are possibilities for system designers or managers to not see system deficiencies; here, the expressions of nine DPD respondents on the lack of reliable institutional resources with which they could supervise and control these systems should be taken into consideration. Therefore, DPD units do not have any option but to strain their facilities and limit their own personnel to meet these deficiencies.

The respondents were asked whether they use personal data during system security tests conducted on databases. This question aimed to obtain information on risk conditions involving personal data. While 86.7% of the respondents expressed that personal data existing on databases are not used in the test process, two respondents stated that all data are included in this process since no data classification is performed on the databases. As mentioned in the EU PDPA, being sensitive to "not using personal data in system security tests" displays the care given to personal data and personal rights in DPD units; however, as mentioned by two respondents, this process is related to the sensitivity shown by other university units in data classification. According to the research data, it is possible to separate these data from other data by using different physical environments or virtual networks by all university DPDs on the condition of classifying data by other university units. Overall, 10 out of 13 respondents who expressed that personal data are not used in the processes on databases highlighted that the databases with personal data such as personnel and student information are kept in different environments and virtual networks from other databases. These respondents commented that using virtual networks is important in providing information security, as it does not carry any financial burden and is applicable in every university. Keeping personal data in different virtual networks or data storage environments is one of the most effective application methods among the precautions taken against unauthorized access. Research by [26] shows that these kinds of technical precautions, which are low cost and highly effective, should be preferred.

In the results, 80% of the respondents gave a "no" answer to the question of whether it is clearly described in the context of which legal arrangements security precautions are taken to protect information assets. Two respondents giving a "yes" answer to this question addressed the "Usage Instruction for Informatics Resources," which does not have enough content for the protection of information assets. According to the data obtained in the research, to base the technical precautions on legal arrangements, the university DPD should examine Turkish Law Regulations, solicit expert opinions on the issue, and study this further because the issue of personal data protection is mentioned in a limited and dispersed way in the legal arrangements, except for the Act numbered 5651. There are no personnel assigned to provide information security and supervision in 60% of university DPD units. Moreover, five of six personnel expressing that one individual is assigned to provide information security stated that the individual carrying out this duty has a different main and prior responsibility. Apart from this, the individual with the responsibility for conducting this duty has a different field of expertise; however, to develop information security policies and take preventative precautions regarding these policies necessitates both expertise and knowledge. For this reason, staffing personnel working in these units, undertaking these duties and responsibilities according to their field of expertise is important. Not assigning personnel to provide information security in university DPD units causes developing policies and action plans regarding information security to be of secondary importance. The basis of this problem is the lack of staffing for providing information security in university DPD units. In only one university, a separate information security unit was found within the university DPD with personnel assigned to this position. This issue has been given a higher priority and work on staff positions has been started in one university. In the interview, some duties are divided into existing personnel as additional duties to utilize the personnel more effectively, especially in universities of foundation. DPD personnel are also given more than one responsibility in 90% of the universities of foundation.Overall, 73.3% of the respondents thought that university senior management gives importance to provisioning information security and stated that hardware requirements for the provision of information security are met quickly; however, responsibilities for information security are not shared between units in approximately half of the universities (i.e., 46.7%). There is no informatics commission arranging informatics activities and no agenda items on personal data protection in the commissions in 60% of the universities; furthermore, no individual responsible for informatics is determined in units in 66.7% of the universities. Furthermore, responsibilities on this issue are not described in the terms of references of DPD personnel in 73.3% of the universities. It is considered that senior management of the university shares in all of these deficiencies. The data obtained in the research show that senior management regards DPD as the only

authorized and responsible unit for information security, and for this reason, they think that precautions are limited in technical applications in 73.3% of the universities.

Finally, the respondents were asked how recorded personal data responsibility is shared between university units; four different answers were given by the 14 respondents. First, responsibilities and authorization conditions of units are described in a written form in only three universities. Eight respondents thought that the DPD unit is fully or partially responsible for the protection of these data. Although three respondents expressed that responsibility is not shared between units, they stated that the DPD is only responsible for storing the data. Although there is no obvious share of responsibilities in 78.6% of the universities, after combining these findings, all respondents were reported to think that they have responsibilities for storing and protecting the data existing in central servers.

4.5. Responsibilities for the Backup and Destruction of Personal Data

Backup of data is one of the most important information processing responsibilities, depending on the notion that every system will crash at some point in the future. Performing frequent backup processes provides access to uncorrupted data in case data violations or unauthorized accesses occur. Therefore, the respondents were asked how frequently personal data, which should be stored centrally, are backed up. All respondents (i.e., N = 15) answered that a daily backup is made. Moreover, a respondent stated that instantaneously changing data such as information center records are backed up hourly. Overall, 86.7% of the respondents also said that the data backup process is one of the most important DPD actions, and therefore, necessary hardware costs are not spared. There are practicesqualified to meet the backup requirements of data that are under the responsibilities of the DPD in all universities; however, according to the findings obtained in the research, there are uncertainties regarding how and who will back up the data in the computers of university units. To back up all personal data processed in university units according to a specific written backup plan and to keep records of the backup will provide an important reference to fight informatics crimes and follow the judicial procedure.

The respondents were asked whether there is a policy regarding data destruction; 93.3% (i.e., with N = 14) answered that there are no policies regarding the permanent deletion of personal data, and they did not indicate any standards used in this process. A respondent expressed that he has no idea regarding this issue. During the interview, the majority of respondents expressed that they are aware of deficiencies, but they still do not have any initiative. Moreover, four respondents emphasized that this issue requires special information and expertise, and for this reason, they need experts. Furthermore, these respondents believe that the process can work properly by creating awareness in the entire university. A draft on data destruction processes was created by the unit responsible for information security in only one university. Finally, not sharing responsibilities between university units is also one of the basic causes of the deficiencies in electronic data destruction. Throwing away information systems that are entirely unused creates risks for data processed on these systems, even if such data are deleted. Utterly removing these risks is only possible with a permanent delete process and physical destruction. On this issue, respondents were asked who the responsible personnel for the destruction process is in university units, with findings shown in Figure 2. To make this question more clear and comprehensive to the respondents, “expired hard disks over in the units” were used as an example of information storage that will be destructed.

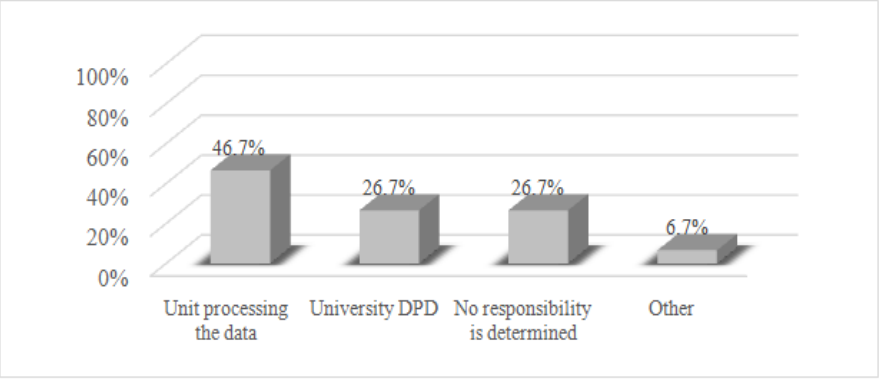

Figure 2. Destruction responsibilities of expired hard disks in university units

While 46.7% of the respondents regard the unit processing the data as responsible for destruction of the data, the rate of respondents who regard the university DPD as the only responsible unit for permanently deleting and destroying expired or defective hard disks with the help of technical methods is 26.7%. Since the destruction of electronic data is not a process that any personnel working in the university unit can do, the respondents were asked about their views on taking on the destruction and deletion process, which requires special technical information and facilities through the support of the DPD unit. All respondents stated that they

can give the necessary support to units in need or have the last step of the destruction process for hard disks be the responsibility of the DPD.Therefore, a unit that can make data destruction processes according to determined standards and give support to university units should be established; however, taking the adequacy and availability of DPD personnel into consideration, according to the research data, DPD support for data destruction to units may be limited. Thus, to develop a destruction policy and implement this policy across all units is critical. Developing data destruction policies and determining and conducting the responsibilities among university units will increase awareness of personnel processing personal data in university units and increase interest in this issue.

4.6. Establishing Risk Factors, Risk Management, and Awareness

Table 5 presents findings regarding the evaluation of information assets, risk management, written action plans, obtaining technical support from outside the university, and attack initiatives on databases. While the question regarding attack initiatives toward personal data in databases was not answered by one of the respondents, the other questions were answered by all respondents (i.e., N = 15).

Table 5. Evaluation of information assets and risk management in universities

	Yes		No		Partially	
	N	%	N	%	N	%
Is any support taken from outside for maintenance/repair of Information Systems?	9	60.0	6	40.0	-	-
Is any security investigation conducted for the workers of companies supporting from outside?	10	66.7	3	20.0	2	13.0
Is there an evaluation of information assets and risk analysis report prepared in the university?	6	40.0	9	60.0	-	-
Do you have a written action plan that can be applied in case of data violation?	2	13.3	13	86.7	-	-
Is there any attack initiative towards databases of personal data?	9	64.3	5	35.7	-	-

Overall, 60% of the respondents said that they received technical support from outside the university. There is a linear relation between the size of the university, the number of supported computers, the number of personnel working in the DPD, and the rate of receiving support from outside. While some respondents emphasized that they receive support only for central systems under the supervision of personnel, other respondents said that they receive support from companies through university units via direct communication under a contract; however, the conditions for receiving this support directly impact the risk level of the university's information security.The importance of increasing user consciousness can be felt much more when the university units receive direct support from outside. Two respondents stated that the user has the responsibility for protecting personal data, and therefore, awareness should be increased if companies giving support from outside are in direct contact with the units. Due to the need to protect such documents as patents, projects, theses, articles, books, etc., on data storage units of computers that faculty members use, not only university administrative units but also faculty members should show sensitivity to this issue.

All respondents except three expressed that partial security investigations are performed for supporting company workers in every kind of activity. Two respondents said that previous work references and records of the concerned company and its workers are evaluated in these partial security investigations. Respondents reported that criminal records and working references are generally requested form company workers. Even though university units, which receive technical support from outside, make some contracts and security investigations, they are still responsible for providing data security. University units receiving technical support are not responsible for controlling all processes that the concerned company makes. Therefore, to overcome the software problems under the supervision of users is important. If there are hardware problems in information systems and these problems cannot be overcome onsite, it is important to not remove hard disks and give them to companies providing external technical support. These points and the obligation of compliance with the information security policy should be included in the written contract made with the concerned company. Finally, note that the respondents giving the answer "no" to the question of whether the security investigation is made or not said that they do not receive any support from outside and therefore answered the question in this context.

Information assets are not evaluated and a risk analysis report is not prepared in 60% of the universities. Performing a risk analysis and generating reports serve as a basis for possible catastrophes or an action plan that will be applied when data violations occur. In this context, respondents were asked whether there is a written action plan in cases of data violations; the existence of a written plan was reported in only two universities (i.e., 13.3%). Although 64.3% of the respondents expressed that there are attack initiatives toward databases every week, the lack of action plans has no relation with data violations and attack initiatives toward

such databases. The density of internal and external attacks toward databases (i.e., 64.3%) shows that the universities are under risk and cyber threats. Universities without a written action plan do not have enough strength to fight the risks and threats in a systematic way, and there can be problems in taking the correct steps except from the perspective of the technical processes.

Respondents were also asked how much time it takes to reactivate the system when a catastrophe occurs. Respondents revealed that daily system backups can be reloaded on the same day in case of a catastrophe and the system can be reactivated. In three universities, the duration of this process can be reduced to between 10 min and 4 h, depending on the classification of data. Considering the existing risks faced by all university DPDs and the need to take precautions, the reactivation of the system at most within 24 h of a catastrophe shows that an important phase has been accomplished for risks and threats. The respondents were asked who or which units are informed in case of personal data violations, with findings shown in Figure 3. All respondents answered this question (i.e., N = 15), and the opportunity to mark more than one option was given to the respondents.

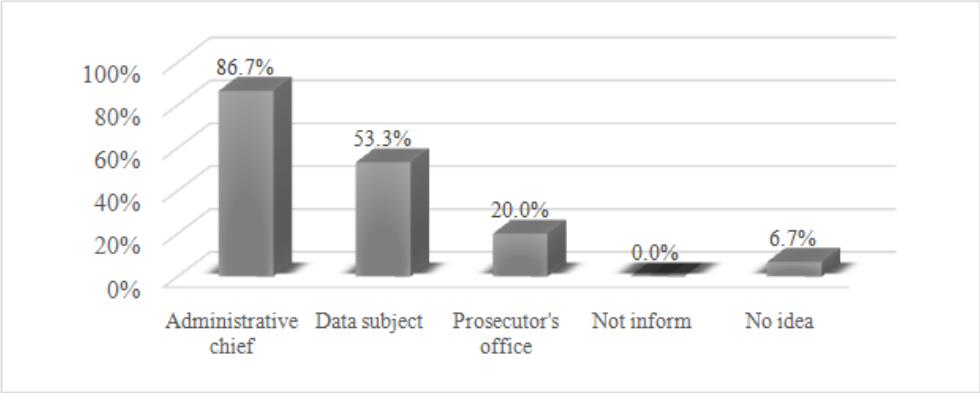

Figure 3. Who or which units are informed when a personal data violation occurs

The respondents expressed that there has yet to be any judicial cases or investigations due to data violations. In addition, 86.7% of the respondents said that the responsible administrative chief of the unit would be the first to be informed when any data violation or attack toward information assets occurred. These respondents thought that the administrative chief should inform the prosecutor's office in situations in which the prosecutor's office should be involved. Moreover, approximately half of the respondents (i.e., 53.3%) thought that the data owners, whose personal data are violated, should be informed to take necessary precautions. None of the respondents marked the option "the system will be reactivated without informing in the shortest time" and this is a key positive indicator of awareness regarding this issue. The dimension of the unauthorized access cannot be foreseen, and changes made on the system can rule out the possibility of damage compensation with legal initiatives [27].The research data indicate that there are attacks that can be called internal attacks toward university databases, and these attacks are generally made by students or graduates of the informatics departments. Although the activities of this group are not malicious, unauthorized access, prevention of the system from working, and the disruption and destruction of data are all informatics crimes and can be defined as harmful activities. Even though creating awareness in this issue is a part of implementing information security precautions, it should not be restricted to only responsible personnel for processing or storing of the data. There should be information about informatics law in all educational programs involving informatics, especially in the computer engineering department and informatics institutions. In spite of not being malicious, unauthorized access, which causes losses not only in university information processing centers but also in public foundations and institutions, can be reduced by creating this awareness.

As Höne and Eloff noted, international information security standards are one of the most important documents to be written among the resources referred to in developing information security policies [28]. Like ISO 27001, international standards are quality guides for analyzing and reporting in universities where risk analysis is not utilized. For this reason, respondents were asked how international standards like ISO 27001 contribute to risk analysis. Nearly all respondents (i.e., 86.6%) thought that it is difficult to provide and preserve the conditions these international standards require, and it is not adequate to provide it only in administrative units; however, all respondents agree that it will be an important gain to know the content of these standards and details of their application in the framework of the policies that the university determines.

Nine respondents expressed that they have not yet had any opportunity to examine and apply the standard in a detailed way for reasons such as personnel inadequacy and differences in the priority of the university's

foundation process. Six respondents said that they revise these standards at least during the application of security precautions on systems.

4.7. Additional Participant Views and Proposals regarding Personal Data Protection

Table 6 shows findings obtained from the additional views and proposals given in the portion in which the respondents could write their opinions on issues at the end of the survey as well as important points raised in the open-ended questions.

Table 6 Additional views and proposals for providing information security in universities

View	Proposal for Solution
Traditional data storing methods and radical changes and differences in the place of data storages should be evaluated.	It is necessary to redefine the responsibilities and responsible personnel for storing, collecting, and using electronic information.
New studies are required in order to see the deficiencies and realize the details of the issue.	These studies have great importance in seeing the deficiencies and examining the details of the issues. The importance of the written policies is better realized thanks to this research. Written policies also contribute to sharing responsibilities between university units. Each institution and unit should have written policies on this issue.
Various legal arrangements are utilized in order to create legal basis for personal data protection. There is no information on which kind of information in which legal arrangements. Also determining these responsibilities within the legal arrangements by the university units necessitates a number of studies to be conducted in a very difficult and long process.	Focusing on studies in which there are also legal responsibilities will be a critical gain for universities.
Since the legal arrangements do not meet the requirements, training and awareness has become more important in recent years.	More importance should indeed be given to awareness training for personnel that process personal data.
Since the personnel working and processing personal data in public universities are civil servants, they also have legal responsibilities.	It is important to add this set of responsibilities to the contract made with personnel in private universities.
There are worries about access authorizations to databases.	The "need to know" principle should be taken into consideration during the preparation of access authorizations of database software in which personal data is processed. It is necessary to arrange access authorization of the personnel working in the same unit or in the DPD to databases and keep process records in the context of this principle. The units processing personal data should regularly control the processes and changes implemented by the DPD and other units.
There is no policy about the standards that will be used in deleting hard disks permanently and destruction in universities.	Coordination with university DPDs should be provided and responsibilities in this issue should be determined and clearly delineated.
Since the processes that DPD should conduct are not recorded, the responsibilities for the processes remain ambiguous.	An information processing help desk should be established for applications for the processes that are requested from the DPD and the registering of these requests. Thus, information can be gained for many processes including mass data entrances into databases in need.
The responsibilities in the scope of ULAKBİM Acceptable Use Policy are not known by university units.	An increase in the effectiveness of internal supervision activities can be provided by transferring the responsibilities in the scope of the ULAKBİM AUP to university units.
University DPD has no authority in authorization, supervision or applying sanctions on information processing activities in the units. Moreover, DPD's awareness-raising studies can be insufficient in the universities that have too many departments.	Conducting this kind of awareness-raising by the personnel responsible for information processing in coordination with the DPD will increase the effectiveness here.

V. CONCLUSION

A University DPD units have responsibilities in the context of legal arrangements; however, the existing legal arrangements are often insufficient in terms of personal data protection and do not have preventative qualities. Since there is difficulty in evaluating the related parts of the limited and scattered legal arrangements in Turkish Law Regulations, there are also deficiencies in developing information security policies that take such legal arrangements into consideration.

The expectation that the secrecy of personal data will be maintained, which provides the decision of data owners in opening their own personal data to the access of others, including when, how, and how much [7] necessitates protection of personal data in university databases at the utmost level. As mentioned in EU directive numbered 95/46/EC, the Convention numbered 108, TCC and PDPAD, the secrecy of data and data owner rights should be protected in access or use of the data by related or other university units. To protect the rights and freedom of the individuals, technical and institutional precautions should be taken both during the design of

the systems in which the data are processed and in the actual processing of the data. Moreover, the structures, risk conditions, and costs of the data that will be protected should be taken into consideration. Increases in data also increase the costs of taking security precautions such as backups and data encryption. In spite of the increased amount of data, it is important to separate sensitive and personal data from other data by classifying them and applying security precautions at different levels. Furthermore, storing personal data under system managers will contribute to decreases in costs and application errors.

University DPD units should take necessary precautions against the accidental or illegal damage created by transferring personal data across networks, unauthorized access, and changes, and should inform university units about the precautions taken. Legal arrangements and international standards should also be taken into consideration in fulfilling these responsibilities. In addition to technical precautions, administrative precautions should include general security elements that are applicable to all university units and protect personal rights. For this reason, besides being under the responsibility of the DPD, information security should also be among the issues that university senior management gives importance to and supports. To take the necessary steps at the university senior management level, an information security council should be established to undertake the duty of coordination in every university, and an information security culture should be generalized inside of the university through this council.

It is necessary to make risk management decisions and share the responsibilities with participation across the university units to not encounter negative results obtained in information security supervision made in some state foundations and institutions [25]. Responsible personnel should be identified to process, store, protect, and destroy personal data, and it is necessary to be ready against security violations. Therefore, the risks stemming from the misuse and mismanagement of information and any failure of execution of responsibilities can be reduced. In addition, recording the processes made and classifying personal data in databases in all universities are issues that can be improved for this purpose. In the framework of the findings obtained from this research, other proposals that should be taken into consideration regarding the protection of personal data and personal rights in university DPD units include the following:

- Precautions that will protect data owner personal rights and freedom by taking technical and administrative conditions into consideration in the context of legal arrangements and university information security policies should be provided.
- Necessary physical, documental, and personnel security should be provided for centrally stored personal data. These data should not be shared in any circumstances except from the protection of a right or the prevention or investigation of a crime as required by law (including public foundations and institutions). Moreover, their destruction should be provided for at the end of an established expiration date.
- Access authorizations should be performed in the context of predetermined policies, and personal data should not be transferred through the Internet.
- In establishing information security policies for personal data protection, different resources such as EU Law Regulations together with Turkish Law Regulations and SSC should be utilized.
- It is not possible for international standards to take the place of information security policies developed by universities, since each university has its own private management and supervision system; however, these standards should be revised and suitable precautions should be applied in the framework of security policies determined by the university.
- Regular coordination should be provided with responsible personnel for information processing of units to keep security precautions for informatics systems, which include non-transferrable information to central databases in university units.
- In university units, data storage, backup, and destruction procedures should be conducted in the framework of defined standards in coordination with the DPD.
- To keep skills and awareness of DPD personnel on information security at an optimum level, more courses on these issues should be included in training programs.
- Deficiencies of technical precautions such as separating information systems from other systems with virtual networks should be corrected as soon as possible, i.e., without waiting to establish legal arrangements or increasing the awareness of all personnel.
- The increased use of informatics technologies in universities causes a weakening of processes and supervision that requires direct personnel support. Therefore, responsible personnel for information processing working in coordination with DPD units should be assigned to regularly supervise computers with personal data and increase user awareness.
- Training programs that include information regarding threats and precautions against such threats should be arranged to increase the awareness of unit managers and the personnel processing the data.

REFERENCES

[1]. T.C. Başbakanlık *Kişisel Verilerin Korunması Kanun Tasarısı ve Gerekçesi*. 2014.
[2]. King, N. and V. Raja, *Protecting the privacy and security of sensitive customer data in the cloud.* Elsevier Computer Law & Security Review, 2012: p. 308-319.
[3]. Avrupa Konseyi *Proposal for a Regulation of theEuropean Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*. 2012.
[4]. Henkoğlu, T. and B. Yılmaz, *Avrupa Birliği (AB) Bilgi Güvenliği Politikaları.* Türk Kütüphaneciliği, 2013. **27**(3): p. 451-471.
[5]. Fischer-Hübner, S., *IT-Security and Privacy: Design and Use of Privacy-Enhancing Security Mechanisms*. 2001, Berlin: Springer.
[6]. HKSAR, *An overview of information security standarts*. 2008, The Government of the Hong Kong Special Administrative Region. p. 1-18.
[7]. Winter, K.A. *Privacy and the rights and responsibilities of librarians*. 1997.
[8]. Aksoy, H.C., *The right to personality and its different manifesttations as the core of personal data*. Ankara Law Review, 2008. **5**(2): p. 235-249.
[9]. Stone, E.F., et al., *A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations.* Journal of Applied Psychology, 1983. **68**(3): p. 459-468.
[10]. Chirillo, J. and E. Danielyan, *Sun Certified Security Administrator for Solaris 9 & 10 Study Guide*. 2005, California: McGraw-Hill.
[11]. Miller, A.R., *Assault on Privacy: Computers, Data Banks and Dossiers*. 1971, Ohio: The University of Michigan Press.
[12]. Avrupa Konseyi *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*. 1995.
[13]. OECD *Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data*. 2013.
[14]. T.C. Anayasası *Türkiye Cumhuriyeti Anayasası*. 1982.
[15]. TCK *Türk Ceza Kanunu*. 2004.
[16]. TMK *Türk Medeni Kanunu*. 2001.
[17]. 5651 Sayılı Kanun *İnternet Ortamında Yapılan Yeyınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun*. 2007.
[18]. Avrupa Komisyonu *Türkiye 2012 yılı ilerleme raporu*. 2012.
[19]. Kaptan, S., *Bilimsel araştırma ve istatistik teknikleri*. 10 ed. 1995, Ankara: Rehber Yayınevi.
[20]. Karasar, N., *Bilimsel araştırma yöntemi*. 23 ed. 2012, Ankara: Nobel Yayıncılık.
[21]. Charette, R. *Zappos.com customer database breached, info on more than 24 million customers potentially accessed*. 2012.
[22]. Charette, R. *This week in cybercrime: Data breaches at Yahoo, Formspring and Nvidia*. 2012.
[23]. TÜBİTAK UEKAE *Kamu Sertifikasyon Merkezi Nitelikli Elektronik Sertifika Raporu*. 2014.
[24]. Whitman, M.E. and H.J. Mattord, *Principles of information security*. 2011, Boston: Course Technology.
[25]. DDK, *Kişisel Verilerin Korunmasına İlişkin Ulusal ve Uluslararası Durum Değerlendirmesi ile Bilgi Güvenliği ve Kişisel Verilerin Korunması Kapsamında Gerçekleştirilen Denetim Çalışmaları*. 2013, Cumhurbaşkanlığı Devlet Denetleme Kurulu: Ankara.
[26]. Wolf, M., D. Haworth, and L. Pietron, *Measuring an information security awareness program.* Review of Business Information Systems, 2011. **15**(3): p. 9-21.
[27]. Henkoğlu, T., *Adli bilişim: Dijital delillerin elde edilmesi ve analizi*. 2011, İstanbul: Pusula Yayıncılık.
[28]. Höne, K. and J.H.P. Eloff, *Information security policy - what do international information security standards say?* Computers & Security, 2002. **21**(5): p. 402-409.