Data Classification Based on Sensitivity in Public and Private Enterprises in the Republic of Kosovo

Elissa Mollakuqe[1], Vesna Dimitorva[1], Aleksandra Popovska-Mitrovikj[1]

[1] Faculty of Information Sciences and Computer Engineering, Skopje, North Macedonia
elissamollakuqe@gmail.com
{vesna.dimitrova,aleksandra.popovska.mirovikj}@finki.ukim.mk

Abstract. Storage of information and individual privacy has become among the preoccupying issues for society nowadays. In this regard, given the importance of information and the protection of personal data, Cybersecurity plays a powerful role not only in the field of information technology but also in the security of society. Cybersecurity includes the techniques used to protect the integrity of networks, software, and access from unauthorized access. It refers to the body of technologies, and processes, and can also be referred to as information technology security. In terms of information technology, security includes cybersecurity and physical security, both of which are used by enterprises to protect against unauthorized access to the information center data center and other computerized systems. This research identifies the highest level of data sensitivity in public and non-public enterprises in the Republic of Kosovo. All the information is separated into seven subcategories. The purpose of this paper is to emphasize the importance of cybersecurity in an environment and the virtual world in which we live.

Keywords: personal data, privacy, security, public enterprises, private enterprise

1. Introduction

The importance of information security in the enterprise is undeniable. One of the basic steps for the company to succeed is to take the essential steps to secure their most sensitive data against data breaches, unlawful access, and other risks to corporate and consumer data security.

To the National Institute of Standards and Technology [1] Information Security is the process of preventing unauthorized access, use, disclosure, interruption, alteration, or destruction of information and information systems in order to maintain confidentiality, integrity, and availability). Information security includes strategies, and various policy tools that identify, prevent, combat, and document threats to digital and non-digital information communication devices [6]. Enterprises that handle massive amounts of sensitive information are more exposed to these threats, such as large, medium, or small businesses, public or private hospitals, hotels, educational institutions, etc [5]. This includes threats to financial accounts, social security numbers, medical information, national security secrets, etc. Individuals are also not immune to

these threats. If you have any sensitive information such as bank accounts, medical information, etc. you are vulnerable [2].

According to Chuck Davis the biggest mistake of the companies in securing sensitive data is that they do not properly classify data and protect them from current threats. To properly protect sensitive data, there are three important components: Data Classification, Encryption, and Cloud Misuse [3].

In this paper, we present the characteristics of data security in 47 enterprises in the Republic of Kosovo by using information classification and their properties at a sensitive level. In Section 2 we define the model that we used to classify data. By using this model, we obtain the results of our research. In Section 3, we give a more complete classification of sensitive data in seven categories with four levels of sensitivity. In the end, we derive some conclusions from our analysis. In this paper, we present the characteristics of data security in 47 enterprises in Republic of Kosovo by using information classification and their properties at a sensitive level. In Section 2 we define the model that we used to classify data. By using this model, we obtain the results of our research. In Section 3, we give a more complete classification of sensitive data in seven categories with four levels of sensitivity. In the end, we derive some conclusions from our analysis.

2. Information security and data sensitivity

Companies must identify the data that needs to be secured and develop a Data Classification Policy to categorize data according to its sensitivity. For data classification, there must be at least 3 levels[3].

- Restricted - the access to these data must be restricted to a need-to-know basis only, because this is the most sensitive information that poses a serious risk if compromised.
- Confidential or Private - the access to these data is internal to the company or department that owns the information, and it is moderately sensitive data that poses a moderate risk to the company if compromised.
- Public - access to this non-sensitive information is either weakly or not at all restricted and poses little to no risk to the firm.

The sensitive data are classified, using the following steps:

1. Creating an overview of the framework based on the level of sensitivity.
2. Checking the Sensitive Security Policies on Enterprises (public and private).
3. Collecting the data.
4. Classifying the data.
    - Data re-classification

Visual presentation of these steps is given in Fig.1.

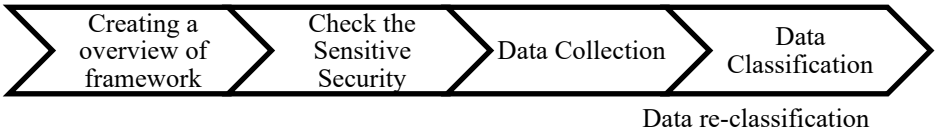

Fig. 1. The process of data classification in Enterprises

In our research, we start by creating an overview of the institutional data classification framework based on the level of sensitivity as required by the Information Security Policy of Public and Private Enterprises. Data classification will help us to determine the basic security controls for data protection.

Sensitive Information Security Policies need to be applied to all external and internal collaborators who are authorized to enter institutions and use the services of these institutions [7]. This research refers to employees responsible for the classification and protection of Institutional data, as defined by Information Security Roles and Responsibilities.

Senior enterprise personnel who manage the lifetime of one or more sets of Institutional Data should be responsible for classifying data in the proper manner. Data stewards classified the collected data according to the function that it provides and use data limiters for some content of individual data. For example, let the collected data contain information: name, surname, email, telephone number, address, and unique ID number. During the classification process, this collection of data is classified as restricted although the name, surname, and address of the collaborator are public (phone number, email address, ID number are unique).

At the end of the data classification process according to the sensitive level, the data is classified into one of the following levels: restricted data, public data, or private data. This classification aims to protect the confidentiality, integrity, and availability of Public and Private Enterprises Data. Data classification reflects the level of impact on the Public and Private Enterprise's Data if confidentiality, integrity, or availability is compromised.

3. Case study: Classification of data in public and private enterprises based on data sensitivity in the Republic of Kosovo

In this section, we analyze data collected for 47 different enterprises (public and private) in the Republic of Kosovo. These data can be stored, transmitted, or processed in any way. They can be classified into one of three sensitivity levels: Restricted, Confidential/Private and Public.

Information about what the data represents and how access, processing, storage, and communication should be managed are identified by the Sensitivity classification. The highest (strictest) level of sensitivity will be chosen if more than one level of sensitivity can be applied to the information [4].

In this research, we identify the highest level of data sensitivity for the employees in 47 public and non-public (private) enterprises, such as universities (5 public universities

and 7 private universities), banks (4 private Enterprises), Programming Enterprises (11 private enterprises), Building Company (5 private enterprises), Municipality in the Republic of Kosovo (5 Municipality: Pristina, Prizen, Gjakova, Peja, Gjilan), Non - Government Organization - NGO (5 private enterprises), hospital (1 public hospital, 1 private hospital), hotels (3 private enterprises).

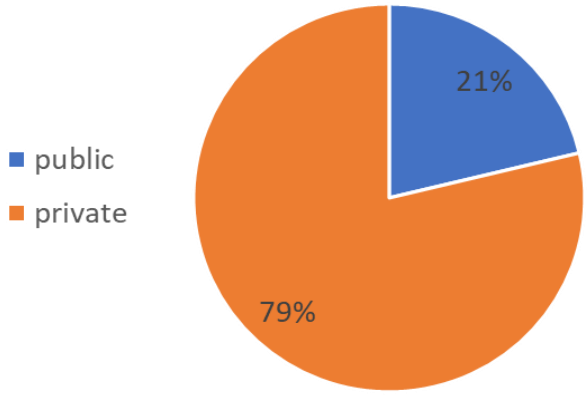

Fig. 2. Percentages of Public and Private Enterprises

In Table 1. we classify all collected data into subcategories.

Table 1. Subcategories and data collected in Enterprises (Public and Private)

Categories	Collected information
Personally Identifiable Information (PII)	State-issued identification card number Financial account number Access code or password that would permit access to the account [6][7] Medical and/or health insurance information State-issued driver's license number
All records and/or other information subjects according to regulations (Reg)	HIPAA - Health Insurance Portability and Accountability Act [7] COPPA -Children's Online Privacy Protection Act [10] GLBA - Gramm-Leach-Bliley Act [10] EU - General Data Protection Regulation US Privacy Act of 1974 [10] LAW NO. 06/L – 082 ON PROTECTION OF PERSONAL DATA

Information regarding an individual's mental or physical condition and/or history of health services use and/or other information subject to HIPAA regulations (HIPAA)	Name, Surname Address Birthday Phone Numbers Fax numbers Email addresses Medical record numbers Health insurance beneficiary numbers Account numbers Certificate/license numbers Device identifiers and serial numbers; Web Uniform Resource Locators (URLs) Internet Protocol (IP) address numbers Biometric identifiers, including finger, retinal and voiceprints Full face photographic images and any comparable images [8]
Financial information (FI)	Name, Surname Address Birthday Phone Numbers Fax numbers Email addresses Credit card Bank information Budgeting Salary Financial report for last 6 month
Human Resources information (HRI)	Name, surname Address Revealing a natural person's race Health status Ethnic social origin Conscience Belief Genetic data Biometric data Property details Marital status Family details including names of the person's children Parents Spouse or spouses Sex Sexual orientation of the data subject
Research (Res)	Name, surname University

	Department Journals Payment
Other data the project sponsor considers sensitive, private, confidential or non-public (Other)	Depends on the declaration of the enterprise

The obtained results for classification of data sensitivity in the considered enterprise are presented in Table 2. In this table for each type of considered enterprise (rows), we give the level of sensitivity (Restricted, Confidential or Private and Public) for the following categories of information (columns): Personally Identifiable Information (PII), All records and/or other information subjects according to regulations (Reg), Financial information including credit card and bank information, budgeting, salary and financial aid information (FI), Human Resources Information (HRI), Research (Res).

Table 2. Classification of data sensitivity in considered enterprises

	Categories of data				
	PII	**Reg**	**FI**	**HRI**	**Res**
Public University	**Private Restricted** Online, financial data	**Public** Internal Regulation	**Confidential and Private** Financial Data		**Public** Online data
Private University	**Private Restricted** Online, financial, medical data		**Confidential and Private** Financial Data		**Public** Online data
Private Bank	**Private Restricted** Online, financial, medical data	**Private Restricted** Online, financial, medical data Internal Reg. EU- General Data Protection Reg.	**Private Restricted** Online, financial data	**Private Restricted** Biometric data	

Private Building Company	**Private Restricted** Online, financial, data		**Private Restricted** Online, financial data	
Private Programming enterp.	**Private Restricted** Online, financial, data		**Private Restricted** Online, financial data	
Public Municipality	**Private Restricted** Online, financial, data	**Private Restricted** Online, financial, medicinal data Internal Regulation	**Private Restricted** Online, financial data	**Private Restricted** Biometric data
Public Hospital	**Private Restricted** Online, financial, data		**Confidential and Private** Financial Data	
Private Hospital	**Private Restricted** Online, financial, medical data	**Public** Internal Regulation HIPAA Health Insurance Portability and Accounta-bility Act	**Confidential and Private** Financial Data	
Private Hotels	**Private Restricted** Online, financial, data		**Private Restricted** Online, financial data	
Non - Government Org. NGO	**Private Restricted** Online, financial, data	**Private Restricted** Online, financial, political, data Internal	**Private Restricted** Online, financial data	

Regulation EU- General Data Protection Regulation	
COOPA- Children's Online Privacy Protection Art	

From the information given in Table 2., we can see that in all considered types of enterprise, Personally Identifiable Information, Financial Information, and Human Resources Information are Private and Restricted or Private and Confidential. In Private Hospitals and Public Universities, information subjects according to regulations (Reg) are Public, but in other types of enterprises, this information is Restricted. Clearly, we have research information only at universities, and at both types of universities, this information is Public.

4. Conclusion

Data classification is lacking in many enterprises in the Republic of Kosovo and personal data in most cases are highly exposed to misuse. Classification based on the proposed categories and finding sensitivity will help companies to increase data security and protect the systems that use this data. The main finding in this research is that the public and private enterprises in the Republic of Kosovo have the main source for Data Security as the Law on Personal Data Protection of the Republic of Kosovo: LAW NO. 06/L – 082 ON PROTECTION OF PERSONAL DATA [9].

References

1. NIST: https://csrc.nist.gov/glossary, last accessed 2022/06/10
2. Montclair State University - Responsible Use of University Computing Resources Policy Document Data Classification and Handling (Safeguarding Sensitive and Confidential Information),https://www.montclair.edu/media/montclairedu/oit/policies/Data-Classification-and-Handling-Policy-1.0.pdf, last accessed 2022/06/10
3. Information Security Office "Guidelines for Data Classification" v 1.4 create 12.02.2021 Mellon Univeristy, https://www.cmu.edu/iso/governance/guidelines/data-classification.html last accessed 2022/06/10

4. Albrechtsen, E., Hovden, J.: The information security digital divide between information security managers and users, Computers & Security, 28 (6), 476-490 (2009).
5. Workman, M.: A field study of corporate employee monitoring: Attitudes, absenteeism, and the moderating influences of procedural justice perceptions, Information and Organization, 19 (4), 218-232 (2009).
6. Tipton, H.F., Krause, M.: Information Security Management Handbook, Taylor & Francis Group, Boca Raton (2007).
7. Schultz, E.E., Proctor, R.W., Lien M.C., Salvendy, G.; Usability and security an appraisal of usability issues in information security methods, Computers & Security, 20 (7), 620-634, (2001).
8. Ruighaver, A.B., Maynard, S.B., Chang, S.: Organizational security culture: Extending the end-user perspective, Computers & Security, 26 (1), 56-62. (2007)
9. Gazeta Zyrtare e Republikes se Kosoves: https://gzk.rksgov.net/ActDetail.aspx?ActID=18616, last accessed 2022/06/15
10. Mróz, K. (2020). Threats to the individual's right to privacy in relation to processing of personal data in order to prevent and combat crime. Ius Novum, 14(1), 82-97. doi:10.26399/iusnovum.v14.1.2020.05/k.mroz