Data protection by defining the necessary controls to reduce the risk of unauthorized access to sensitive data

Elissa Mollakuqe[1], Vesna Dimitrova[1]
[1] Faculty of Information Sciences and Computer Engineering, Skopje, North Macedonia

{elissamollakuqe}@gmail.com
{vesna.dimitrova}@finki.ukim.mk

Abstract. Data protection is given as an interlinked process of monitoring sensitive data within the frameworks, regulations and jurisdiction of a country, region or specific organization. Where each country based on the GDPR appoints a data protection authority which is responsible for investigating cybercrimes, correcting data and giving advice on data protection. The cyber threats developed in the Western Balkans threatened privacy and data protection in almost every country of this region, where many sensitive data fell into the hands of hackers or many systems were blocked for a certain period of time. To prevent these two types of problems, it is necessary to assign controls or filters to reduce the risk of unauthorized access to sensitive data. In our research, the collected data is classified into three main categories (private, public, private), which are then analyzed based on the amount and type of data circulating in the implemented systems, the type of encryption used, encryption configurations and data backup, a solution is provided in data protection by defining access controls to sensitive data. The purpose of our research is to provide insight into the current state of data protection in governmental, public institutions, and various service companies in order to provide a new solution that offers data protection which is based on the specifics of the amount and type of data, encryption and coding of data before and during transmission and data backup.

Keywords: data, protection, unauthorized, risk, attack and control

1 Background, motivation and research question

Data protection is an essential process that involves monitoring sensitive data and ensuring its security within the frameworks, regulations, and jurisdiction of a country, region, or specific organization [1]. Each country appoints a data protection authority responsible for investigating cybercrimes, correcting data, and giving advice on data protection, based on GDPR regulations. These threats have resulted in hackers gaining access to sensitive data or blocking critical systems for a particular period of time. To mitigate these risks, it is essential to assign controls or filters to reduce unauthorized

access to sensitive data. These data can be stored, processed, or transmitted in any way. They can be classified into one of three levels of sensitivity: Restricted, Confidential/Private and Public [3]. We have analyzed this data based on the amount and type of data circulating in the implemented systems, encryption configurations, and data backup, providing a solution in data protection by defining access controls to sensitive data. Our research aims to offer insight into the current state of data protection in governmental and public institutions, and various service companies, providing a new solution that offers data protection based on the amount and type of data, encryption, and coding of data before and during transmission and data backup. The importance of data protection has increased significantly in recent years, as more and more sensitive information is being stored and shared digitally [7]. This includes personal data, financial data, medical records, and other types of confidential information that can be used for malicious purposes if they fall into the wrong hands. The General Data Protection Regulation (GDPR) is a European Union regulation that sets out rules for the protection of personal data. It applies to all EU member states and regulates the processing of personal data both within the EU and outside of it. GDPR is a set of rules designed to give individuals more control over their personal data, and to ensure that organizations take adequate measures to protect personal data from misuse, loss, unauthorized access, and disclosure [2]. Each country based on the GDPR appoints a data protection authority which is responsible for enforcing the regulation and ensuring compliance.

The motive of this research is based on the identification of the necessary requirements for the protection of sensitive data based on international data protection standards. The motive for such a research comes after the many threats that have developed in the last three years in many government institutions where many hackers from different countries manage to break government systems, get data for important individuals and with state influence or on February 26, the Ministry of Internal Affairs of Kosovo issued a statement about a large-scale "phishing" attack, but which did not block information or data. Furthermore, even North Macedonia has declared several cases of cyber attacks, where the attack of July 15, 2020, which was a powerful DDoS attack directed at the website of the State Election Commission, is considered the most serious. This attack took place on the day of the elections in the Republic of North Macedonia, where then the commissioners were forced to open a YouTube channel and manually update the election results. Such attacks are located in many countries of the Western Balkans and beyond which they targeted various institutions, commercial banks, public and private institutions and various service enterprises.

The specific problem addressed is data protection by defining the necessary controls to reduce the risk of unauthorized access to sensitive data. By determining the amount and type of data circulating in implemented systems, the type of encryption used, encryption configurations and data backup, a solution is provided in data protection by determining access controls to sensitive data.

While the research questions of the research are:

- What is the current state of data protection in front of our model?
- Will government institutions, public and private enterprises, commercial banks, hospitals and other service companies be able to assess the current situation through the analysis of the amount of data, the type of data moving through the

systems, encryption and pre-coding and during transmission and creation of backups.
- How many other factors such as (political situation, economic situation and social structure) will affect the implementation of the data security model created after the current analysis?

Many other authors and researchers gave different ideas on how to protect against attackers, such as: classifying data based on sensitivity, assigning a regulator for access to information, using different filters to access data, etc. But our research provides a new solution in ensuring data protection, which is based on the specifics of the amount and type of data, encryption and coding of data before and during transmission and data backup. Based on the basic function of this research, which consists in finding a concrete answer to the question of what is the current situation in terms of data protection. The results of this research will be used to take appropriate measures and activities that will lead to faster achievement of improved performance in terms of data protection.

The research follows the paradigm of qualitative research, which is a deep insight into the nature of the problem of the phenomenon under investigation, for a limited number of respondents, quantifying some of the results obtained, the frequency of which is significant. Research will be reduced to interpreting findings and providing a solution. Surveys, interviews, content analysis will be used as data collection techniques. As an instrument, survey questionnaires will be completed by all research participants.

The research questionnaire for determining the current state consists of data for the respondent and is divided into five groups of questions, questions related to the current functionality of the security system.

1. The amount and type of data circulating in and out of the system
2. Backups and copies of data as an example: can data be downloaded by users
3. Linking data with other applications and systems
4. Coding data during non-working days and during transmissions
5. Encryption, encryption configuration and encryption deployment

Data processing will be carried out by applying the SPSS software package in the following phases: data collection and grouping, logical control, entering data into computer, verification of entered data, processing and tabulation, graphic design and presentation.

2 Comparison of Public and Private Institution of data protection and the risk of unauthorized access to sensitive data

Cyber threats are becoming increasingly sophisticated and can cause significant harm to individuals, organizations, and even countries. In the Western Balkans, cyber attacks have become a major issue, threatening the privacy and data protection of many institutions and individuals. To address these threats, it is necessary to implement controls

and filters that can reduce the risk of unauthorized access to sensitive data. This can include measures such as encryption, access controls, and data backup.
Data protection is the process of safeguarding sensitive data from unauthorized access, use, disclosure, destruction, or modification. It involves implementing various controls and measures to ensure the confidentiality, integrity, and availability of data.
The controls used for data protection can include access controls, encryption, backup and recovery processes, network security, and physical security measures. Access controls limit the people who can view, modify, or delete data [5]. Encryption helps protect data in transit and at rest by converting it into a code that can only be read by authorized parties. Backup and recovery processes ensure that data can be recovered in case of data loss or corruption [8]. Network security measures help protect data as it is transmitted across networks, and physical security measures help protect data storage devices from unauthorized access or damage [6]. Defining necessary controls for data protection involves a comprehensive evaluation of the risks associated with the sensitive data being processed, the regulatory requirements and guidelines that apply, and the technological capabilities of the systems being used. By implementing appropriate controls, organizations can reduce the risk of data breaches and ensure that sensitive data is protected from unauthorized access.

In this section, we analyze 107 different enterprises (public and private) where we identify 62% of the institutions included in the research have not determined the capacity of the data that can be removed from system and 84% of institutions do not have preventive measures for data copying.

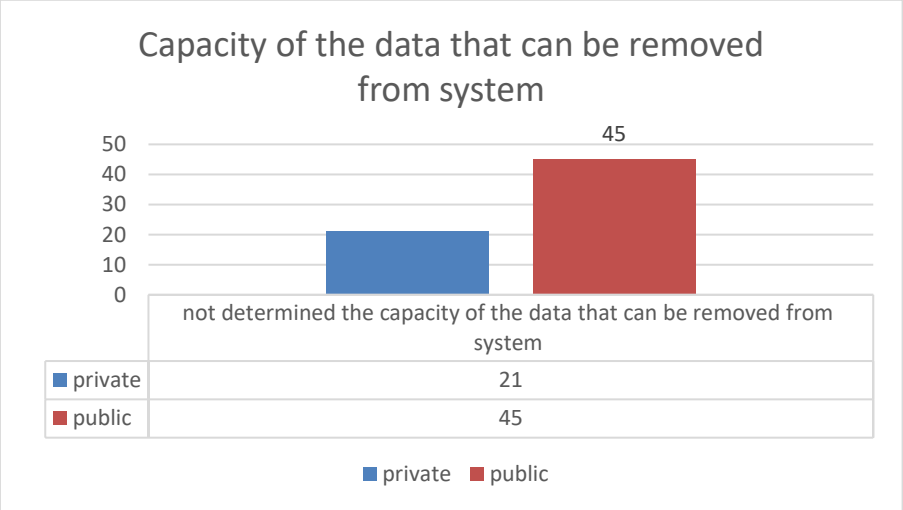

Figure 1. Total number - 62% of the institutions included in the research have not determined the capacity of the data that can be removed from system

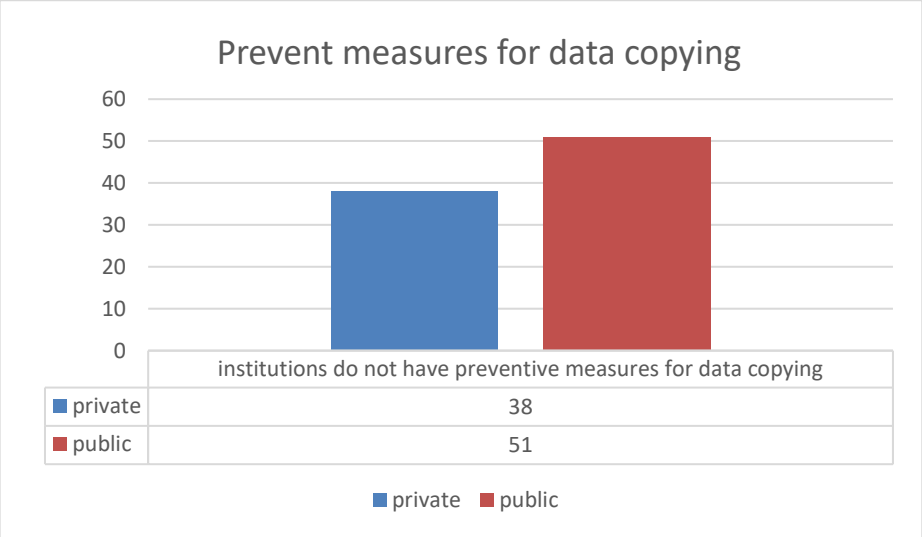

Figure 2. Total number - 84% of institutions do not have preventive measures for data copying

The table 1 and 2 presents a comparison of data protection requirements between public and private Institutions. The tables lists the data protection requirements, including restrictions on data leaving the system, creation of shadow copies of data, data interface with other systems, encryption of non-public data at rest, encryption of data transmitted over untrusted networks, and the type of encryption used and its configuration.

Table 1. Data Protection Requirements for Public Institutions

	PUBLIC INSTITUTIONS
Restrictions on data leaving system	Yes, limited to authorized personnel and with proper authorization
Shadow copies of data created	No, not anticipated
Data interface Shadow copies of data created with other systems	Yes, with proper security measures in place and in compliance with data protection regulations
Encryption of non-public data at rest	Yes, with strong encryption and access controls in place
Encryption of data transmitted over untrusted networks	Yes, with strong encryption and proper security measures in place
Type of encryption used and configuration	AES 256-bit encryption with proper key management and configuration

The Table 1 presents how public Institutions fulfill each requirement. For instance, public Institutions restrict the data leaving the system to authorized personnel with

proper authorization. They do not anticipate the creation of shadow copies of data. They interface their data with other systems while ensuring compliance with data protection regulations. They use strong encryption and access controls to protect non-public data at rest and transmit data with strong encryption and proper security measures in place using AES 256-bit encryption with proper key management and configuration.

Table 2. Data Protection Requirements for Private Institutions

	PRIVATE INSTITUTIONS
Restrictions on data leaving system	Yes, limited to authorized personnel and with proper authorization
Shadow copies of data created	Yes, with proper authorization and security measures in place
Data interface with other systems	Yes, with proper security measures in place and in compliance with data protection regulations
Encryption of non-public data at rest	Yes, with strong encryption and access controls in place
Encryption of data transmitted over untrusted networks	Yes, with strong encryption and proper security measures in place
Type of encryption used and configuration	RSA 2048-bit encryption with proper key management and configuration

Similarly, the Table 2 shows how private Institutions fulfill each requirement. Private Institutions restrict data leaving the system to authorized personnel with proper authorization. They create shadow copies of data with proper authorization and security measures in place. They interface their data with other systems while ensuring compliance with data protection regulations. They use strong encryption and access controls to protect non-public data at rest and transmit data with strong encryption and proper security measures in place using RSA 2048-bit encryption with proper key management and configuration.

The previous Tables 1 and 2 provides a concise and clear comparison of how public and private Institutions protect their sensitive data, allowing the reader to quickly and easily understand the similarities and differences between the two:

2.1 A comparison of the data protection requirements for public and private institutions using set theory

Let A represent the set of data protection requirements for public institutions and B represent the set of data protection requirements for private institutions.

Restrictions on data leaving system

Public*: A* = {limited to authorized personnel and with proper authorization}
Private: *B* = {limited to authorized personnel and with proper authorization}
A = *B*, as both sets have the same requirement

Shadow copies of data created:

Public*: A* = {not anticipated}
Private: *B* = {with proper authorization and security measures in place}
$A \cap B = \{\ \}$, as there are no common elements between the sets

Data interface with other systems

Public: *A* = {with proper security measures in place and in compliance with data protection regulations}
Private: *B* = {with proper security measures in place and in compliance with data protection regulations}
A = *B*, as both sets have the same requirement

Encryption of non-public data at rest

Public: *A* = {with strong encryption and access controls in place}
Private: *B* = {with strong encryption and access controls in place}
A = *B*, as both sets have the same requirement

Encryption of data transmitted over untrusted networks

Public: *A* = {with strong encryption and proper security measures in place}
Private: *B* = {with strong encryption and proper security measures in place}
A = *B*, as both sets have the same requirement

Type of encryption used and configuration

Public: *A* = {AES 256-bit encryption with proper key management and configuration}
Private: *B* = {RSA 2048-bit encryption with proper key management and configuration}
$A \cap B = \{\ \}$, as there are no common elements between the set

Comparisons are made between public and private institutions regarding data protection and the risk of unauthorized access. Data protection requirements, including data restrictions, shadow copies, data interfaces, encryption at rest and during transmission, and encryption types and configurations, are examined. The main differences between the data protection requirements for public and private institutions

are related to the creation of shadow copies of data and the type of encryption used and configuration.

Based on the provided information, data protection can be summarized as follows: Data protection is crucial in today's digital landscape due to the increased storage and sharing of sensitive information, including personal, financial, and medical data and the General Data Protection Regulation (GDPR) is a significant regulation that sets rules for protecting personal data within the European Union and beyond. Each country appoints a data protection authority responsible for enforcing the regulation and ensuring compliance.

3 CONCLUSION

Cyber threats have become increasingly sophisticated, and attackers can gain access to sensitive data or disrupt critical systems. Implementing controls, filters, and encryption can help mitigate these risks. The research analyzed the current state of data protection in governmental and public institutions, as well as various service companies, and provide a solution based on the analysis of data amount and type, encryption configurations, and data backup. Our main conclusions are:

Implementing appropriate controls and measures, organizations can reduce the risk of data breaches and ensure the confidentiality, integrity, and availability of sensitive data.

The current systems in terms of the amount of data must be adapted to new policies and strategies for combating cybercrimes where they must function and be administered based on Regulation (EU) 2018/1725, as well as under the GDPR

- The current strategy for data quality management should refer to the principles referred to GDPR and Article 4 of Regulation (EU) 2018/1725
- 62% of the institutions included in the research have not determined the capacity of the data that can be removed from system
- 84% of institutions do not have preventive measures for data copying
- In all institutions there is cooperation of systems among themselves
- In all institutions there are implementations for coding and encryption of data

According to the analysis, a new proposal has been reached on the management of attacks with the aim of increasing data protection. The research came to the conclusion that in government institutions, public and private institutions, commercial banks and service companies, it is necessary to review strategies for cyber warfare and to design new strategies that cover the aspects of the amount and type of data they process, encryption and coding of data as well as back up or copy of data.

References

1. Jonathan Armstrong and Paul Lanois , *Data Protection and Compliance in Context*, https://www.perlego.com/book/787825/data-protection-and-compliance-in-context-pdf
2. Elissa Mollakuqe, Vesna Dimitrova, *Privacy and Data Security Assessment for IT Vendor Services - strategic approach for Vendor IT Services analysis under GDPR*, https://iconcs.karabuk.edu.tr/
3. Elissa Mollakuqe, Vesna Dimitrova, Aleksandra Popovska-Mitrovikj *Data classification based on sensitivity in public and private institutions*,14th ICT Innovations Conference 2022 - https://proceedings.ictinnovations.org/2022/paper/573/data-classification-based-on-sensitivity-in-public-and-private-Institutions-in-the-republic-of-kosovo, ICT Innovations 2022, Skopje, North Macedonia
4. Theo P. van der Weide, Giovanni Iachello, and Jason C. Watson, *Data Protection: Governance, Risk Management, and Compliance*, http://dret.net/biblio/dret.xml
5. Bart Preneel, *Data Protection and Privacy: The Age of Intelligent Machines*, https://ieeexplore.ieee.org/author/37272469600
6. John D. Kielbus, *Data Protection: Ensuring Data Availability*, ISBN 9780367474102422 Pages 141 B/W Illustrations, Published May 18, 2020 by Auerbach Publications
7. Tom Petrocelli, Data Protection and Information Lifecycle Management. Released Septeber 2005, Publisher(s): Pearson. ISBN: 0131927574
8. Moira Pollock, Paul Ticher, *Data Protection Strategy: Implementing Data Protection Compliance*, https://www.aiac.world/pdf/January%e2%80%93March2014Issue?pdf_url=//ovugri.ml/mon13aiacworld7oz655