Analysis of data security and privacy in public institutions according to GDPR in the Republic of Kosovo

Elissa Mollakuqe[1], Ersan Hamdiu[1], Nida Santuri Fishekqiu[1] and Samir Jakupi[1]
[1] Faculty of Computer Science- AAB College/ Pristina 10000, Republic of Kosovo
elissa.mollakuqe@universitetiaab.com, ersan.hamdiu@universitetiaab.com,
nida.santuri@universitetiaab.com, samir.jakupi@universitetiaab.com,

Abstract - **Data security is a major issue for every institution. The data for each individual who interacts with an institution, whether an employee or a seeker of services from the institution, must be stored and protected. The process of securing data and implementing privacy requires a high degree of investigation and certain professionalism. In order to provide such a service, many institutions use high standards to prevent data attacks and privacy violations. GDPR - 2016/679 - General Data Protection Regulation) comes in two versions OJ L 119, 04.05.2016; cor. OJ L 127, 23.5.2018. In this paper, we present the harmonization between the regulation which contains the privacy laws and the current state of data security in public institutions and the preservation of privacy. The paper used the method of analysis of current documents and comparison with GDPR - 2016/679 - General Data Protection Regulation.**

Keywords **–attack, security, privacy, GDPR, data, and institution**

I. INTRODUCTION

The General Data Protection Regulation 2016/679 is applicable to the following types of processing of personal data: processing that is entirely or partially automated; processing that is not automated but incorporates or is intended to incorporate personal data into a filing system. (ico. Information Commisioner's Office, 02.Aug.2018)

According to the General Data Protection Regulation 2016/679 - "personal data" refers to any information pertaining to a named, recognizable, or locatable individual (a "data subject"). An identifiable natural person is one who can be located, directly or indirectly, especially by reference to an identifier like a name, identification number, location information, online identifier, or one or more characteristics unique to that natural person's physical, physiological, genetic, mental, economic, cultural, or social identity [4].

To be able to implement suitable security measures, it is crucial to distinguish between processed personal data and sensitive personal data. Personal Information is any information a person may possess about another is deemed personal information as long as it may be used to identify a natural person. illustrative personal. Name, address, phone number, social security number, email, photographs, as well as license number, IP address, and cookies, are all examples of data [11].

Additionally covered by the General Data Protection Regulation 2016/679 are "special category" and "sensitive" personal data. Such information might relate to the data subject's race, ethnicity, politics, religion, union membership, genetics, biometrics (if used for identification reasons), health, sexual orientation, or sex life [4].

The most significant ones to which we make reference in this article are listed below. Personal data represent all information relating to an individual who can be directly or indirectly identified is considered personal data. Email addresses and names are obviously personal information. Political viewpoints, browser cookies, ethnicity, gender, biometric data, and location details can all be considered personal data. The term can also apply to pseudonymous data if it's pretty simple to identify a person using it. Data processing are any data-related action, whether automatic or human. Examples given in the text include gathering, recording, structuring, using, deleting, and arranging. therefore, anything. Data controller present person will be in charge of deciding how personal data will be processed. If you have access to data in your organization, this is you. Data Processor are the third party that processes personal data on behalf of a data controller. The General Data Protection Regulation 2016/679 has specific rules for these individuals and organizations. They could include cloud-based services such as Tresorit or email providers such as Proton Mail.

In this paper, are present data security in public enterprises according to General Data Protection Regulation 2016/679 in the Republic of Kosovo. In section 2, are provided details for the management and administration of enterprises according to General Data Protection Regulation 2016/679.

In section 3, is a complete guide about the process of resolving issues related to data security, the staff responsible for the prevention and investigation of security breaches, encryption standards and the recovery of access in case of any incident.

At the end are presented some conclusions and recommendations are given.

II. DATA SECURITY AND PRIVACY

As long as users are entirely anonymous and cannot be identified from the data you retain; you are permitted to store and collect certain information under the GDPR. The information must be retained for as short a time as possible.

Organizations must only gather personal data on a legal basis, according to the GDPR. The following 6 legal bases are provided under Article 6 of the GDPR: (Privacy research team, 2022)

- Consent
- Contact performance
- Observing a legal requirement
- Important interest
- Social interest
- Authentic interest

A. Data retention

The GDPR data retention regulations typically provide that any personal data gathered or processed must only be maintained for as long as it is required to achieve the purpose for which it was collected, with a few exceptions, such as for scientific or historical study. The GDPR also provides the "right to be forgotten" or the right to erasure.

In the following situations, data subjects have the right to request that their personal data be deleted (and to stop that personal data from being processed):

a) When the personal data is no longer needed for the original reason, it was collected or processed [8].

b) When the data subject withdraws their consent[8].

c) When the data subject objects to the processing of their personal data and the Organization does not have an overriding legitimate interest [8].

d) When the personal data is processed unlawfully (i.e., in violation of the GDPR)[8].

A local data protection authority (DPA) must be notified of a data breach that potentially endangers data subjects within 72 hours. In accordance with GDPR, affected subjects must be informed: "without undue delay." Test breach management processes and answers to data subject requests on a regular basis to make sure staff members can achieve these dates [2].

B. Data verification

To fulfill a data access request, you must confirm the identity of the consumer making the request and the consumer to whom you are disclosing the personal information.

Identity verification guarantees that the consumer and the individual requesting their data are the same person in order to comply with GDPR. It accomplishes this by conducting an identification check on the requester using both previously collected consumer identity data and extra information [5].

The right to request that their personal data be deleted or otherwise disposed of (notwithstanding the retention periods otherwise set forth in this Data Retention Policy), the right to limit the use of their personal data by the Organization, and additional rights relating to automated decision-making and profiling are all provided to data subjects with regard to the personal data held by the Organization[4].

C. What exactly is the right to information

The right to information protects several of the most significant GDPR transparency principles. It requires telling people in clear, explicit terms what you do with their personal information.

When information is acquired directly, the individual must be told as soon as possible, or at the time the information is acquired. (ico. Information Commisioner's Office, 02.Aug.2018)

Additionally, the right to be informed covers details such as how long personal data will be kept, the data subject's rights, the capacity to revoke consent, the right to file a complaint with the appropriate authorities, and whether or not providing personal data is required by law or contract. In addition, all automated decision-making processes, including profiling, must be disclosed to the data subject [7].

The right to information in a clear, visible, understandable, and freely available format belongs to the data subject. It is possible to fulfill the obligation to inform in writing or electronically.[7]

D. Data Principels Protection

If you process data, you have to do so according to seven protection and accountability principles

- Processing must be lawful, fair, and transparent to the data subject in order to protect their privacy.
- Purpose Limitation - They must process the data for the legitimate purposes expressly indicated to the data subject at the time of collection.
- Data minimization - You should only collect and process as much data as is strictly necessary for the stated purposes.
- Accuracy You must keep Personal Data accurate and up to date.
- Storage limitation You may only store personal data for as long as is necessary for the stated purpose.
- Integrity and confidentiality - Processing must be carried out in a way that ensures appropriate security, integrity and confidentiality (e.g. by using encryption).
- Accountability - The data controller is responsible for being able to demonstrate compliance with all of these principles by the GDPR [5]

Data protection by design and by default - Art. 25 GDPR

- Taking into account the state of the art, the implementation costs and the nature, scope, context and purposes of the processing, as well as the risks of different likelihood and severity associated with the processing for the rights and freedoms of natural persons, the person responsible both at the time of determining the Means of processing as well as at the time of the processing itself appropriate technical and organizational measures, such as way and to integrate into the processing the necessary guarantees to meet the requirements of this Regulation and to protect the rights of the data subjects [5].
- The person responsible takes appropriate technical and organizational measures to ensure that by default only the personal data required for the respective processing purpose are processed. This obligation applies to the amount of personal data collected, the scope of their processing, the duration of their storage and their accessibility. In particular, such measures ensure that, by default, personal data is not made available to an indefinite number of natural persons without individual intervention [5].

E. Appropriate technical and organisational measures

The protection of the rights and freedoms of natural persons with regard to the processing of personal data requires that appropriate technical and organizational measures are taken to ensure that the requirements of this regulation are met. In order to be able to demonstrate compliance with this regulation, the controller should issue internal guidelines and implement measures that correspond in particular to the principles of data protection by design and data protection by default [5]. Such measures could include, inter alia, reducing the processing of personal data to a minimum, pseudonym mising personal data as soon as possible, enabling transparency in relation to the functions and the processing of personal data, enabling the data subject to monitor data processing and enable the person responsible to create and improve security functions. When developing, designing, selecting and using applications, services and products that rely on the processing of personal data or process personal data to fulfill their task, manufacturers of the products, services and applications should be encouraged to take the right to data into account To protect data protection in the development and design of such products, services and applications and to ensure, taking into account the state of the art, that controllers and processors can fulfill their data protection obligations [5]. The principles of data protection by design and by default should also be taken into account in the context of public tenders.

F. Role of the Right of access

The right of access plays a central role in the General Data Protection Regulation (GDPR). On the one hand, because only the right of access allows the data subject to exercise further rights (such as rectification and erasure) [5]. On the other hand, because an omitted or incomplete disclosure is subject to fines. In the GDPR, the right of access plays an important role, because the right of the access allows data subject exercise further rights (such as rectification and erasure) also an incomplete or omitted disclosure is subject to fines.

There are two stages to request right of access. First the controller must check whether any personal data of the person seeking information is being processed at all and must report a result based on search. If the answer is positive, the second stage involves a whole range of information[5].

The right of access includes information about the processing purposes, the categories of personal data processed, the recipients or categories of recipients, the planned duration of storage or criteria for their definition, information about the rights of the data subject such as rectification, erasure or restriction of processing, the right to object, instructions on the right to lodge a complaint with the authorities, information about the origin of the data, as long as these were not collected from the data subject himself, and any existence of an automated decision-taking process, including profiling, with meaningful information about the logic involved as well as the implications and intended effects of such procedures[5].

Depending on the circumstances, information can be disclosed to the data subject in writing, electronically, or verbally under Art. 12(1) sentences 2 and 3 of the GDPR[5]. According to GDPR Article 12(3), information must be shared as soon as possible, but no later than one month. Only in extraordinary circumstances may this one-month limit be exceeded. In most cases, the information must be provided free of charge. If more copies are required, a reasonable fee reflecting administrative costs can be requested. The controller may also refuse a data subject's right of access request if it is unjustified or excessive. If the controller is processing a large volume of information on the data subject, he or she has the additional right to specify their request within the right of access for specific data processing or kind of information [5].

"The Right of Access." *Data Protection Commission*, https://www.dataprotection.ie/en/individuals/know-your-rights/right-access-information. Accessed 13 November 2022.

"Right of Access - General Data Protection Regulation." *GDPR*, https://gdpr-info.eu/issues/right-of-access/. Accessed 13 November 2022

G. Data Processing based on Contract

The General Data Protection Regulation (GDPR) provides a standard, Europe-wide option for so-called "commissioned data processing," which is the collection, processing, or use of personal data by a processor in accordance with the controller's contractual instructions.

In most circumstances, commissioned data processing follows a contract. GDPR Article 28(3) specifies the minimal standards. The contract must specify the sort of personal data that will be processed, as well as the object and purpose of the processing [5]. In addition, the processor has other responsibilities. For example, he must keep a record of the processing activities, which contains the names and contact information of each controller for whom he works, as well as the processing categories carried out for them [5].

The controller must ensure, in selecting the processor, that it has implemented sufficient technical and organisational measures to ensure that processing meets the requirements of the Regulation.

Basically, the controller is the first contact for the data subject and responsible that the data processing complies with the legal requirements [5].

"Processing - General Data Protection Regulation." *GDPR*, https://gdpr-info.eu/issues/processing/. Accessed 13 November 2022.

H. Data Security Regulations

A crucial component of regulatory compliance is data security. Data security is a crucial part of compliance in the majority of regulatory frameworks in our case GDPR. As a result, you must take data security seriously and collaborate with a knowledgeable compliance partner to make sure you're taking all the necessary precautions [5]. The right data security technologies can help your organization in preventing breaches, lowering risk, and sustaining protective security measures. To prevent data breach you may use Data Auditing, Data Real-Time Alerts, Data Risk Assessment, Data Minimization, Purge Stale Data To minimize the chances of a data breach, loss, and exposure we have to Quarantine Sensitive Files, Behavior-

Based Permissions, Prepare for Cyber Threats, Delete Unused Data.

The analysis of the current state of data security in public institutions was done by analyzing the appropriate technical and organizational security measures according to Article 32 of the General Data Protection Regulation (GDPR). A total of 18 institutions were analyzed, which belong to different categories: government institutions, municipal institutions, public service institutions, public schools and public universities.

Table 1. Number of public institutions

institution	government institutions	municipal institutions	public service institutions	public schools	public universities
in total	2	5	2	3	6

Government institutions, municipal institutions, public service institutions, public schools and public universities have been analyzed by dealing with the assessment of risks during data processing, the documentation of the security program during the processing of personal data which specifies technical, administrative and physical protections, the process of solving the problem in the event of filing a complaint, determining an individual who is responsible for the prevention and investigation of security breaches, the use of encryption standards, personal information is systematically destroyed, deleted or anonymized when it is no longer legally required to be stored , the return of personal data in time in case of a physical or technical incident.

III. Analysis of data security and privacy in public institutions according to GDPR in the Republic of Kosovo

The strictest privacy and security law in the world is the General Data Protection Regulation (GDPR). Although it was created and approved by the European Union (EU), it imposes requirements on any organizations that target or gather information about individuals residing in the EU. An exhaustive list of legal terminology is defined in the General Data Protection Regulation 2016/679. Based on the General Data Protection Regulation (GDPR), 18 public institutions were analyzed. Table 2 presents the results generated after the analysis done for: the assessment of risks during data processing, the documentation of the security program during the processing of personal data which specifies the technical, administrative and physical protections, the process of solving the problem in in case of filing a complaint, determining an individual who is responsible for the prevention and investigation of security breaches, the use of encryption standards, personal information is systematically destroyed, deleted or anonymized when it is no longer legally required to be stored, the recovery of data personal in time in case of a physical or technical incident.

Table 2. Analysis of public institution based on the General Data Protection Regulation (GDPR)

	GI	**MI**	**PSI**	**PS**	**PU**
Have you assessed the risks involved in processing personal data and put measures in place to mitigate them	yes	no	no	no	yes
Is there a documented security program that specifies the technical, administrative, and physical safeguards for personal data?	yes	yes	no	no	no
Is there a documented process for resolving security-related complaints and issues?	no	no	no	no	no
Is there a designated individual who is responsible for preventing and investigating security breaches?	yes	yes	no	no	no
Are industry-standard encryption technologies employed for transferring, storing, and receiving individuals' sensitive personal information?	yes	no	no	no	no
Is personal information systematically destroyed, erased, or anonymized when it is no longer legally required to be retained?	yes	yes	no	no	no
Can access to personal data be restored in a timely manner in the event of a physical or technical incident?	no	no	no	no	no

The obtained results presented in table 2: government institutions (GI), municipal institutions (MI), public service institutions (PSI), public schools (PS) and public universities (PU) for each of these, the current conditions are initialized, where "YES" means that the institution is equipped with that request and "NO" means that the institution is not equipped with that request. The requests are according to the General Data Protection Regulation (GDPR) Article 32.

IV. Conclusion

Strategies for combating cybercrime, current policies and regulations of public institutions are outdated and do not meet the requirements of the General Data Protection Regulation (GDPR). And as such it results that:

- municipal institutions, public service institutions, public schools do not have risk assessors involved in the processing of personal data measures to mitigate the risks
- public service institutions, public schools and public universities do not have a security program documented that specifies the technical, administrative and physical safeguards for personal data
- government institutions, municipal institutions, public service institutions, public schools and public universities not have a documented process for resolving complaints and issues related to security?
- public service institutions, public schools and public universities do not have a designated individual responsible for the prevention and investigation of security breaches
- municipal institutions, public service institutions, public schools and public universities do not have an industry standard encryption technology for transfer, storing and receiving sensitive personal information of individuals
- public service institutions, public schools and public universities do not have any mechanism that systematically destroys, deletes or anonymizes personal information when it is no longer legally required to be stored
- government institutions, municipal institutions, public service institutions, public schools and public universities do not have techniques that can restore access to personal data at the right time in case of a physical or technical incident.

Public institutions must review the management documents of cybercrimes and adapt them according to the Regulation General Data Protection Regulation (GDPR).

REFERENCES

[1] Gerardus Blokdyk, *Sensitive Data A Complete Guide - 2019 Edition*, 5STARCooks (July 12, 2021), ISBN-10 : 0655817905, ISBN-13 : 978-0655817901

[2] Cobb, M. (2021, November). TechTarget Search Security. Retrieved from 7 best practices to ensure GDPR compliance: https://www.techtarget.com/searchsecurity/tip/7-best-practices-to-ensure-GDPR compliance?utm_source=google&int=off&pre=off&utm_medium=cpc&utm_term=GAW&utm_content=sy_lp09222022GOOGOTHR_GsidsSecurity_OneTrust_Essential_IO163813_LI2595380&utm_campaign=OneTr

[3] Elissa Mollakuqe, V. D.-M. (2022). Data Classification Based on Sensitivity in Public and Private Enterprises in the Republic of Kosovo. ICT Innovations 2022 (pp. 192-200). Skopje: Association for Information and Communication Technologies www.ict-act.org.

[4] Every one . (2021, 07). every one making wellbeing personal. Retrieved from GDPR Data Retention Policy: https://every-one.org.uk/wp-content/uploads/2021/07/EveryOne-GDPR-Data-Retention-Policy.pdf

[5] GDPR, G. D. (2022, 9 19). IT GOVERNANCE EUROPE. Retrieved from General Data Protection Regulation GDPR: https://www.itgovernance.eu/blog/en/the-gdpr-what-is-sensitive-personal-data ico. Information Commisioner's Office. (02.Aug.2018).

[6] Guide to the General Data Protection Regulation (GDPR). United Kingdom.

[7] Intersoft consulting. (n.d.). Intersoft consulting.eu. Retrieved from GDPRRight to be Informed: https://gdpr-info.eu/issues/right-to-be-informed/#:~:text=The%20data%20subject%20has%20a,in%20writing%20or%20electronic%20form.

[8] NetSec.news. (2018). NetSec.news. Retrieved from GDPR Data Retention: https://www.netsec.news/gdpr-data-retention/#:~:text=Generally%20speaking%2C%20GDPR%20data%20retention,or%20historical%20research%20for%20example.

[9] Organization, S. (2022, 09 10). SINA Organization. Retrieved from SINA Organization: https://www.snia.org/education/what-is-data-protection Privacy research team. (2022, September 2).

[10] Securiti.ai. Retrieved from GDPR Data Collection Requirements: https://securiti.ai/blog/gdpr-data-collection/#:~:text=Data%20Collection%20Requirements%20under%20GDPR,-You%20can%20store&text=The%20GDPR%20requires%20organizations%20to,one%20or%20more%20specific%20purposes.

[11] Serenhov, M. (2018). Forensic Breach Response in Compliance with GDPR. Sweden : Tryckeriet i E-huset, Lund. veratad. (2021, March 2). veratad.com. Retrieved from How to Verify Identity for GDPR Data Access Requests: https://veratad.com/verify-identity-gdpr-data-access-requests/#:~:text=For%20GDPR%20compliance%2C%20identity%20verification,check%20of%20the%20requester's%20identity.

[12] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage". In Proceedingsof the 13th Annual Network and Distributed SystemSecurity

[13] Symposium, San Diego, CA, Feb. 2006.

[14] D. Akhawe, P. Saxena, and D. Song, "Privilege separation in HTML5 applications". In Proceedings ofthe 21st Usenix Security Symposium, Bellevue, WA, Aug. 2012.

[15] J. Li, M. Krohn, D. Mazieres, and D. Shasha, "Secure untrusted data repository (SUNDR)". In Proceedings of the 6th Symposium on Operating Systems Design and Implementation (OSDI), pages 91–106, San Francisco, CA, Dec. 2004.

[16] A. J. Feldman, W. P. Zeller, M. S. Bajaj and R. Sion."TrustedDB: a trusted hardware based database with privacy and data confidentiality", In Proceedings of the 2011 ACM SIGMOD International Conference on Management of Data, pages 205– 216, Athens, Greece, June 2011.

[17] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage". In Proceedingsof the 13th Annual Network and Distributed System Security Symposium, San Diego, CA, Feb. 2006.