Manja Konkolič[1]

POSSIBLE SOLUTIONS REGARDING THE ACCESS AND MANAGEMENT OF DOCUMENTS CONTAINING CLASSIFIED DATA

Abstract:

Purpose: *In this paper, we will present the methods and forms of marking classified data, physical, organizational and technical measures, as well as mandatory components of procedures for the protection of classified data, which must be taken into account by those who work with such documentary material when establishing a system of measures and procedures for the protection of classified data. This is especially important for the organisations that deal with public security, defence, foreign affairs or intelligence and security activities of the state, because classified information is defined as a fact or means from their working area, which must be protected from uninvited persons for reasons specified in the law. The challenges of accessing archival material containing the aforementioned data are also presented.*

Method/approach: *We used a review of relevant literature and a comparative method to compare access to archival material containing classified information in three European countries.*

Limitations: *The research is limited to the area of access to and management of documents that contain the mark "confidential" in the Republic of Slovenia. For comparison, we limited ourselves to three European countries, namely: Hungary, Germany and the Czech Republic.*

Results: *It is believed that different countries treat access to archival material containing classified and sensitive information differently. We can also note that some countries restrict access to archival material containing the aforementioned data and condition access on the anonymization of personal and sensitive data.*

Findings/Applicability: *Some solutions are provided regarding access and handling of documents containing classified information.*

Keywords: *legislation, documentary material, documents, classified information, security.*

1 Manja Konkolič, Master in security, Faculty of criminal justice and security studies, University of Maribor, doctoral student of Archival sciences at Alma Mater Europaea, konkolic.manja@gmail.com

1 INTRODUCTION

Every democratic society relies on the rights of access to data and information of state bodies, because when it is lost, public trust and legitimacy are called into question. Nevertheless, each country must ensure a comprehensive national security, i.e. sovereignty in its territorial area, security of citizens, critical infrastructure, state institutions, etc. In doing so, the state also uses a system of classified data, because in this way it can ensure that the security of the previously mentioned elements is not jeopardized (Prezelj and Tarman, 2015). The Resolution on the National Security Strategy of the Republic of Slovenia (2019), which is a fundamental document in the field of national security, does not directly mention the tasks of the classified data protection system, but emphasizes the importance of classified data in the field of national security.

Žirovnik, (2005, 1) emphasizes that certain information and data must be subject to a certain legal regime, since there are legitimate interests and benefits to limiting their general accessibility and usefulness. Prezelj and Tarman (2015, 688-689) point out that the principle of public work and accessibility to data and information of state bodies and holders of public authority cannot apply absolutely and without limits. In this regard, the most important question is in which cases, in what manner and under what conditions it is permissible to withhold certain data and information from the public. Certain data and information, created or existing in state bodies must be marked as classified in order to protect certain state interests and benefits, thereby significantly limiting their accessibility. To protect secrecy, the state must establish instruments that protect the state's privacy from the public and actual or potential adversaries. When the state is allowed to protect secrecy, it is also necessary to ensure sufficiently strong levers that make it impossible and difficult to abuse this institution.

The operationalization of the protection of state secrets is carried out with a comprehensive system of marking, protection, access and control over classified data (Brezovšek and Črnčec, 2004).

2 SECRECY AND CLASSIFIED INFORMATION

Brezovšek and Črnčec (2004) believe that secrecy is not something unknown, but quite the opposite. Its contents are known things that its "owner" (individual, institution or state) cannot or does not want to make available to the general public. Secrecy therefore means the existence of known facts about social, security, defence, economic and other data and information entrusted to an individual or institution for use and protection. Trbovšek (2004) adds that due to the existence of different, often conflicting interests, institutions hide them from the public consciously, in an organized and formalized fashion.

Anžič (1997, 156) believes that the word secrecy (slo. tajnost) is taken from other Slavic languages. Considering that the use of the term secrecy in Slovenian regulations increased under the influence of the Yugoslav legislation, where the term "secret" was used, the concept of secrecy is often equated with the concept of secret in the Slovenian state. Dictionary of Slovenian Literary Language (SSKJ) also separates the two terms, but in the part where it is essential for the work of the state administration, it allows equal use of both and does not give preference to one or the other.

Brezovšek and Črnčec (2007, 96) do not agree with the statement, but partially reject it and believe that "SSKJ clearly defines secret as a synonym of secrecy. In its second meaning, mystery is synonymous with secrecy. It is a secret: what one knows, what is entrusted to him and must not be told to others. Business, official, and military secret is illustrated as an example" (Brezovšek and Črnčec 2007, 95). Anžič (1997) believes that

it is important not to equate secrecy in the sense of protecting what is known and inaccessible to the general public with the concept of mystery, which is something incomprehensible, inexplicable, never discovered and represents a mystery. There is a danger that the principle of privacy for the state would prevail over the principles of legality and constitutionality, therefore "a state governed by the rule of law must carefully protect the concept of secrecy, even under criminal law, and rarely use it, and even then, according to predetermined legal conditions and frameworks." From another point of view, secrecy can be a good, if those who should protect it and prevent the outflow of information and data that can endanger the interests of individuals, institutions, and the state (Anžič 2000, 854).

The main purpose of classified information is to protect the vital interests of the country. The disclosure of this would endanger and harm the interest of the country and its national security and may even threaten its existence. A complete system for handling classified information must be established. In addition to the technical, physical, and organizational measures established for the implementation of the protection of classified data, special attention must be paid to the rules of access to classified data (Brezovšek and Črnčec, 2004).

In the Classified Information Act (ZTP, 2006, 2020), classified information is a fact or means from the sphere of activity of an agency relating to public security, defence, foreign affairs or the intelligence and security activities of the state which, for reasons defined in this Act, must be protected against unauthorised persons and which has been defined and marked as confidential in accordance with this Act. This Act represents the uniform security minimum according to which certain data, important for the security and interests of the country, must be treated. It is also a prerequisite for the establishment of a national system for the protection of classified data.

3 CLASSIFIED INFORMATION IN DOCUMENTARY MATERIAL

Confidential and classified information appears in written sources and oral communication. From the archival point of view, a written source that preserves cultural value over a longer period of time is all the more important. The importance of confidential data in documentary and archival material indicates that all things, events, and contents are not freely accessible to various interested groups or individuals, but the principle applies that authorized individuals may be informed of important information and data, when those are marked as such. This is the essence of confidentiality protection (Lavrič, 2008).

The information is determined to be confidential under the conditions and in the manner specified by the Classified Information Act (ZTP, 2006, 2020), by an authorized person. Every classified information or every document containing classified information must be marked with the level of confidentiality and information about the authority, if this is not already clear. Only those persons who have permission and need to become familiar with this information in order to perform their function or work tasks have the right to access classified data. The Classified Information Act (ZTP, 2006, 2020) also stipulates that no one may obtain classified information earlier and to a greater extent than is necessary for the performance of his job duties or function.

In order to ensure the legal and safe handling of classified data, the Confidential Data Act (ZTP, 2006, 2020) stipulates that all authorities and organizations must establish a system of procedures and measures for the protection of classified data that corresponds to a certain level of secrecy and prevents their disclosure to unauthorized persons. The protection of classified data includes:

- procedures and measures related to persons who have access to classified information,
- familiarizing users with the measures and procedures for safeguarding classified data,
- the method of marking the levels of secrecy and the protection of documents and media containing classified information,
- physical, organizational, and technical measures for the protection of premises in which classified data is handled as well as equipment used to handle classified data,
- procedures and measures for secure transmission, reproduction, storage, and destruction of classified data,
- protection of the communication and information infrastructure, which is used to manage classified data,
- control and recording of accesses to classified data and transmission of this data,
- procedures and measures in case of security incidents and other forms of endangering the confidentiality, integrity, and availability of classified data, and
- control over handling and protection of confidential data.

4 MANAGEMENT OF DOCUMENTARY MATERIAL CONTAINING CLASSIFIED INFORMATION

When managing documentary material, it is important that procedures are carried out in a timely and correct manner. Work processes must be described in an internal act (e.g. in the instructions on the management of documentary material).

Žumer (2008, 26, 129-130) states that the management of documentary material includes the following management procedures: organization and implementation of procedures for receiving electronic and classic mail, opening mail, checking the validity of electronic signatures, receiving stamp impressions, sorting and classifying materials by function, determining the number of documents, signing and assigning material for resolution, recording documents, cases and files, resolving cases, keeping a diary, sending mail and storing documentary material in business and at work for both natural and legal persons. In the Republic of Slovenia, this is governed by regulations harmonized with international ISO standards, resolutions of the Council of Europe, recommendations of the European Commission and modern requirements of information science. All regulations are harmonized with each other.

4.1 DOCUMENTATION SECURITY

Documentation security defines a unified system of determining and marking classified information, transferring, duplicating, recording, destroying, and archiving, as well as the procedure in case of misuse of classified information. The legal basis that is taken into account here are the regulations in the field of classified data and the regulations dealing with handling of documentary and archival material in general. Organizational measures for dealing with classified data are interwoven with physical and technical measures for the protection of classified data, and together they form a comprehensive system of protecting classified data, the aim of which is to prevent access by unauthorized persons and to have the traceability of data throughout their lifetime.

State authorities are responsible for data security. Sources of threats to classified information are an integral part of the broad spectrum of threats to any country. In modern society, they are completely different than they were in the past (Office of the Government of the Republic of Slovenia for the Protection of Classified Data).

4.2 DETERMINING THE LEVER OF SECRECY

The authorized person determines the level of secrecy of the information:

- when data is created,
- at the beginning of the task that will result in classified information,
- if with merger of non-classified data information is produced that needs to be protected.

The minimum level of secrecy is determined, which still ensures the protection of data necessary for the protection of interests or the security of the state.

A document consisting of data with different secrecy levels shall be assigned at least the same level of secrecy and durability validity as the data with the highest level or the longest period of secrecy.

The amendment of ZVDAGA-A from 2014 brought changes to Articles 65 and 66, which regulate the legal basis of access to archival material containing secret information according to the Secret Information Act, tax secrets and personal data. The term "data relating to state and public security, defence, foreign affairs or the intelligence and security activities of the state or its economic interests" from Article 65 is replaced by the term "classified data according to the Act on Classified Data", as the content covers, but at the same time they do not allow any other information that is not formally secret to be declared inaccessible. Archival material that contains classified information according to the applicable Secret Information Act or tax secrets and the disclosure of which to an uninvited person could cause harmful consequences for the security of the state and other persons or for their legal interests becomes accessible, as a rule, 40 years after its creation, if with designated as inaccessible by the sender.

The regime of exceptional access to public archival material in public archives at a time when it is not yet accessible to the public is defined. The Government of the Republic of Slovenia may, on the basis of the opinion of the archive commission and upon fulfillment of legal conditions, grant a scientific research organization, researcher or journalist exceptional access to material containing classified information or tax secrets, if the use of such material is unavoidably necessary to achieve a scientific goal and public the interest in disclosure outweighs the public interest in keeping that information unavailable. Also, the archive commission can grant exceptional access to archive material containing personal data to the specified users, if they meet the prescribed conditions. In the event that archival material contains such secret data, data on tax secrecy and personal data, the government decides on exceptional access based on the opinion of the archive commission (Kremenšek, 2014).

Lavrič (2008) points out that the fundamental principle of protecting confidential data is precisely ensuring their inaccessibility to persons who are not entitled or authorized to access them. Klasinc (2016) adds that the Act on the Protection of Personal Data and the Act on Secret Data (both often with different names) are important for research into projections of access to archival material, because they began to have a strong influence on the operation of archives, and above all on the procedures for use of archival material. This is also reflected in national archival laws, such as the Slovenian Act on the Protection of Archival and Documentary Materials and Archives (ZVDAGA, 2006, 2014).

MARK	CRITERIUM – Possible adverse consequences
TOP SECRET (ST)	Disclosure would threaten vital interests of RS
SECRET (T)	Disclosure could seriously harm the security and interests of RS
CONFIDENTIAL (Z)	Disclosure could harm security and interests of RS
INTERNAL (I)	Disclosure could harm operations of the body

Table 1: Possible consequences of disclosure of classified information; Source: Office of the Government of the Republic of Slovenia for the Protection of Confidential Data

A change or revocation of secrecy can be made by an authorized person when conditions for secrecy no longer need to be met. This must be done in writing and an assessment of possible adverse consequences must be attached. Consequently, the original classification markings are crossed out, a new marking of the classification level or revocation is indicated below or above the old marking, and a reference to the written explanation of the revocation or changes in classification is given. Everyone who has accepted or has access to classified information is also notified in writing.

Classified information can end on a certain date, with the occurrence of a certain event, with the passage of a certain time, with the revocation of secrecy, with the passage of time determined by the law governing archival material.

Classified data is reviewed by an authorized person who assesses the need for its confidentiality, namely:

- TOP SECRET – once a year,
- SECRET, CONFIDENTIAL, INTERNAL – every 3 years.

If the conditions for the protection of classified data in the system for recording classified data are not met, the content of classified data cannot be discerned from individual entries, and documents marked with a level of secrecy are not scanned into the system for recording classified data. The authority also keeps a list of views for classified information for SECRET and TOP SECRET groups, which contains the document number, date, classification level and number of the copy or copy of the document containing the classified information, the name and surname of the person who became familiar with the classified information, date and time of familiarization, signature of the person who became familiar with the classified information.

The distribution may only be administered to persons who have the appropriate permission to access classified information and who must become familiar with the classified information in order to perform a function or work task. If it is not possible to determine the recipient of the classified information from the address, the distribution is ordered by the head of the authority or organization, a person who has written authorization or the head of an organizational unit, for his work area. The distribution list can be created for individual documents or for documents that belong to a common content area and contains at least the designation of the authority/organization/organizational unit, content area or document number and recipients of classified information.

Documents containing classified information are transferred/sent in a double envelope, the inner envelope contains the classification code, the document number, addressee and sender information, and other important markings; outer envelope is made of solid, opaque, impermeable material, without classification markings; the outer envelope may be replaced by a locked or sealed case, box or bag - when transferring outside the security area.

When the classification level is marked as INTERNAL – the transfer is made by:

- the courier service,
- via own transfer network,
- by registered mail with return receipt.

When the classification level is marked as CONFIDENTIAL or higher – the transfer is made by:

- via own transfer network,
- the courier service.

4. 3 STORAGE AND MAKING OF DOCUMENTS

According to Article 39 of the Classified Data Act (ZTP, 2006, 2020), classified data must be stored by the authorities in a way that ensures that only persons who have permission to access classified data and who need the data to conduct their work tasks or functions, have access to this data.

According to the Regulation on the Protection of Classified Information, documents with confidential information must be marked in a visible place with the type of secrecy and the level of confidentiality. All document attachments must also have the same designation. When creating a document that contains information that is "state secret" or "official secret", or marked as "strictly confidential", the number of copies in which it was made (written, printed, drawn, reproduced) and to whom it was given/sent is indicated on the original. Each copy of such a document must have its own registration number.

Documents marked "state secret" and "official secret - strictly confidential" are kept in locked security cabinets that are technically protected or in locked safe deposit boxes unless they are under the direct control of the employee to whom such material was assigned. Documents classified with a lower level of secrecy are kept in locked security cabinets.

Classified INTERNAL information can be managed in the administrative area. Classified information marked as CONFIDENTIAL or higher can only be managed and stored in a designated, visibly designated area, which, depending on the way the classified information is handled, is classified in security area of 1st or 2nd degree (Level I or Level II).

A level I security area is a marked area in which classified information of the CONFIDENTIAL or higher level of secrecy can be managed, so that the very entry into the security area allows access to this information. Level II security area is a marked area in which classified information of the CONFIDENTIAL level or higher levels is treated in such a way that the mere entry and movement in this area does not yet allow access to this data.

Around Security levels I and II or on the route leading to such a security area, an administrative area is established, which can include all the business premises of the authority. Such an area requires a visibly defined space in which the authority can control the entry or movement of persons and vehicles. In administrative areas only data, classified with INTERNAL level may be stored and processed, and security procedures and measures must ensure that only persons who have confirmed in writing that they are familiar with the regulations governing the handling of classified data have access to this data. These persons must familiarize themselves with this information in order to perform work tasks.

To enter a level I security zone, a person is issued a special permit by the head of the body or organization in which the security zone is located. The special permit can also be issued by a person authorized in writing by the head of the body or organization.

The entry and exit of persons into security areas and the access of vehicles must be controlled. All entries and exits must be recorded.

After the creation of a confidential document marked "state secret" or "official secret" - "strictly confidential", all auxiliary materials that were created during the creation document (e.g., matrices, calculations and charts, sketches, test, or failed printouts, etc.) must be destroyed through a special procedure with appointed committee.

Documents containing classified information are archived in accordance with the regulations governing archival activity. Archivists who work with documents containing confidential and secret information know and apply the relevant articles of the Classified Information Act, and Protection of personal data Act, and ensure that there is no abuse when using archival material. Each archive usually formulates its own work regulations, which the archivist must know well, and which usually specifically define the handling of archival material stored by a particular archive.

The Regulation on administrative operations distinguishes between three collections of documentary material: Collection of unresolved cases, in which the cases are kept until their solutions. They are usually kept in the departments where the cases are resolved. They can also be kept in the main office but separately from the current and permanent collection of documentary material.

The current collection of documentary material (Archive at hand) is a space in which resolved cases and documents for the current year and two more years after the final resolution are kept. Organizations usually keep it in their head office or business premises. They can have several Archives at hand.

The fourth point of Article 183 of the Regulation on Administrative Operations (2005) emphasizes that the employee who resolves the case must, before filing it in the current collection of documentary material, eliminate unnecessary materials such as copies, duplicates, auxiliary forms, blank forms, etc. Draft documents are not allowed to be excluded, as they reflect the way in which the final documents in the case were created. Electronic material is stored as a current collection in a computer information system with hardware and software.

The permanent collection of documentary material (archive) is a collection of finally resolved cases and closed records, as well as material that the organization must keep in accordance with regulations or business needs for more than two years. According to regulations and standards, the permanent collection or archive of an organization is the space, equipped with computer information system, in which documentary material is kept together with records, which the organization must keep for more than two years. Documentary material is kept in the permanent collection until the expiration of the storage period, when the material can be removed and destroyed, or until the material is opened and handed over to the competent archive (Žumer, 2008, 210).

Regulations on the protection of data secrecy, privacy protection and personal data protection, meaning that documents contain secret, protected, and personal data, must be:

- marked accordingly,
- stored separately from the rest of the documents,
- specially protected (ZAL, 2022).

5 ACCESS TO CLASSIFIED INFORMATION

One of the key criteria for accessing classified data is the need to know that an individual or organization has, to perform their tasks. Another criterion for accessing confidential data is the security clearance of individuals.

This is about determining the will to keep classified data and related risks.

In Slovenia, all persons who have access to confidential data for the purpose of performing tasks or functions at their workplace must be properly screened (with the exception of some statutory exceptions and for the "internal" level, where basic training and signing of a declaration on the protection of confidential data is sufficient) (Secret Information Act, 2006). This means that in the security screening process, a person's loyalty, reliability, and credibility are checked, with the aim of granting or withholding permission to access classified information. The security screening process deals with aspects of personal character and circumstances that could lead to the emergence of potential security problems. The above criteria for accessing classified information also have an exception. According to the Confidential Information Act (ZTP, 2006: Article 3), precisely defined categories of persons can access secret data without an access permit: the President of the Republic, Prime Minister, Member of Parliament, State Councillor, Mayor and Municipal Councillor, Minister and Head of Government Service, who is directly responsible to the prime minister, ombudsman and his deputy, governor, deputy and vice governor of the central bank, member of the court of audit, judge, president and member of the state audit commission, state prosecutor, state attorney general and information officer (Prezelj and Tarman, 2015, 695-696).

Access to classified data is enabled with the cumulative fulfilment of at least two conditions. These conditions are permission to access classified data and compliance with the *need to know* principle. The key factor in protecting confidential data is the human (Brezovšek and Črnčec, 2004).

The amendment of ZVDAGA-A from 2014 brought changes to Articles 65 and 66, which regulate the legal basis of access to archival material containing classified information according to the Classified Information Act, tax secrets and personal data. The term "data relating to state and public security, defence, foreign affairs or the intelligence and security activities of the state or its economic interests" from Article 65 is replaced by the term "classified data according to the Act on Classified Data", as the content suggests, but at the same time they do not allow any other information that is not formally classified to be declared inaccessible. Archival material that contains classified information according to the applicable Classified Information Act or tax secrets and the disclosure of which to an uninvited person could cause harmful consequences for the security of the state and other persons or for their legal interests, becomes accessible as a rule, 40 years after its creation, if designated as inaccessible by the sender.

The regime of exceptional access to public archival material in public archives at a time when it is not yet accessible to the public is defined. The Government of the Republic of Slovenia may, on the basis of the opinion of the archive commission and upon fulfilment of legal conditions, grant exceptional access to material containing classified information or tax secrets to a scientific research organization, researcher or journalist, if the use of such material is unavoidably necessary to achieve a scientific goal and if the public interest in disclosure outweighs the public interest in keeping that information unavailable. Also, the archive commission can grant exceptional access to archival material containing personal data to the specified users, if they meet the prescribed conditions. In the event that archival material contains such secret data, data on tax secrecy and personal data, the government decides on exceptional access based on the opinion of the archive commission (Kremenšek, 2014; Hajtnik, 2022).

Lavrič (2008) points out that the fundamental principle of protecting confidential data is precisely ensuring their inaccessibility to persons who are not entitled or authorized to access them. Klasinc (2016) adds that the Act on the Protection of Personal Data and the Act on Confidential Data (both often with different names) are important for research

into projections of access to archival material, because they began to have a strong influence on the operations of archives, and above all on the procedures for use of archival material. This is also reflected in national archival laws, such as the Slovenian Act on the Protection of Archival and Documentary Materials and Archives (ZVDAGA, 2006, 2014).

The user using archive material must sign a statement before using this archive material that:

- he is aware of his obligations and restrictions regarding the use of data from Article 65 of this Act, which he would be made aware of in case of access to archival material based on Articles 66 and 68 of this Act,
- is aware of his obligations and restrictions regarding the use of data from Article 65 of this Act, which he might encounter when using archival material that has not otherwise been marked as inaccessible by the sender, or that contains personal data,
- will protect the data obtained in this way in accordance with this Act and legislation in the field of personal data protection, protection of confidential data, tax and professional secrets, and
- that he is aware that the misuse of the specified data is sanctioned in the Criminal Code and other regulations and that he assumes all material responsibility for the misuse of the specified data.

Levels of secrecy TP	Handling TP	Staff	Safekeeping TP	Transferring TP
TOP SECRET	Security Level I or II	Permission to access classified information of the level TOP SECRET	Safe with at least anti-burglary level III.	Own transmission network
SECRET	Administrative area, Security Level I or II	Permission to access classified information of the level SECRET	Safe with at least anti-burglary level II.	Own transmission network
CONFIDENTIAL	Administrative area, Security Level I or II	Permission to access classified information of the level CONFIDENTIAL	Safe with at least anti-burglary level II.	Own transmission network
INTERNAL	Administrative area	Basic training and signed declaration of familiarity with regulations.	Office cabinet or metal cabinet.	Minimum: recommended with return receipt.

Table2: Handling, access, storage and transmission of documents containing classified information by classification level; (Source: Office of the Government of the Republic of Slovenia for the Protection of Classified Data).

5. 1 COMPARISON OF SOME CRITERIA FOR THE PRESERVATION AND MANAGEMENT OF THE MATERIAL OF THE FORMER INTELLIGENCE AND SECURITY SERVICES IN THE EU

Country	Storage	Legal basis	Access to archival material
Federal Republic of Germany	Yes / 1990 / Office of the Federal authorized representative for the archival services, national security in the former GDR	Law/ 1991/2012	Monitored persons: restriction of access to sensitive personal data of "third" persons (anonymization) researchers: restriction of access to sensitive personal data (anonymization), but at the same time exceptional access without anonymization is also regulated (e.g. researchers, employees of the Office; after the last amendment of the law access to non-anonymized material is also provided to "external" academic researchers); otherwise, the term of inaccessibility of the said data is 30 years after the death of the individual.
Czech Republic	Yes / 2008 / Institute for studying totalitarian regimes and Archive security	Law / 2007	Availability of all material to all users without anonymization.
Hungary	Yes / 1997 / 2003 / Historical archive Hungarian National security	Law / 1997 / 2003	Accompanied persons: limited access to personal data of "third" persons (anonymization) researchers (need special license researcher): limited access to sensitive personal data (race, nationality, religion...) according to the formula 30-90-60. Early access to this data is possible with special permits competent authority. Especially sensitive personal data (health status, addictions, sex life) victims of the regime are inaccessible until the period of inaccessibility expires after formulas 30-90-60). Access to other sensitive personal data (race, nationality, religion) possible before expiration deadline 30-90-60 in case of special approvals. The researchers sign the statement on data protection.

Table 3: Comparison of some criteria for the preservation and management of the material of the former intelligence and security services in the EU (Source: Ministry of Culture, 2013)

6 LEVELS OF CLASSIFIED INFORMATION IN THE EUROPEAN UNION

The Council Decision on security regulations for the protection of classified EU data sets out the basic principles and minimum security standards for the protection of EU classified data. These principles and standards apply to the Council and its General Secretariat and must also be respected by Member States in their work with EU classified information.

There are four levels of classified data in the EU: EU Top Secret, EU Secret, EU Classified, EU Restricted.

Très Secret UE /EU Top Secret: information and material the unauthorised disclosure of which could cause exceptionally grave prejudice to the essential interests of the European Union or of one or more of the Member States.

Secret UE /EU Secret: information and material the unauthorised disclosure of which could seriously harm the essential interests of the European Union or of one or more of the Member States.

Confidentiel UE /EU Classified: information and material the unauthorised disclosure of which could harm the essential interests of the European Union or of one or more of the Member States

Restreint UE /EU Restricted: information and material, the unauthorized disclosure of which could be disadvantageous to the interests of the European Union or one or more member states.

The Organization for Joint Armament Cooperation, a European defence organization, has three levels of classification: OCCAR Secret, OCCAR Classified and OCCAR Restricted.

ECIPS, the European Centre for Information Policy and Security, has four levels of security information, COSMIC (Top Secret), EC-Secret, EC-Classified and EC-Committees (Decision on Security Rules for the Protection of Classified Information in the EU, 2013).

The Council Decision on security regulations regulates several ways to protect this data, including personal security, physical security, data handling, information security, industrial security or the ways in which classified EU data is exchanged between EU institutions or between the EU and third countries and international organizations.

The Slovenian regulation differs from the EU regulation, which effectively exempts classified data of the three highest levels of confidentiality from the general legal regime of access and stipulates that they can only be disclosed with the consent of the author (Prepeluh Magajne, 2011).

7 ARCHIVING CLASSIFIED INFORMATION

The Regulation on the Protection of Classified Data states that classified data shall be kept in accordance with the deadlines set by the regulations governing the handling of documentary and archival material. After the retention period has expired, they are removed and destroyed, unless they are designated as archival material in accordance with the regulations governing the handling of documentary and archival material. When handing over archival material with classified information to the competent archive, the regulations governing the field of archival activity are taken into account.

The Act on the Protection of Documentary and Archive Material (ZVDAGA, 2006, 2014) specifies that public legal entities must hand over public archival material to the archive no later than 30 years after the creation of the material, including material:

- which contains confidential information in accordance with the law,
- which is specially protected as confidential, if the law or the rules of procedure of a state body or a body of a self-governing local community stipulate it.

On the basis of Article 40 of the ZVDAGA (2006, 2014), archival material can also be taken over later for professional reasons, e.g., if the public legal entity still needs the material for operational activities.

Until the public archival material is handed over to the competent archive, the regulations governing access to public information, protection of confidential data, protection of personal data, business and tax secrets and other regulations shall apply with regard to access and use of archival material, regardless of the time of creation of the material, except for archival material of public legal entities, which, in accordance with Article 62 of this Act, ensure their own protection of archival material.

7. 1 CODE OF ETHICS

The Archives Code (ICA, 1996), which was adopted at the 13th International Archives Congress in Beijing in 1996, states that archivists must respect the accessibility and confidentiality of information and operate within the limits of the relevant legislation.

They need to ensure that corporate and personal privacy and national security are protected without data destruction, especially with computer records where addition and deletion of data is widespread practice. They must respect the privacy of the individuals

who created the material or are the subject of that material, especially those who cannot decide on its use or destruction.

They must justify the trust placed upon them for the common good and avoid using their position to take unfair advantage of themselves or others.

They must refrain from actions that would harm their professional integrity, objectivity, and impartiality. They must not take personal advantage, either financial or otherwise, to the detriment of institutions, users, and colleagues. Archivists may not collect original documents or engage in trading with them for their own benefit. They must avoid activities that would create the appearance of conflicting interests in public opinion. Archivists may use their institution's material for personal research and publication, provided they do so under the same conditions as other users of the same material. They may not disclose or use information obtained in their work with material whose accessibility is restricted. Their private interest in research and publication must not interfere with the performance of their professional or administrative duties, which are their work obligations. When archivists use their institution's materials, they must not use their knowledge of unpublished researchers' findings without first informing them of their intention. They may write reviews and commentaries on the work of others in their fields, including works based on material from their institutions. Archivists must not allow archivists to interfere with their work and responsibilities.

7. 2 PROVISIONS

The ten stipulations or principles written in the archival professional code cover all relationships that arise in all phases of handling archival material. In them, we find all the principles of archival professional conduct in their most general form, and they can therefore also be considered the ten archival stipulations. We highlight those, relating to classified information.

The third provision requires that archival material must not lose its authenticity during professional processing, use and storage (protection). In the explanation of the provision, it is said that even conservation and restoration interventions must not harm the authenticity of the material. If, for example, the authenticity of the material is not guaranteed due to the confidentiality of the data, the archives must inform the users who study the archival material or the archive fund that has been reduced in this way. If the authenticity of the material is temporarily compromised due to secrecy, it is necessary to inform the users when such a situation will change.

The seventh provision refers to the protection of confidential and personal data, within the framework of the relevant legislation. In archives, it is necessary to protect all forms of privacy and state secrets found in the content of the archival material they store. They must take special care to protect the privacy of persons who cannot decide on the use or destruction of documents containing their privacy. In order to protect such data, archive material must not be destroyed. The interpretation of the provision particularly points to the danger of destroying electronically (computerized) recorded data, as it is quite easy to destroy them.

Those, responsible for declassification, such as employees of the creator of the material whose material is to be reviewed for declassification, must ensure a professional and timely review of the material for declassification.

General restrictions apply to all archival material and, depending on the institution's field of activity, include the protection of personal data and privacy, security, data protection on investigative procedures or law enforcement, trade secrets and national security. However, the scope and duration of the general restrictions must be clear.

7. 3 DESTRUCTION OF DOCUMENTARY MATERIAL

The destruction of unnecessary documentary material is a prescribed procedure for the elimination or destruction of documentary material that has passed the prescribed retention periods, is no longer relevant to the institution's operations or is not designated as archival material. Unnecessary documentary material is submitted to the commission for direct raw material commission processing with a record of destruction. The institution itself is fully responsible for the destruction of documentary material. The record of destruction, in which the material is only tentatively listed, is kept permanently. The regulation on administrative operations stipulates that the material for which a record of elimination was drawn up must be destroyed within 15 days and that such destruction must ensure the unreadability of any secret or personal data, for which the said commission records the destruction of the documentary material in writing. The procedure for destroying documents labelled "official secret" - "confidential" and "official secret" - "internal" is determined by the superior.

Documents containing TOP SECRET classified information may only be destroyed in the EU central register. These documents can only be destroyed by record, in accordance with the "three person" rule. Certificates of destruction and documentation of distribution are kept in the EU register for at least ten years from the date of destruction.

Documents containing classified information classified as SECRET are destroyed by the competent EU registries. Certificates of destruction and documentation of distribution shall be kept in the EU register for at least three years from the date of destruction. Documents containing classified information classified as CONFIDENTIAL are destroyed by competent EU registries. Certificates of destruction and documentation of distribution are kept in the EU register in accordance with Slovenian regulations in the field of secret data. Documents containing classified information of the INTERNAL classification level are destroyed by the competent EU registries or the user if this is permitted by Slovenian regulations in the field of classified data (Office of the Government of the Republic of Slovenia for the Protection of Classified Data).

It is worth reminding that the 3rd indent of Article 259 of the Criminal Code (KZ-1, 2012) states that anyone who illegally alienates, destroys, or conceals archival material, or renders it unusable, shall be punished with imprisonment from three months to three years.

In relation to the release of classified information, Article 260 of the Criminal Code (KZ-1, 2012) states that an official or other person who, contrary to their duties to protect classified information, communicates or hands over classified information to someone or otherwise enables them to them, or collects such information in order to hand it over to an uninvited person, shall be punished by imprisonment for up to three years.

Anyone who unlawfully obtains confidential information in order to use it unjustifiably, as well as anyone who publishes such information publicly without permission, shall be punished in the same way.

A person who fulfils the signs of a criminal act from the first paragraph of this article shall not be punished if it is secret information that reveals an illegal interference with human rights or fundamental freedoms, other constitutional or legal rights, serious abuse of power or authority, or other serious irregularities in the exercise of authority, public powers or the performance of a public service, and the act is not done out of self-interest and does not threaten people's lives or have serious or irreparable harmful consequences for the security or legally protected interests of the Republic of Slovenia.

Regardless of the provision of the second paragraph of this article, whoever publicly publishes, acquires, transmits, or possesses classified information with the intention of disclosing it to the public is not punished, if, depending on the circumstances of the case, the public interest after the disclosure of the classified information prevails over the public interest after maintaining its secrecy, and if the action does not directly endanger the life of one or more persons.

If the act referred to in the first paragraph of this article was implemented out of self-interest, or if the publication directly endangered people's lives, or if the publication had serious or irreparable adverse consequences for the security or legally protected interests of the Republic of Slovenia, the perpetrator shall be punished with imprisonment of up to eight years.

If the act referred to in the first paragraph of this article is committed due to negligence, the perpetrator shall be punished with imprisonment of up to one year.

8 CONCLUSION

In order to protect certain data and information, it is necessary to limit their general availability and usability. In other words: classified information is defined by all regulations as an exception to free access to information of a public nature, as it is necessary to ensure the public security of the country and thus the entire nation. Based on this, the state is determined to protect certain information and data with classified information. The method and extent of protection is defined in more detail in the Classified Information Act (ZTP, 2006, 2020) (*lex specialis*) and in some by-laws. In accordance with the Classified Information Act (ZTP, 2006, 2020), certain information can be classified as secret if it cumulatively meets the material and formal conditions.

The material condition dictates that information can be classified as secret only if it is so important that its disclosure would cause, or could clearly cause, harmful consequences for the security of the country or for its political or economic benefits, and at the same time, in terms of its content, to public safety, defence, foreign affairs or intelligence and security activities of state bodies of the Republic of Slovenia, or refers to systems, devices, projects and plans or scientific, research, technological, economic and financial matters that are important for the aforementioned goals. One can deduct from this definition that the disclosure must (at least potentially) cause a certain type of damage and that certain fundamental interests of the state or society as a whole must be threatened. The formal criterion further dictates that the information must be designated as secret by an authorized person, in the manner of and according to the procedure specified in the ZTP (2006, 2020), and in doing so, the level of its secrecy (top secret, secret, confidential or internal) must be appropriately marked in relation to possible harmful consequences, which would arise from its disclosure. While formal criteria do not cause problems in practice, more attention is paid to material criteria. The terms "public security", "defence", "foreign affairs" and "intelligence-security activity" are indeed very flexible and are therefore often used (or misused) by authorities to arbitrarily conceal information that is not in the interest of certain layers of power. The information must not be designated as secret in order to conceal a committed crime, abuse or misuse of authority or any other illegal act or conduct (Prepeluh Magajne, 2011).

Classified documents must become available to the public when the data protection expires in accordance with the original determination of their classified state; when the data in them no longer meet the legal conditions for the determination of being "clas-

sified" and are declassified by the authorities themselves; with the expiration of the time specified for archival material and archives; or when a certain level of "classified" is withdrawn at the request of an individual because the information in the document was defined as classified in violation of the law.

Nowhere, however, is it possible to completely protect classified information. Therefore, for the sake of clarity and transparency, it is necessary to approach this comprehensively and systematically.

The first condition can be defined as the human factor. All persons who have access to confidential data for the purpose of performing tasks or functions at their workplace must be properly screened. This means that the person's loyalty, reliability, and credibility are checked during the security check process, with the aim of issuing or withholding permission to access classified information. Such screening process deals with aspects that concern personal character and circumstances that could lead to the emergence of potential security problems. A person is therefore expected to have an elevated level of integrity and a moral-ethical stance. It is also necessary to be aware of criminal liability, as the release of classified information is punishable by a prison sentence of up to three years.

The second condition is that the instructions and regulations governing documentation operations with confidential data, including classified documents, are strictly followed.

In this way, the confidentiality issue will also be raised and the system of protecting classified data will be consistently implemented, as well as the belief of the leakage of secret data to the public.

Given that with the development of information technologies and the related development of information processing, which can be easily intercepted and changed, digital records of data need to be protected only when they are processed and transmitted through communication and information systems. For this purpose, new technical and security requirements for cryptographic solutions have also appeared. They need to be developed and implemented, but they must be in accordance with European directives.

Novak (2019) writes that in the context of archival theory and practice, archival experts have developed several methods and procedures for data management over time. Their solutions are mainly based on practical experience of manually managing quantities of preserved archival material or related records about it. It also notes that formalized and established procedures are a prerequisite for data management in archives.

In relation to access to archival material containing classified information, an amendment to the Act on Amendments to the Act on the Protection of Documentary and Archival Material and Archives was adopted in 2014. It brought some innovations in relation to the concept of confidential data, namely that data relating to state and public security, defence, foreign affairs or intelligence security activities of the state or its economic interests" from Article 65 of ZVDAGA (2006, 2014) are replaced by the term " confidential data according to the Confidential Data Act", as they are covered in terms of content, but at the same time they do not allow any other data that is not formally confidential to be declared inaccessible. Archival material that contains confidential data, business or tax secrets becomes accessible 40 years after its creation, while public archival material with sensitive personal data becomes generally accessible 75 years after its creation, or 10 years after the death of the person to whom it relates. Exceptionally, the Government of the Republic of Slovenia may, based on the opinion

of the archives commission and upon fulfilment of legal conditions, grant exceptional access to a scientific research organization, researcher or journalist to material containing classified information or tax secrets, if the use of such material is unavoidably necessary to achieve the scientific goal and the public interest in disclosure prevails over the public interest in the inaccessibility of this data. Also, the archive commission can grant exceptional access to archival material containing personal data to the specified users, if they meet the prescribed conditions. In the event that archival material contains such secret data, data on tax secrecy and personal data on exceptional access, the government decides on the basis of the opinion of the archives commission.

Novak (2016) warns that Article 65 of the ZVDAGA (2006, 2014) regulates the deadlines for the inaccessibility of archival material, namely for public archival material in public archives that contains classified information or tax secrets or personal data, as well as for archival material in public archives that was created before the constitution of the Parliament of the Republic of Slovenia, before May 17, 1990. Modern requirements for managing sensitive data in archives, which arise from the needs and requirements of the information society, can no longer be realized simply by limiting access to such data at the level of archival material. By systematically changing the status of this type of data, archival practice may unknowingly violate the rights defined by law, which arise from the protection of sensitive data. Remediation of the resulting damage, especially in view of the large amounts of metadata in electronic form, can represent large losses, especially of human potential in the archives.

If we compare Germany, the Czech Republic and Hungary, we can see that only the Czech Republic has free access to all archive material for all users. Germany on the other hand has restrictions regarding access (namely: limited access to sensitive personal data, extraordinary access without anonymization is also regulated, e.g. researchers, office employees, and after the last amendment to the law, access to non-anonymized material is also enabled » external" academic researchers). Archival material containing the above data becomes accessible 30 years after the death of the individual. In Hungary, access to personal data and personal sensitive data (race, nationality, religion, etc.) is limited. In exceptional cases access to the material is permitted. Researchers sign a data protection declaration.

We note that different countries treat access to archival material containing classified and sensitive information differently. We can also note that some countries restrict access to archival material containing the aforementioned data.

The entire archival legislation must be harmonized in accordance with international legal acts that are directly applicable and with which individual legal acts of the member states of the European Union must also be harmonized. It makes sense to regulate the anomaly in this area systematically, it is necessary to involve the archival profession and good practices.

REFERENCES

Anžič, A. (1997). *Varnostni sistem Republike Slovenije*. Ljubljana: Uradni list RS.

Anžič, A. (2000). Tajnost: vrednota in zlo. *Teorija in praksa* 37(5): 849 - 863.

Brezovšek, M. & Črnčec, D. (2004). Tajnost v demokraciji. *Teorija in praksa*, 41, (3-4).

Council decision on the security rules for protecting EU classified information, (2013/488/EU), (2013). *Official Journal of the European Union 56*. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:274:0001:0050:EN:PDF

Hajtnik, T. (27. 9. 2022). Zakonodaja, ki obravnava osebne, tajne in zaupne podatke. *Forum Media.* https://www.e-dokumentacija.si/vsebine/predpisi-in-terminologija/varstvo-tajnosti-zasebnosti-in-osebnih-podatkov/zakonodaja-ki-obravnava-osebne-tajne-in-zaupne-podatke/zakonodaja-ki-obravnava-osebne-tajne-in-zaupne-podatke/

Kazenski zakonik (KZ-1). (2012, 2015, 2016, 2017, 2020, 2021). Uradni list RS, (50/12 – uradno prečiščeno besedilo, 6/16 – popr., 54/15, 38/16, 27/17, 23/20, 91/20 in 95/21).

Klasinc, P., P. (2016). Nekatere projekcije dostopnosti in uporabe arhivskega gradiva. In I. Fras (ed.), *Tehnični in vsebinski problemi klasičnega in elektronskega arhiviranja*, *Popisovanje arhivskega gradiva*: 15. zbornik mednarodne konference *[Radenci, 13. - 15. april 2016]*(pp. 81–90). Maribor: pokrajinski arhiv Maribor.

International Council on Archives (ICA). (1996). *Kodeks etike*. https://www.ica.org/sites/default/files/ICA_1996-09-06_code%20of%20ethics_SL.pdf.

Kremenšek, M. (24. 2. 2014). *Ali bo referendum o arhivski noveli*? Inslov-info. https://www.insolvinfo.si/medijsko-sredisce/v-srediscu/113476.

Lavrič, T. (2008). Zaupni podatki v dokumentarnem in arhivskem gradivu. V: S. Tovšak (ur.), *Tehnični in vsebinski problemi klasičnega in elektronskega arhiviranja*. Zbornik referatov z dopolnilnega izobraževanja (pp. 41–51). Maribor: Pokrajinski arhiv Maribor

Ministrstvo za kulturo. (2013). *Predlog Zakona o spremembah in dopolnitvah Zakona o varstvu dokumentarnega in arhivskega gradiva ter arhivih (ZVDAGA-A)*.

http://arhiv2014.skupnostobcin.si/fileadmin/sos/datoteke/pdf/Barbara/PREDLOGI_PREDPISOV/Kultura/2013/ZVDAGA_29_5_2013.pdf

Novak, M. (2019). Methods og linear and hierarchical sequences in archives. *Atlanti* +,. 29-(1), 26-40.

Novak, M. (2016). Klasična in nova paradigma varovanja občutljivih podatkov v arhivih. Alanti, 26(1), 55–63.

Prepeluh Magajne, U. (2011). Tajni podatki. *Komentar Ustave Republike Slovenije*. https://e-kurs.si/komentar/tajni-podatki/.

Prezelj, I. & Tarman, M. (2015). Sistem varovanja tajnih podatkov v Republiki Sloveniji v luči demokratičnega zagotavljanja nacionalne varnost. *Teorija in praksa 52*(4). http://dk.fdv.uni-lj.si/db/pdfs/TiP2015_4_PrezeljTarman.pdf.

Resolucija o strategiji nacionalne varnosti Republike Slovenije. *Uradni list RS*, (59/19).

Trbovešk, F. (2004). *Varnostni in pravni vidiki varnostnega preverjanja oseb*. Magistrsko delo. Ljubljana: Fakulteta za podiplomske državne in evropske študije.

Urad vlade za varovanje tajnih podatkov. (2022). https://www.gov.si/drzavni-organi/vladne-sluzbe/urad-vlade-za-varovanje-tajnih-podatkov/

Uredba o varovanju tajnih podatkov. (2022). *Uradni list RS*, (50/22).

Uredba o upravnem poslovanju. (2018, 2020, 2021, 2022). *Uradni list RS*, (9/18, 14/20, 167/20, 172/21, 68/22, 89/22 in 135/22).

Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih (ZVDAGA). (2006, 2014). *Uradni list RS*, (30/06 in 51/14).

Zakon o spremembah in dopolnitvah Zakona o varstvu dokumentarnega in arhivskega gradiva ter arhivih. (2014). *Uradni list RS*,(51/14).

Zakon o tajnih podatkih. (2006, 2010, 2011, 2020). *Uradni list RS* (50/06 – uradno prečiščeno besedilo, 9/10, 60/11 in 8/20).

Zgodovinski arhiv Ljubljana (ZAL). (2022). *Upravvljanje z dokumentarnim gradivom v stalni zbirki.* https://www.zal-lj.si/project/upravljanje-z-dokumentarnim-gradivom-v-stalni-zbirki/.

Žirovnik, J. (2005). Dostop do tajnih podatkov v zvezi NATO in EU ter v izbranih tujih zakonodajah. V B. Lobnikar (ed.), *Zbornik prispevkov [Elektronski vir] / 6. slovenski dnevi varstvoslovja, Bled, 2.-4. junij* (pp. 1–15). Ljubljana: Fakulteta za policijsko-varnostne vede.

Žumer, V. (2008). *Poslovanje z zapisi. Upravljanje in hramba dokumentarnega gradiva*, klasifikacijski načrt za razvrščanje gradiva z roki hrambe in elektronska hramba gradiva *v digitalni obliki*. Ljubljana: Planet GV.

TYPOLOGY: 1.01 Original scientific research