SYSTEM OF ACCESS TO CLASSIFIED INFORMATION IN THE REPUBLIC OF SLOVENIA

Kristina Kotnik Šumah, Deputy Information Commissioner

Nataša Pirc Musar, Information Commissioner of the Republic of Slovenia

1. Regulation of classified information in the Republic of Slovenia: reasons for the adoption of the law, its aims and main features

Transparency of work of state agencies and the right to access to public information are two principles which have become established in all modern and democratic societies. However, there is a need to protect certain information in order to protect the benefits of the state and the society as a whole. Thus the right of the public to acquire public information sometimes needs to be withdrawn for the benefit of public security, defence, state security, or to protect international relations of the state. State security is one of the most important assets of modern democratic society, and enjoyment of other human rights depend on it. Thus the interests between of state and the interest of the public for obtaining public information need to be continuously and carefully weighed. The main problem in dealing with these issues is not to limit the right of the public to know because of the protection of public security; the problem is a potential abuse which might occur in any public authority when dealing with the phenomenon of »confidential«[1].

The area of classified information In the Republic of Slovenia is regulated by the Classified Information Act [2], which came into force on Nov. 23, 2001. So far, the Act has been amended four times with no significant changes in terms of regulatory framework of this field. None of the changes concerned the basic principles of the law, i.e. the system of determination, declassification and access to classified information. The most important changes, however, from the aspect of the topic we are dealing with here, is the amendment to this Act, made in March 2006[3] , which introduced an explicit provision, namely that by this act the Information Commissioner too is allowed access all classified information of any level of confidentiality without performing security testing [4], as well as a new provision introduced under Art. 21.a[5], which regulates the declassification of data due to the prevailing interest of the public.

As can be seen from the proposal of the Classified Information Act [6], in preparing the law the Government RS drew upon the principle of transparency of work of all branches of

[1] Urška Prepeluh, The right of access to public infrmation; doctoral dissertation, Ljubljana, September 2004, p. 172.
[2] Classified Infromation Act (Official Gazette RS, No. 87/01, with amendments, hereinafter: ZTP), Englsih version of the consolidated text is available at: http://www.uvtp.gov.si/en/legislation_and_documents/legislation_in_force/;
[3] Act amending the Classified Infromation Act (Official Gazette RS, No. 28/2006, ZTP-B).
[4] See Art 3 ZTP.
[5] See Art. 21. a ZTP.
[6] Proposed Act on Classified Information, first reading, Poročevalec Državnega zbora RS, No. 10/2000.

national authority, particularly transparency of the work of state administration. An interesting fact is that the statute governing access to public information, i.e. ZDIJZ[7] was adopted only in 2003, which is two years after the Classified Information Act had been passed. What is also interesting is that as early as 2000, which is before the ZDIJZ was adopted, the draft of the Classified Information Act incorporated the right of the public to request public information, and also introduced an exemption to this rule if the case concerned classified data. The draft also envisaged that refusal decisions need to contain the grounds for the decision and that and that a client has the right to make an appeal.[8] This provision, however, was deleted during second parliament reading on the grounds that »the area of access to public information, as well as possible limitations, should be regulated by a special act.«[9]

ZDIJZ treats confidential data as one of the exemptions to free access to public information. Subpara 1, Par 1. Art. 6 stipulates that the body must deny the applicant access to the information if the request relates to the information which, pursuant to the Act governing classified data, is defined as classified. Determining data as classified means that the data have been subjected to a special regime of protection by which unauthorised persons, including the public, are prohibited access. What is important is that ZDIJZ defines exemptions only for the information which is suitably defined as confidential according to the law governing confidential data. The law governing confidential data in Slovenia is ZTP. ZTP regulates definition of concepts, protection and access to public data in a complex and uniform manner for all state agencies. This means that no state body is *a priori* excluded from this regime (the regime of classified information protection according to ZTP encompasses also the Slovenian Intelligence Agency, Ministry of Defence, and Police). Therefore, allowing or not allowing access to the information needs to be assessed only on the basis of what the information contains and the statutes for a particular document.

In the assessment of the state of affairs and among the reasons for introducing the law, the proposers of the Classified Information Act basically referred to the fundamental human right to access public information[10] and its role in a democratic society. Classified Information Act has been designed on the basic premise that it is a *duty* of government agencies to ensure everyone access to data and information, of course within the conditions and limitations defined by law. The principle of transparency and accessibility to the data and information of government agencies can not be absolute and limitless, therefore, the *limitations* to public accessibility *need to be determined by law.* What is required is maximum clarity and precision of statutory provisions, using limitations consistently and only according to the law, and restrictive use of limitations determined by law in practice, as well as time limitation. The proposer of the law stated that: »Regulation of these issues is extremely demanding and sensitive. It is very difficult to find proper balance between the powers of national authority on the one hand and rights and freedoms of individuals on the other. For all these reasons it is necessary to incorporate consistently the following generally accepted principles into legislation:

- definition by law;

- restrictiveness in defining;

[7] Access to Public Information Act (Official Gazette RS, No. 24/2003, with amendments, hereinafter ZDIJZ).
[8] See: Art. 4, Proposed Act on Classified Information, first reading, Poročevalec Državnega zbora RS, No. 10/2000.
[9] Proposed Act on Classified Information, second reading, Poročevalec Državnega zbora RS, No. 22/01 of March 30, 2001, No. 53.
[10] See Par 2. Art. 39 of the Constitution of RS.

- urgency and validity in the application of principles,

- legal binding.

With this we also need to consider the fact that the reasons for determining limitations to access, or determining data as classified, depend on the various categories and circumstances which may be rather more political than legal in nature. And since in the rule of law it is necessary to establish legal binding for these categories, this can only be achieved by integrating all relevant questions into a comprehensive and consistent system of legal rules, procedures and measures«.[11]

From what has been said it derives that those who were preparing the ZTP Act wanted to organise the system of classified information comprehensively, uniformly and compulsory for all state agencies and other users of classified information. Prior to this Act the area of classified information was regulated by several different laws, while the operation of some state agencies was not regulated at all. In practice, there was a great amount of classified information, however the system of determining classified information and its protection was non-transparent and difficult to manage. The competences of public officers for determining confidentiality of information, and accessing confidential documents and their protection were not clearly defined. One of the reasons behind the preparation of ZTP was also Slovenia was in the process of integration into European Union and other international integrations and associations, e.g. NATO and WEU (nowadays, Slovenia is already member of all these integrations). Unfortunately, from the proposed act we cannot see which particular comparable legal systems (or model states) Slovenia followed.

Among the aims set out by the proposer of the law, the following need to be particularly mentioned:

- clear regulation of legally permissible exemptions in exercising the constitutional right of people to be informed on the activities of the state and its agencies, which is one of the fundamental rights and freedoms of citizens. Regulation of exemptions requires clear definition of reasons, conditions, procedures and powers and competences in dealing with confidential information;

- protection of state interests and benefits needs to be regulated by law;

- for the protection of state secrets there needs to be a unified system of responsibilities of state officials and employees;

- limitations of discretionary in arbitrary actions of state officials in limiting accessibility to information and data need to be provided by law;

- there must be a unified system of decision making which would apply to all fields and all levels of organisation of the state. For the protection and access to classified information and the information which is the result of the work of state agencies the system should be regulated by a special act and general acts deriving from it.

[11] Proposed Act on Classified Information, first reading, Poročevalec Državnega zbora RS, No. 10/2000.

Thus, the purpose of ZTP[12] was to provide a system for unified treatment of questions which had not been properly regulated before. This involved:

- defining the reasons for limiting access to the information of state agencies;
- determining the conditions which need to be fulfilled in order to determine a particular information as confidential;
- setting out the procedures for determining data confidential;
- defining the bodies and authorised persons in charge of determining classified information;
- treatment of different levels of confidentiality, period of restricted access and methods of declassification;
- introducing the rules and standards for defining classified information;
- defining responsibilities for protecting classified information ;
- defining minimal standards for the protection of classified information, to be followed by all state administration bodies and other state agencies and the users of such information when dealing with the data with a particular level of classification.

2. Definition and criteria for defining classified information

Among concept definitions ZTP[13] defines classified information as 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 country which, for the 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. **Thus, for defining a data as confidential, two criteria need to be fulfilled cumulatively:**

1. **material criterion, and**
2. **formal criterion**

Material criterion means that a data can be defined as confidential only if: (1) it is of such importance that by disclosing the information to unauthorised person would it would threaten the vital interests of the country, its security or its political and economic benefits, and (2) if it refers to public security, defence capability, foreign affairs, intelligence and security activities of state agencies of the Republic of Slovenia , or if it refers to systems, appliances, projects and plans or research, technological, economic and financial matters which are important to these goals.

[12] This derives from the Proposed Act on Classified Information, first reading, Poročevalec Državnega zbora RS, No. 10/2000.
[13] See item 1, Art. 2 of ZTP.

From the definition above we can see that material criteria have two characteristic features: (1) potential harm due to disclosure of information, and (2) relevance to particular fundamental interests of the state or the society which are also listed in the Act. An authorised person is required to prepare a written assessment on potential harms. The assessment needs to include the object of protection (i.e. which particular interest would be jeopardized -- the security of the state, or its political or economic benefits--, as well as the description of the intensity of possible negative effects. What is interesting is that economic interests are listed among the objects for protection to which a confidential information may refer to, however they can represent an area of potential harm (i.e. the information needs to be of such importance that its disclosure would cause harmful effects to the economic interests of the state).[14] The areas of interest to which the confidential information may refer to are listed in ZTP.[15]

In other words, if the information does not refer to any of the areas of interest defined under ZTP, the state body is not allowed to determine the information as classified. Some examples from the practice of the Information Commissioner show that if it is found out during the appellate procedure concerning access to public information that the contents of a document does not refer to any of the protected areas according to Art. 5 of ZTP, the material criterion for the existence of confidential information has not been fulfilled. The document may be correctly assigned a label classified but the data can not be treated as confidential.

Case study:

There was case where the applicant requested access to a part of verbatim record of the session of Government RS[16]. The Information Commissioner brought a decision that the document in question was not confidential since by its contents it *obviously* did not refer to public security, defence, foreign affairs or intelligence or security activities of state agencies of the Republic of Slovenia. The written assessment of harmful effects did not make any evidence on concrete damage which might be caused by disclosing the document, or describe in what manner the disclosure could jeopardize the security of the state, or the interests of the Republic of Slovenia, its political and economics interests. **Making just an overall reference to one of the protected interests is not enough to fulfil the material criterion.**

The concepts, such as »public security«, »defence«, »foreign affairs « and »intelligence« can be broadly interpreted under different social (and in particular) political circumstances and can be easily abused in practice. In explaining the concepts, the Slovenian legal order drew upon the Resolution on the strategy of national security RS adopted in 2001[17]

[14] Urška Prepeluh, The right of access to public information, doctoral dissertation, Ljubljana, September 2004, p. 176.
[15] See Art. 5 of ZTP.
[16] See the decision No. 090-87/2010 of Aug 11, 2010; A similar decision was brought by the Commissioner in the case Ref. No. 021-16/2006/4, Englsih version is accessible at: http://www.ip-rs.si/index.php?id=373.
[17] Resolution on the strategy of national security RS (RESNV), Official Gazette RS, No. 56/01 and 110/02 – ZDT-B.

and in 2010[18]. The authors of Slovenian legal theory applied EU standards in explaining the material criteria for confidential information[19] as well as international legal standards, particularly referring to two sources: the Siracusa Principles on the Limitation and Derogation Provisions MPDPP[20], prepared in 1985 by a group of experts of international law which was then broadly accepted by the professional community in UN, as well as the Johannesburg principles of national security, freedom of expression and access to information. These principles emphasize that limiting access to information in order to protect national security is legitimate only if there is a real purpose or evidence that the existence of the state or its territorial integrity are jeopardized, or there is a threat of violence, or when we need to protect the ability of the state to respond to actions of violence or threat from external sources in any form (e.g. military threat), of from internal sources (e.g. incitement to violent overthrow of the government).[21]

Both elements of the material condition for the existence of confidential data are reflected in **the formal criterion**. A data can be justifiably labelled as confidential only if all the three criteria, described further below, are fully met. These are:

(1) The first element is that information can be determined as confidential only by an authorized person. Authorised persons are defined under Art. 10 of the ZTP[22]. These include: directors of state agencies who can authorise *in writing* another person from the state agency, however the authorisation can not be transferred further on. With this it is ensured that only persons who have sufficient knowledge to assess potential danger of disclosing information to unauthorised persons can bring decisions on confidentiality of the data. However, documents with TOP SECRET label may only be assigned by persons defined by ZTP. These include: the President of the Republic, the President of the National Assembly, the chairman of the Commissions of inquiry set up by the National Assembly, the Prime Minister, ministers and directors of agencies attached to the ministries, certain military commanders, certain heads of diplomatic and consular representations of the Republic of Slovenia and heads of Government services directly answerable to the prime minister or their deputies. The authorised person must determine the level of classification of a piece of information at the origin of that piece of information, i.e. at the beginning of the performance of a task of the agency that results in classified information. [23].

If the information has not been determined as classified by an authorised person, or if this was not done at the origin of that piece of information, it is deemed that one of the formal criteria has not been met and consequently the information can not be treated as confidential. Therefore, such information can not be protected under ZTP and becomes public information accessible to anyone,

[18] Resolution on the strategy of national security RS (RESNV-1), Official Gazette RS, No. 27/10).
[19] Security Regulations of the Council of European Union, II/2/6 and Commissions Provisions on Security, 16.3.
[20] Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights, U.N Doc. E/CN.4/1985/4, Annex.
[21] the same principles for the asessment of the material criterion are mentioned als in: Urška Prepeluh, The right of access to public information, doctoral dissertation, Ljubljana, September 2004, š. 178.
[22] See Art, 10 of ZTP.
[23] See Par 1, Art. 11 of ZTP.

Case study:

In this particular case the Information Commissioner followed the same principle [24], and decided that the formal criterion for the existence of confidential information was not fulfilled since the state body failed to submit corresponding authorisation, showing that the person who assigned this document as confidential was also authorised to do so. In fact, this particular document carried a label CONFIDENTIAL and it also contained a written assessment of adverse effects, however, the body did not provide suitable authorisation document which should indicate that the acting General Secretary of the Government was authorised by the President of the Republic to assign the level of classification to this document. In fact, the Information Commissioner did receive such authorisation but found out that it was issued after the written assessment on possible damage had been made. Since the body failed to present suitable authorisation for determining the level of classification, the Information Commissioner established that one of the criteria which had to be met cumulatively to determine the information as confidential, was not met.

(2) ZTP also prescribes methods and procedures for determining the level of classification, where the most important element is a written assessment on adverse effects of the disclosure of information[25]. Such written assessment, as a rule, needs to be elaborated simultaneously with determining the level of classification to a document, as defined under Par 3, Art 11 of ZTP, which also stipulates that » Where the elaboration of a written assessment prior to the performance of urgent tasks of an agency would make the performance difficult or impossible, the authorised person may determine the level of classification of a piece of information orally and mark it with the level of classification. A written assessment shall be elaborated as soon as possible, but within three days at the latest«. From this diction it derives that immediate elaboration of a written assessment on adverse effects is a rule, while deviations from this rule are possible only exceptionally and in particular circumstances. Such written assessment represents the second formal criterion and the object of protection needs to be determined. The object is an interest which might be endangered by disclosure of the information. In addition, written assessment needs to include a description of the damage and how intense the adverse effects might be. Such written assessment is a formal attachment to the document and is kept by the body which assigned the level of classification. **Written assessment on possible adverse effects, from the point of view of access to the document, later allows for the assessment of the reasons and circumstances which led to the decision to determine the document as confidential.** The provisions of ZTP, which require a written elaboration of adverse effects, are also helpful for the authorised persons when determining confidentiality. They can carefully analyse and weigh all possible circumstances and develop a more responsible attitude towards decision making. All state agencies need to be aware that free access to documents is a rule, while confidentiality is only an exemption (both, ZTP and ZDIJZ draw upon this premise), and it is the state agency which carries the burden of proof for the existence of such exemption.

(3) The third formal criterion refers to assigning a correct label. Information can be treated as confidential only if it carries a suitable label[26]. Classified information, in view of

[24] See the IC decision No. 090-87/2010 of Aug 11, 2010, p. 14.
[25] see Art. 11 of ZTP.
[26] See Art. 17 of ZTP.

possible adverse effects on the security of the sate or its political or economic interests if access was allowed to an unauthorised persons, can be assigned with the following levels of classification: TOP SECRET, SECRET, CONFIDENTIAL and RESTRICTED. The TOP SECRET classification is used for classified information the disclosure of which to unauthorised persons would put in jeopardy or do irreparable damage to the vital interests of the Republic of Slovenia. The SECRET classification is applied to classified information the disclosure of which to unauthorised persons could seriously harm the security or interests of the Republic of Slovenia. The classification CONFIDENTIAL is applied to classified information the disclosure of which to unauthorised persons could harm the security or interests of the Republic of Slovenia. RESTRICTED, which is the lowest level of protection, protects only the work of the body, and may be applied for the classified information the disclosure of which to unauthorised persons could harm the activity or performance of tasks of an agency. Among the basic concept definitions, ZTP does not precisely define the various levels of damage or differences between »irreparable damage«, »serious damage« or »damage«[27] however it defines the concept of » threat to the vital interests of the country « as a threat to the constitutional order, independence, territorial integrity and defence capability of the country. Therefore, it is the authorised person who takes decisions on the level of damage and makes assessment of adverse effects for each particular case. Since the assessment on possible adverse effects needs to be very concrete and substantiated, the authorised person needs to give an explanation why and how the disclosure of a document would jeopardize the interests and what would be the level of the damage. It is the written assessment which can later be used to evaluate the suitability of the assigned level of confidentiality with regard to the level of potential damage. Thus a written assessment becomes indispensable in all appellate procedures dealing with access to public information and requests for declassification of a document before the appeal body (Information Commissioner) and later, before the administrative court.

ZTP also explicitly stipulates that the authorised person, when classifying information, must assign the lowest level of classification that still ensures such a degree of protection as it is necessary to safeguard the interests or ensure the security of the country[28]. If only a smaller part of a document contains classified information that part of the document needs to be detached from the remaining document and treated and protected in accordance with the level of classification markings.[29] Here we need to consider the principle of partial access and establish whether the protected part of the document can be detached from the whole text without jeopardizing its confidentiality. If this is possible, the authorised person needs to apply this rule. There was a case when a question arose whether the whole programme of an event, which contained a plan for providing security to the president of the state who was to visit the event, could be marked confidential, because in its contents the matter was complex since it was kept in one folder of documentary material. The answer was negative because the security plan could be easily detached from the rest of the material and for this reason it would not be permissible to mark the whole folder as confidential to protect only one document which was part of the whole documentation.

[27] See Subpara 10 Art. 2 of ZTP.
[28] See Art. 14 of ZTP.
[29] See Par 2, Art. 12 of ZTP: Where only a smaller part of a document or an individual document of a matter contains classified information, that part of document shall be detached from the remaining document and treated and protected in accordance with the level of classification markings.

In determining the level of confidentiality, agencies are allowed to use only the markings defined by ZTP and no other markings. In other words, documents which are not labelled with one of the four markings by ZTP, can not be protected by law. The only exemption are confidential data of foreign countries and international organisations which communicate the information to the Republic of Slovenia or its agencies and expect that the information will remain confidential, as well as the information which is the result of cooperation between Slovenia and its agencies with a foreign country or international organisation or its bodies and for which it has been agreed that the information is to be treated as confidential. These data are treated under a special regime.[30] As a rule, confidential data of foreign countries or international organisations retain the markings which are used in foreign countries or international organisation, or are marked according to the rules set out by ZTP, however, the levels of classification need to be comparable and ensure equal degree of protection. The method of marking classified information of the Republic of Slovenia in a foreign country or international organisation, and the determination of such a degree of protection of that information, comparable with the provisions of ZTP, should be specified in an international treaty on the exchange or provision of classified information between a foreign country or international organisation and the Republic of Slovenia[31].

As for the marking procedure and treatment of confidential data of NATO and EU, the provision under Art. 43b ZTP[32] must be applied, and based on which the Instructions for handling NATO and EU classified information was adopted.[33] Article 4 of the Instructions defines which classification levels of NATO and EU are comparable with the classification levels from ZTP, and Art. 6 stipulates that the NATO classified information must be handled in the RS in compliance with the NATO security policy, and EU classified information in compliance with the EU security policy unless a referral to national legislation is made in the provisions of the NATO or EU security policy.

In addition to the material and formal criteria for defining classified information, which are both positive conditions and have been described above, there is however a negative condition: According to Art. 6 of ZTP[34], a piece of information that has been defined as classified in order to cover up a criminal offence, the exceeding or abuse of authority, or some other unlawful act or behaviour, must not be considered classified. It may happen that a state agency will invoke the grounds for protection of state security or national defence or its international relationships whenerver they feel that the disclosure of information would reveal some irregularities, cases of abuse or illegal actions within the agency. Therefore, we need to make a distinction between the actual interests of the state, which are legitimately protected aims, and mocking interest to preserve certain persons to remain in power, i.e. a combination of personal interests

[30] See Art 9 of ZTP: »Protection and access to classified information of a foreign country or international organisation shall be carried out in accordance with this Act or the regulations based thereon, or in accordance with international treaties concluded between a foreign country or international organisation and the Republic of Slovenia.«.
[31] See Art. 20 of ZTP.
[32] See Art. 43.b of ZTP.
[33] English version of the text is avaiable at: http://www.uvtp.gov.si/en/legislation_and_documents/legislation_in_force/;
[34] Art. 6 of ZTP: »A piece of information that has been defined as classified in order to cover up a criminal offence, the exceeding or abuse of authority, or some other unlawful act or behaviour shall not be considered to be classified.«.

with the interests of the state. In practice, such assessments to evaluate whether the conditions from Art. 6 of ZTP have been fulfilled can be very demanding and must be treated separately, case by case.

Case study:

The position of the Information Commissioner in dealing with the case Ref. No. 090-29/2009/5 dated May 3, 2009[35] was that according to Art. 6 of ZTP two conditions had to be fulfilled: (1) that the information was not obtained by some criminal act, or exceeding or abuse of authority or some other unlawful act, and that (2) the information was defined as classified to cover up an unlawful act. In this case the Information Commissioner concluded that the two conditions were not fulfilled. The applicant only made an overall reference, namely that »certain violations have been found out several times which are obvious since the Republic of Slovenia filed criminal complaints for unlawful acts and abuse of authority, therefore the requested information can not be defined as classified«. The applicant, however, did not make any precise statements what irregularities were in question and whether the judicial procedures had been concluded with the force of res judicata. The provision of Art. 6 of ZTP cannot be applied if the applicant only expresses a doubt that a state agency was acting unlawfully. When it is found out that the case meets the conditions under this article, the information loses the confidentiality character and becomes public information.

3. Termination of the period of restricted access to classified information

According to ZTP confidentiality of a data may terminate in the following ways: on a particular date, after the occurrence of a particular event, after expiration of a particular period, or by revocation of confidentiality. The provisions on determining classified information implicitly stipulate that termination of protection period needs to be defined as soon as the information has been defined as classified.

ZTP does not prescribe a period of restricted access but stipulates that the authorised person must revoke confidentiality of the information *immediately* after the conditions for giving the status of confidentiality have been fulfilled according to the law (i.e. when no adverse effects can be expected by disclosing such information). The revocation needs to be provided in a written form, while all persons possessing such document, or having access to it need to be informed about termination of restricted access. In case the confidentiality is not revoked, restricted access to information terminates after the period set out by the act governing archives and archival institutions.[36] Art. 65 of this Act stipulates that »*the period of restricted access to public archives containing information which refers to state and public security, defence, international affairs, or intelligence and security of the state and its economic and business interests or tax secrets and the disclosure of which to unauthorised persons could cause adverse effects on the security of the state and other persons and their interest, terminates 40 years after the creation of*

[35] A summary of the Decision No. 090-29/2009/5 dated May 3, 2009 in Englsih is available at: http://www.ip-rs.si/fileadmin/user_upload/Pdf/odlocbe/IC_Decision_Sova_newspaper_Dnevnik.pdf.
[36] Protection of Documents and Archives and Archival Institutions Act (Official Gazette, No. 30/2006, hereinafter: ZVDAGA).

the document«. The Government RS may extend the period of restriction, however only exceptionally, for the period of maximum 10 years. The Government RS, based on the proposal of a natural or legal person, may shorten the general period of inaccessibility «*provided that the use of public archives is absolutely necessary for attaining the set scientific goal and provided that public interest prevails over the interests to be protected.*«[37] There have been no such cases in practice where the Government of RS would either extend or shorten the period of restricted access to archival documents. However, the Information Commissioner believes that 40 years is a too long period and, therefore the Commissioner is planning to suggest the Government of RS to shorten the period to 20 years to become comparable with other European states.

Notwithstanding the provisions on protecting classified information for archives, the documents which were created before the constitution of the Assembly of the Republic of Slovenia i.e. prior to May 17, 1990, and which refer to previous socio-political organisations, such as The Slovenian Communist Party, Socialist Worker's Union, Trade Union Confederation, Union of Socialist Youth of Slovenia, Association of Slovenian Reserve Officers of Slovenia, Association of Yugoslav National Liberation War Combatants, bodies under the ministry of interior (e.g. police), judicial authorities (e.g. courts, prosecution services, prisons) and intelligence service, can be accessed without any limitations, with an exception of archival material which contains sensitive personal data obtained by violation of human rights and fundamental freedoms and which refer to persons who were not holders of public authorities. In the event of doubt a special archive commission must decide about allowing access.

An interesting point to make is that the period of restricted access to archives is determined only by ZVDAGA and not by ZTP. Period of restriction, compared to other systems and international standards, is absolutely too long, which calls for making changes in ZTP, namely that archival material should become public after 10 years, except if a body explicitly prolongs the duration, or reclassifies the document. In this case the authorised person needs to make a new written assessment of adverse effects. By Par 2, Art. 18 of the ZTP the authorised person is required to review classified data assigned with the mark TOP SECRET once a year, while other levels of classification need to be rechecked every three years and assessed whether there is still a need to keep the information classified. The law, however, does not provide any consequences for not complying with this rule and the documents are automatically declassified.

Classification of documents can be also revoked upon a proposal[38]. According to ZTP, the proposal can be made either by: (1) an individual whose request for classified information has been turned down, or (2) an entitled user of classified information that has legally received the information. In both cases it is the authorised person who deals with the case and makes a decision on declassifying the document and needs to notify the proposer about the decision. The procedure for **declassification of information upon a proposal** is a kind of internal procedure which is not precisely defined by ZTP. It means that the same body which has determined that the information is classified, also handles proposals for declassification, however, there are no legal remedies against such decisions of the body.

[37] See Art. 42 of ZVDAGA.
[38] See Par 3,Art. 15 and 21 of the ZTP.

However, this internal procedure is different from the **declassification procedure**, which is formalised and precisely regulated by ZTP and ZDIJZ. By Art. 21a of ZTP[39] it is the Government RS which decides on questions of declassification if the director of the agency considers, in accordance with the law governing access to public information, that justification of the prevailing public interest for disclosure should be assessed. With other bodies, which are not accountable to the Government (e.g. the Parliament), the director of the body must decide if access to classified information is justifiable, and use the same procedure as the Government.

The Government decides on the justification of access to the piece of information on the basis of a provisional opinion of the Commission which consists of representatives of the ministry responsible for defence, the ministry responsible for the interior, the ministry responsible for external affaires, the Slovene Intelligence and Security Agency and the National Security Authority. The representative of the agency that classified the information may not participate in the Commission. The Commission must call upon the agency which classified the piece of information to submit an assessment of adverse effects on the basis of which the classification of the piece of information was made, and also upon every recipient of the classified piece of information to give his opinion on the justification of the disclosure of the piece of information and the reasons for the preservation of its confidentiality. The Commission must, within 30 days after the submission of the request for access to public information, prepare an opinion on the justification of the request and submit it to the Government.

Should the Government decide that the public interest for the disclosure is stronger than the public interest for limiting access to the piece of information due to its confidentiality, it must order the agency which classified the piece of information to declassify it no later than 15 days after receiving the decision of the Government, and also acquaint the applicant.

If the Government RS turns down the request for declassification, the applicant can file an appeal with the Information Commissioner. The appeal procedure is defined by ZDIJZ.

4. Prevailing interest of the public test and appellate procedure for declassification of information before the Information Commissioner

In addition to Art. 21 of ZTP, the procedure for declassification is also regulated by ZDIJZ[40], which stipulates that if someone holds, that information is denoted classified in violation of the Act governing classified data, he can request the withdrawal of the classification according to the procedure from the article 21 of this Act.

[39] See Art. 21.a of ZTP.
[40] See Par 4, Art. 6 of ZDIJZ.

As for the procedure itself and competences in dealing with the requests for declassification, Par 3, Art. 21 of ZDIJZ refers to the provisions of ZDIJZ[41], which define the conduct and decisions in cases where the applicant has referred to the prevailing interest of the public, or when the bodies hold that this provision should be applied. **In other words, for procedural questions in handling requests for declassification, the provisions which are used in the assessment of the public interest are applied.** After completed procedure at the first instance, the applicants may file a complaint against the decision of a state body with the Information Commissioner.

The public interest test was introduced into ZDIJZ by amendment in 2005[42]. However, two years after the adoption of ZDIJZ practice showed that absolute exemptions should be reduced to minimum. It is difficult to give a proper definition of the public interest test since it has been changing over time, but with this test it is possible to detect most hidden irregularities or faults which occur in the public sector. In Par 2, Art. 6 of ZDIJZ the public interest is defined as follows[43]: Without prejudice to the provisions in the preceding paragraph (which defines exemptions to free access), the access to the requested information is sustained if public interest for disclosure prevails over public interest or interest of other persons not to disclose the requested information, except in the cases defined by this Act. The public interest test can not be applied to all the exemptions listed in Par 1, Art. 6 of ZDIJZ. These include the data which pursuant to the Act governing classified data, are denoted with one of the two highest levels of secrecy. **In other words, the use of public interest test for the data classified as SECRET and TOP SECRET, is not possible.** Thus, the top classification levels remain absolute exemptions to free access to the information. Absolute exemptions are also the data which contain, or have been prepared based on classified information of other countries or international organizations, with which the Republic of Slovenia concluded an international agreement on the exchange or transmitting of classified information, as well as the information which contains, or has been prepared based on tax procedures, transmitted to the bodies of the Republic of Slovenia by a body of a foreign country.

In practice, the public interest test is used by the Information Commissioner for making assessments during appellate procedures, but is less used by the bodies at the first instance or by the administrative court in the requests for judicial protection against the decisions of the Information Commissioner. Since 2005, the Information Commissioner has issued 22 decisions in which the public interest test was applied.

[41] See Par 2, Art. 21 of ZDIJZ.
[42] Act amending the Access to Public Information Act (Official Gazette No. 61/2005, ZDIJZ – A).
[43] By Par 2, Art. 6 of ZDIJZ:« 2) Without prejudice to the provisions in the preceding paragraph, the access to the requested information is sustained, if public interest for disclosure prevails over public interest or interest of other persons not to disclose the requested information, except in the next cases:
- for information which, pursuant to the Act governing classified data, is denoted with one of the two highest levels of secrecy;
- for information which contain or are prepared based on classified information of other country or international organization, with which the Republic of Slovenia concluded an international agreement on the exchange or transmitting of classified information,
-For information which contain or are prepared based on tax procedures, transmitted to the bodies of the Republic of Slovenia by a body of a foreign country;
- for the information mentioned in Subpara 4, Par 1 of this article;
- for the information mentioned in Subpara 5, Par 1, except if the tax procedure has become final, or the taxable person has recognised tax obligation but failed to pay taxes within the prescribed time limit.«.

Case study:

In one of the decisions, the Information Commissioner[44] explained the essence of this test as follows: »*The essence of such assessment is that it provides a possibility of relativisation of a certain exemption, which needs to be limited only to situations where the interest of the public prevails over the interest for which that information was protected as an exemption. In applying the prevailing interest of the public we also need to assess whether the interest of the public for the disclosure of information is stronger than the potential damage which might be caused by disclosure. Theory emphasizes that public interest test needs to be used extremely carefully and conscientiously since it requires a significantly higher degree of sensitivity in decision making, where different contradicting rights or interests are being weighed. Thus, the public interest test means an exemption above all exemptions and can be used only when we know that it could lead to discovering a fact which would contribute to a broader discussion and understanding of something relevant for the broader public. The public interest test is all about weighing between the rights and to establish whether the right of the public to know prevails over some other right or an exemption from ZDIJZ, eventually leading to a decison which interest is more important. For example, public interest for the disclosure of information is rather strong in situations concerning obtaining or spending public funds, public security, public health, transparency of decision making which lead to public or parliamentary discussions, etc. Considering that both, the Contract, as well as the Agreement in this case had been assigned the marking CLASSIFIED, the Commissioner had to assess whether the interest of the public for the disclosure of this information is greater than the interest for which the information was protected, i.e. the interest of public security and defence. The concept of public security is not precisely defined and is most frequently considered as casuistic reasoning, i.e. as an interest of the defence, or the state to protect itself against war or against a conflict, and in particular for the protection of military forces, their equipment and capacities. Public interest, as a general interest, which does not satisfy only small particulate interests of a group of people, is on the other hand defined as something which could be of importance for the public to know, and allow public control and their participation in matters which require public control. The concept of interest of the public is not always the same, nor can be defined in advance; it can be manifested in different forms. Also, it may change over time, depending on various circumstances. Thus the interest of the public is not a constant but rather changing category which depends on the circumstances in a particular moment and therefore requires individual treatment of a case with considerations to different (also changing) factors which constitute public interest. In this case the interest of the public security and defence was to protect the information about the equipment of military vehicles used in military operations, as well as to protect technical details about the production of these vehicles. The disclosure of such data would jeopardize public security and consequently have negative effects on the army and efficiency of their military operations. The disclosure would particularly impair military position of the army which has a great strategic value in military operations as an element of surprise. Indirectly, the interest of public security is also to protect health and lives of soldiers. Another important factor is that the data in question had been created about six months before the request was made and are still of interest. An additional circumstance which calls for protection of the information is the fact that military vehicles have not even been supplied yet, thus the disclosure of the information in this moment could cause extensive damage. For the same reason, the statement of reasoning in this matter needs to be sustained in order to prevent the disclosure of any information which needs to be protected against public access, and not to nullify the significance of this exemption. Also, it is necessary to protect*

[44] See the Information Commissioner's decision No. 021-20/2007/10 dated Aug 6, 2007.

the information from the Agreement which has not come into force yet. The interest of the public in this case is not as clear and focused than the opposite interest for not disclosing the information. It is rather abstract and general and can be interpreted as a demand for transparency of work of the public sector bodies to act carefully and with full responsibility in decisions on such important public matters as spending public funds. The interest of the public is manifested in the need for an open discussion on matters of importance for the society. By weighing between the circumstances described above, the Commissioner concluded that the interest of the public for disclosure of information does not outweigh the interest of public security and defence to protect these data. It needs to be noted that time factor plays and important role too. After careful consideration of the circumstances these data need to be exempted from free access because at that particular moment the disclosure would cause such negative effects to public security and defense which the public interest could not outweigh. The disclosure would undermine the legitimate interest of the state to protect the information which concerns future defense power of the state. It also needs to be taken into account that confidential information in these documents is rather new and that neither the Contract, nor the Agreement have not been implemented yet. The fact that the Parliament appointed a special commission to enquire this case, and the commission has practically only started with its work, is not a strong enough reason which would justify the disclosure of this information. The first founding meeting of the commission of enquiry was held on May 24, 2007. The fact that some deputies expressed some doubts in this matter, pointing to clientelism, corruption, non-transparent and irrational use of money, and political connections in the purchase of military vehicles, is not a strong enough reason to justify the disclosure of information. We need to consider that these accusations came from the opposition parties and the whole discussion had not yet reached a critical threshold limit to become a turning point for disclosing the information. Allegations based on mere speculations cannot approve the interest of the public since this could lead to artificially created public interest, which would degenerate the meaning of the public interest test.

The Commissioner established that the interest of the public for the disclosure of information was not given sufficiently in this case to overrule the interests for limiting access to the documents, or parts of document, which were marked as restricted to protect the interests of public security. Here we need to reemphasize that the public interest test means weighing between two interests: the interest for limiting access on the one hand and interest of the general public (not only the applicant's interest) on the other. The fact itself that a special commission was established for enquiry into the purchase of military vehicles, cannot encompass the interest of the public. Should the commission find any irregularities, or other relevant facts which would justify public interest, a new assessment of the case should be made, weighing again between the two interests, which eventually might bring different results«.

With the use of public interest test we need to emphasize that the test can be applied only when it has been found out that an exemption to free access has actually been proved. If it is found out by procedure that the conditions for the existence of an exemption referring to classified information have not been fulfilled, the public interest test is not needed since the information is then treated as public information.[45]

[45] See the Information Commissioner's Decision No. 090-161/2009 dated Jan 22, 2010; the summary of Englsih version is available at: http://www.ip-rs.si/fileadmin/user_upload/Pdf/odlocbe/Pop_TV_Ministrstvo_za_zdravje-ENG.pdf, see page 5.

Case study:

There was a case of an appeal against refusal of a request for declassification of a document, where the Information Commissioner did not apply the public interest test[46] because the examinations during the appellate procedure showed that the conditions for the existence of an exemption were not fulfilled. The document in question did not meet the material criterion for defining the information as classified. The Government, which created the document and assigned it with the marking level secret, stated in the assessment of adverse effects, that the document contained details about the procedure for granting a consent agreement, i.e. information whether the proposed candidate was suitable to be nominated as ambassador to the Republic of Slovenia, and which institutions or agencies of Slovenia as a recipient country, verified possible impediments to the nomination. In the elaboration of adverse effects, the Government RS stated that by allowing assess and allowing the public to analyze the merits for the nomination of a foreign ambassador to the Republic of Slovenia would jeopardize bilateral relations between Slovenia and the sending state, which would also have negative effects on economic, political and other interests of Slovenia. By inspection of the document the Information Commissioner found out that the document did not contain any information on the procedure for nominating foreign diplomats to the Republic of Slovenia at all (neither specific nor general). The document merely explained the provisions of the Foreign Affairs Act and the Vienna convention from 1961 on diplomatic relations, and referred to already established international practice for issuing such consent agreements. As already said, such procedures are informal and run by generally accepted principles of international law. All that was mentioned in the nomination agreement was based on the sources such as Foreign Affairs Acts, or the Vienna Convention, or text-books on diplomatic law, which are all generally accessible sources to the public. Therefore, the Information Commissioner decided that there was absolutely no reason why the document should carry a label secret, since the material condition for the existence of classified information, according to ZTP, was not fulfilled. As a result, the Commissioner granted the applicant's appeal and imposed the Government a duty to declassify the document within three days.

In appellate procedures concerning the requests for declassification of documents the Information Commissioner has several options for taking decisions: (1) either to establish that the conditions for the existence of exemptions for classified information have not been met and to impose the body a duty to supply the requested document because the exemption for classified information has not been proved, or (2) to establish that the document fulfills both, the material and formal criteria for the existence of classified information, but there is no evidence of possible adverse effects in case of disclosure, and hence to impose the body to declassify the document, or (3) establish that the exemption to classified information exists, but there is a prevailing interest of the public for the disclosure of the document. Hence, the body needs to declassify the document and make it available to the public, and (4) decline the applicant's appeal having found out that the information represents an exemption to accessing classified information and there is no prevailing interest of the public for the disclosure of the document.

Persons can lodge a request for judicial protection against the decision of the Information Commissioner by initiating and administrative procedure with the Administrative Court of RS. According to the experience so far, state agencies only rarely decide for such action

[46] See the Information Commissioner's Decision No. 090-181/2009 dated Jan 25, 2010.

and so far the Administrative Court has never taken a substantive decision on any matter concerning exemptions to classified information. There was once case when the Court annulled the decision of the Information Commissioner for some procedural reasons and remitted the case for re-examination. Thus, in the field of classified information and access to public documents there has been no judicial practice so far.

5. Office of the Government of the Republic of Slovenia for the Protection of Classified Information and surveillance over the implementation of the Classified Information Act

Directors of agencies are responsible for internal surveillance over the implementation of the Classified Information Act. State agencies which deal with documents assigned with the label CONFIDENTIAL or information of a higher level, need to provide a special post for internal supervision and other professional duties in connection with the determination and protection of classified information within the job classification system, or charge an existing organisational unit of the agency or organisation to execute such duties[47]. In practice, the agencies, in which their employees handle classified documents, a job description needs to include a provision on security clearance, a permission for access to classified information of a particular level. This permission may be obtained also after the employee has been recruited to the job. The employment agreement for such persons needs to include a provision on obligation of protection of classified information. Infringement of such obligation is treated as a serious breach of discipline which can consequently lead to breaking up the employment agreement with the employee.

For monitoring the implementation of ZTP at the system level, a special Government Office for the Protection of Classified Information was established which is also responsible for carrying out tasks of the national security agency. The agency has primarily an advisory and prevention role without inspection authority, and is not an appellate body. In practice, the Office for the Protection of Classified Information monitors the situation in the area of classified information, and ensures the development and implementation of physical, organisational and technical standards of classified information protection, prepares regulations in this area, gives opinion on proposals for other regulations pertaining to the field, implements training programmes for persons dealing with classified information, issues permission for access to classified information, etc. In addition, the Office is responsible for the execution of international obligations and international treaties on the protection of classified information and cooperates with corresponding agencies of foreign countries and international organisations.[48]

Under Art. 42 of ZTP the inspection control over the implementation of ZTP (and consequently for imposing possible penalties for infringements[49]) is in the hands of the Inspectorate of the Interior within the Ministry of RS of the Interior, with the exception of defence, where the inspections must be carried out by the Inspectorate of the Republic of Slovenia for Defence. According to ZTP, penalties may range between 400 EUR to 850

[47] See Art. 41 of ZTP.
[48] For more information see: http://www.uvtp.gov.si/en/about_the_government_office/tasks_and_objectives/;
[49] Penalties are defined in Art. 44, 44a. and 45 of ZTP.

EUR for individuals, 850 EUR to 2.000 for responsible persons from state agencies, and from 4.100 EUR to 12.500 EUR for legal entities. So far there have not been many cases where a fine was charged for such infringements.

In addition to the provisions for violations provided under ZTP, sanctions for breach of confidentiality of data as a criminal act are also provided by the Criminal Code of the Republic of Slovenia [50]. Article 260 of the Code[51] treats the disclosure of classified information as a special criminal act, and provides sentence to imprisonment to three years, and if the offence has been committed out of greed imprisonment can extend to five years. Lower penalties (one year imprisonment) are charged for unintentional criminal acts.

Actually, since 1991, after Slovenia gained its independence, there have been no cases in judicial practice of sentencing someone to imprisonment for breaching confidentiality of classified information, and also there has been no such case where such criminal act would be considered before a court.

6. Conclusion

From the aspect of public access to documents, we believe that the Republic of Slovenia has developed a well-balanced system of classified information. One of the reasons is definitely the fact that those who were preparing the law on classified information worked on the premises of the fundamental human right to access public information, which is evident from the preamble to the draft law. The ZTP regulates the system of classified information systemically, uniformly and binding to all state agencies as well as other users. The Act draws upon the premise that free access to information in a democratic society should be a rule and classified information should only be an exemption. The criteria for defining classified information are clearly and precisely defined by the statute, as well as the system for qualifying and treatment of data. The law provides a procedure for declassification of documents as well as the appellate procedure before the independent state agency, i.e. the Information Commissioner. The public interest test has been implemented in the provisions of ZDIJZ. However, one of the deficiencies of the statute is the period of restricted access to documents which could be considered as archival material, as well as the absence of efficient mechanisms for declassification of such documents.

[50] Criminal Code (Official Gazette RS, No. 55/08, 66/08 and 39/09, hereinafter: KZ).

[51] Art. 260 of KZ: » (1) An official or any other person who, in non-compliance with his duties to protect classified information, communicates or conveys information designated as classified information to another person, or otherwise provides him with access to such information, or with the possibility of collecting such information in order to convey the same to an unauthorised person, shall be sentenced to imprisonment for not more than three years.
(2) Whoever, with the intention of using without authority, obtains information protected as classified information or publishes such information shall be punished to the same extent.
(3) if the offence from paragraph 1 of this Article has been committed out of greed or with a view to publishing or using the information concerned abroad, the perpetrator shall be sentenced to imprisonment for not more than five years.
(4) If the offence under paragraph 1 of this Article has been committed through negligence, the perpetrator shall be sentenced to imprisonment for not more than one year.«.