REGIONAL CONSULTATION ON
NATIONAL SECURITY AND THE RIGHT TO INFORMATION

National Questionnaire
European Consultation, Copenhagen, Denmark, 20-21 September 2012

Country analysed:

Slovenia

Expert analyst:

Name of person completing this form:

Rosana Lemut Strle, Deputy Commissioner

Institutional or organizational affiliation:

Information Commissioner of Republic of Slovenia

1. **A National Security Exception to the Right to Information**

   a. Does the term "national security" or a similar term (*e.g.*, "state security"; "vital national interest") appear in the law as a basis for restricting the public's access to information? *[Principle 2]*

      Please check one: ☒ Yes ☐ No

      If your answer refers to a similar term, please state that term here:

      Access to information may be restricted if information contains "classified information". Classified information is defined as 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 reasons defined in the Classified Information Act, must be protected against unauthorised persons and which has been defined and marked as confidential in accordance with this Act;

      If you checked "Yes":

      i. How is "national security" (or the similar term) defined for purposes of justifying non-disclosure of information? *[Principle 2, 3a]*

      There is no specivic definition of "national security"; however the Classified Information Act justifies restriction of access in this way: "a piece of information may be defined as classified if it is so important that its disclosure to unauthorised persons could or might obviously prejudice the security of the country or its political or economic interests, and is related to:
      1. public security;
      2. defence;
      3. foreign affairs;
      4. the intelligence and security activities of Government agencies of the Republic of Slovenia;
      5. systems, appliances, projects and plans of importance to the public security, defence, foreign affairs and intelligence and security activities of Government
      6. scientific, research, technological, economic and financial affairs of

importance to the public security, defence, foreign affairs and intelligence and security activities of public authorities.

ii. Does the definition of "national security" include international relations?

Please check one: ☒ Yes ☐ No

iii. Does the definition of "national security" include protection against domestic security threats (*e.g.*, law enforcement)?

Please check one: ☒ Yes ☐ No

b. Are there any categories of information (*e.g.*, intelligence operational files) that are exempt from disclosure on the basis of national security? *[Principle 9]*

Please check one: ☐ Yes ☒ No

If you checked "Yes":

i. Please list the categories of information that are exempt:

see above

ii. Is exemption of these categories absolute?

Please check one: ☐ Yes ☐ No

If you checked "No", please explain when the exemption does and does not apply?

c. Are there any public offices or officials (*e.g.*, military branches, intelligence agencies, police) that are exempt from disclosure obligations? *[Principle 6]*

Please check one: ☐ Yes ☒ No

If you checked "Yes":

i. Please list the offices or officials that are exempt:

ii. Is the exemption of these offices or officials absolute?

Please check one: ☐ Yes ☒ No

If you checked "No", please explain when the exemption does and does not apply?

d. Do disclosure obligations apply to non-state actors that are serving as agents or contractors for the government? *[Principle 1a]*

Please check one: ☒ Yes ☐ No

e. Beyond any obligation to disclose information upon request, do public authorities have an affirmative obligation to publish information? *[Principle 1b]*

Please check one: ☒ Yes ☐ No

If you checked "Yes", what information do the security sector, defence, and intelligence agencies have an affirmative obligation to publish? How often is this information affirmatively published by these agencies in practice?

The positive obligation to publish information on the Internet is defined in the Access to Public Documents Act (Art. 10/1):
"Each body is obliged to transmit to the World Wide Web the following public information:
1. Consolidated texts of regulations relating to the field of work of the body, linked to the state register of regulations on the Web;
2. Programmes, strategies, views, opinions and instructions of general nature important for the interaction of the body with natural and legal persons and for deciding on their rights or obligations respectively, studies, and other similar documents relating to the field of work of the body;
3. Proposals for regulations, programmes, strategies, and other similar documents relating to the field of work of the body;
4. All publications and tendering documentation in accordance with regulations governing public procurements;
5. Information on their activities and administrative, judicial and other services;
6. All public information requested by the applicants at least three times;
7. Other public information."
The Act is available here: https://www.ip-rs.si/index.php?id=324

Most Slovenian public bodies publish a lot of information about their work and services, however they do not cover all 7 categories of information listed above. That goes also for the security sector, defence and intelligence agencies. Police and Ministry of Defence are quite proactive in publishing information. No classified information should be published, of course.

2. Requirements for Denying a Request for Information

a. Upon receipt of a request for information, is a public authority always required to confirm or deny whether it holds the requested information? *[Principle 21]*

Please check one: ☐ Yes ☒ No

If you checked "No", under what circumstances may a public authority refuse to confirm or deny whether it holds the requested information?

If the mere affirmation or denial of possession of information would disclose the protected information (e.g. classified information, personal data...).

Classified Information Act has a special provision in this regard:

Article 19
If confirmation of the existence of classified information might adversely affect the interests or security of the country, the agency receiving a request for classified information shall not be obliged to either confirm or deny the existence of the requested information.

b. In denying a request for information, is a public authority required to provide written reasons for the denial? *[Principle 22, 4c]*

Please check one: ☒ Yes ☐ No

c. What requirements are there for a public authority to describe information responsive to a request that it withholds (*e.g.*, Is there a duty to specify the number of pages withheld, or to identify the category of information)? *[Principle 25]*

There is no general obligation to describe the requested information, but only to make sure that it is clear upon which request the authority is deciding. If the authority allows partial access to documents it must specify exactly which parts of information is restricted and that may mean specifying pages and other descriptive information.

d. Is a declaration or certification by the public authority, denying a request for information, that disclosure would cause harm to national security conclusive? *[Principle 4d]*

Please check one: ☐ Yes ☒ No

e. What information or documentation must support an assessment that disclosure would cause harm to national security? Is this information provided to the public? *[Principle 4c]*

An authorised person (defined in Article 10 of the Classified Information Act) determines the level of classification of information at the origin of that piece of information. The authorised person must make a (written) assessment of the possible adverse effects of the disclosure of information to an unauthorised person on the security of the country or on its political or economic interests.

The access to the assessment of the harm to national security may not be restricted, it should be provided to the public upon request.

f. Where there is doubt about whether disclosure would harm national security, does the law favour disclosure? *[Principle 4b]*

Please check one: ☒ Yes ☐ No

g. Is a public authority required to segregate and disclose non-exempt information within a document if those portions of the document are reasonably segregable? *[Principle 24]*

Please check one: ☒ Yes ☐ No

h. What time limits exist for a public authority to respond to a request for information? Are these time limits enforced in practice? *[Principle 27]*

The time limit is 20 working days (in exceptional circumstances may be prolonged for maximum 30 additional working days). The limits are strictly enforced in practice - if the authority does not respond in the provided time limit, the Information Commissioner forces the authority to respond (in specific circumstances also the Inspectorate for Public Administration may react and issue a fine).

3. Classification Procedures

a. Are classification rules publicly available? *[Principle 13]*

Please check one: ☒ Yes ☐ No Cite:

Section 2 of the Classified Information act (unofficial and outdated English version available at https://www.ip-rs.si/index.php?id=505)

b. What criteria are used to determine whether information may be classified? *[Principle 12]*

A piece of information may be defined as classified if it is so important that its disclosure to unauthorised persons could or might obviously prejudice the security of the country or its political or economic interests, and is related to:
1. public security;
2. defence;
3. foreign affairs;
4. the intelligence and security activities of Government agencies of the Republic of Slovenia;
5. systems, appliances, projects and plans of importance to the public security, defence, foreign affairs and intelligence and security activities of Government
6. scientific, research, technological, economic and financial affairs of importance to the public security, defence, foreign affairs and intelligence and security activities of public authorities.

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.

Classified information shall, in view of possible adverse effects its disclosure to an unauthorised person might have on the security of the country or on its political or economic interests, be given one of the following levels of classification:
1. A TOP SECRET classification shall be applied to 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;
2. A SECRET classification shall be applied to classified information the disclosure of which to unauthorised persons could seriously harm the security or interests of the Republic of Slovenia;
3. A CONFIDENTIAL classification shall be applied to classified information the disclosure of which to unauthorised persons could

harm the security or interests of the Republic of Slovenia;
4. A RESTRICTED classification shall be applied to classified information the disclosure of which to unauthorised persons could harm the activity or performance of tasks of an agency.
In determining the levels of classification of information, agencies shall only apply the levels set out in the preceding paragraph.

c. Is the classification status of information conclusive in determining whether a request for that information will be denied? *[Principle 20]*

Please check one: ☐ Yes ☒ No

d. Does the law consider the public's interest in the disclosure of information when deciding whether to classify information? *[Principle 5]*

Please check one: ☒ Yes ☐ No

If you checked "Yes", please explain, in the terms provided by the law, what consideration is given to the public's interest:

There is no specific mentioning of the public interest when deciding to classify, but the law do state that "In classifying information an authorised person shall give the lowest level of classification that still ensures such a degree of protection as is necessary to safeguard the interests or ensure the security of the country."

e. Does the law specify levels of classification (*e.g.*, "Top Secret", "Secret", "Confidential")? *[Principle 12c]*

Please check one: ☒ Yes ☐ No

If you checked "Yes", please list and define the classification levels:

1. A TOP SECRET classification shall be applied to 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;
2. A SECRET classification shall be applied to classified information the disclosure of which to unauthorised persons could seriously harm the security or interests of the Republic of Slovenia;
3. A CONFIDENTIAL classification shall be applied to classified information the disclosure of which to unauthorised persons could harm the security or interests of the Republic of Slovenia;
4. A RESTRICTED classification shall be applied to classified information the disclosure of which to unauthorised persons could harm the activity or performance of tasks of an agency.
In determining the levels of classification of information, agencies shall only apply the levels set out in the preceding paragraph.

f. Who has the authority to classify information? May this authority be delegated? *[Principle 14a]*

Authorised persons that may designate an information as classified are:
1. the director of an authority;

2. elected or appointed officials of the authority authorised to classify and disclose information in accordance with the law or the regulation based thereon, or in accordance with a written authorisation from the director and
3. employees of the authority to whom the director of the agency has issued written authorisation to classify information.
The authorised persons referred to in points 2 and 3 may not transfer their authorisation to third persons.
The TOP SECRET level may only be assigned by certain persons (e.g. the President of the Republic, the President of 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 etc. (for more see: Article 10 of the Classified Information Act, https://www.ip-rs.si/index.php?id=505).

g. Do classification authorities have a duty to classify information? *[Principle 11b]*

Please check one: ☐ Yes ☒ No

If you checked "Yes", when is that duty triggered?

Note: There is no clear duty to classify information (the Act states that the authorised person may classify information), but there is an obligation of any official, employee, or other person performing a function or working in an agency, within the scope of their duties or competencies, to assess the security importance of information and propose to authorised persons that such information be designated as classified if they deem it should be classified.

h. Is there a duty for public authorities to state reasons for classifying information? *[Principle 11b]*

Please check one: ☒ Yes ☐ No

i. Are there any penalties for improperly classifying information?

Please check one: ☒ Yes ☐ No

If you checked "Yes", what are the penalties?

The penalty is monetary (a fine between EUR 417 and EUR 12,519, depending on the misdemeanor and the liable entity). The penalty is prescribed, inter alia,
- if in determining the level of classification, an authorised person does not assess the possible adverse effects of the disclosure of information to an unauthorised person on the security of the country or on its political or economic interests;
- if in classifying information an authorised person does not give the lowest level of classification that still ensures such a degree of protection as is necessary to safeguard the interests or ensure the security of the country;
- if an authorised person changes the level of classification of a document in contravention of the Act;

- if an authorised person does not give a classified document the prescribed markings;
- if an authorised person, in determining the level of classification, exceeds the competencies within the authority for the classification of information;
- etc.

j. When documents are classified, must the documents bear classification markings? *[Principle 12]*

Please check one: ☒ Yes ☐ No

If you checked "Yes":

i. What information is contained in the classification marking?

Classified Information Act
Article 17
Every classified information or every document containing classified information shall be marked with the level of classification and the information about the agency, unless otherwise obvious.
The markings from the preceding paragraph shall be used in a manner appropriate to the kind and characteristics of the medium.
A piece of information or a document shall be treated as classified even if it is marked only with the level of classification.
The Government of the Republic of Slovenia shall prescribe in detail the methods and forms of marking the classification of information or documents.

The Decree on the protection of classified information states:
Article 3
(Marking of classified information)
Any written documents, including books and brochures and their reproductions, shall have their classification level marked in their heading and foot on every page of the document, including the external side of the front cover, if any.
Article 4
(Marking)
(1) When assigned the appropriate classification level, each document and medium shall be visibly marked with markings in compliance with the preceding Article.
(2) All documents or media classified SECRET and TOP SECRET shall also bear the following data in addition to the markings defined in the preceding paragraph:
– the copy number of the document, and
– the number of any annexes.
(3) Any documents classified TOP SECRET shall be marked by a red line at least 4 millimetres thick, extending diagonally at an angle of 45 degrees at a distance of four centimetres from the top right corner of the page, in addition to the markings prescribed in the preceding Article.
(4) Classification level markings shall be clearly distinguished from other inscriptions and shall use bold block lettering for the

inscriptions, which must be larger than the letters used in the remaining inscriptions.
(5) The classification level markings referred to in this Article are indicated in the RESTRICTED, CONFIDENTIAL, SECRET and TOP SECRET marking samples, listed in Annex I hereof, and shall form an integral part of this Decree."

ii. Is a separate classification marking needed for each section of a document?

Please check one: ☒ Yes ☐ No

k. Is the identity of the person responsible for a classification decision indicated on the document, or otherwise easily traced, to ensure accountability? *[Principle 14b, 22b]*

Please check one: ☒ Yes ☐ No

l. Does classified information lose its classified status if it becomes widely available in the public domain?

Please check one: ☐ Yes ☒ No

If you checked "Yes", please explain how the declassification of information based on its availability in the public domain is triggered in practice:

m. Can information be classified if it originated in the public domain?

Please check one: ☐ Yes ☒ No

If you checked "Yes", please explain under what circumstances:

4. Declassification Procedures

a. When information is classified, does the classifier specify a time (date or event) that triggers the declassification of the information? *[Principle 18b]*

Please check one: ☒ Yes ☐ No

b. What is the maximum duration of classification? Can this time period be extended? *[Principle 18c]*

There is no legally prescribed maximum of duration. However, the classification of information terminates on a specified date, with the advent of a specified event, with the expiry of a specified time period or with declassification.
Where, due to the nature or content of information, the termination as set out in the preceding paragraph cannot be applied, classification shall terminate with the expiry of the time period laid down in the law governing archival materials and archives -> that is, as a rule, 40 years after the creation.

c. May information ever be classified indefinitely (in law or in practice)? *[Principle 18c]*

Please check one: ☐ Yes ☒ No

d. Are decisions to classify information reviewed periodically to ensure that the original reason for the classification is still valid? *[Principle 14a]*

Please check one: ☒ Yes ☐ No

If you checked "Yes", how often are classification reviews performed?

An authorised person shall check TOP SECRET classified information once a year, whereas the remaining levels of classification only every three years and shall assess whether the need for the classification of information still exists.

e. What is the procedure for requesting the declassification of documents?

Access to Public Information Act
Article 6
(4) If the applicant 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.

Article 21 holds that when the applicant requests a withdrawal of the classification according to the fourth paragraph of Article 6 the matter is, based on the suggestion of the representative of the authority, decided on by the:
- Government, when the body liable is a government administration body, public prosecutor's office, attorney general's office, entity of public law, the founder of which is the state, public powers holder or public service contractor on a state level;
- Supreme Court, when the body liable is a court;
- Council of local self-governing community, when the body liable is a body of local self-governing community, entity of public law, the founder of which is a self-governing community, public powers holder or public service contractor on a local self-government level.
- The body itself, when not one of the bodies stated in the previous indents.

The applicant has the right of appeal against this decision, the matter is decided on by the Information Commissioner.

Classified Information Act
Article 15
(3) Declassification of information may be requested by a person whose request for classified information has been turned down.
(4) The request from the preceding paragraph shall be decided on by the director of the agency concerned.

f. Can declassification requests be made by the public? *[Principle 19d]*

Please check one: ☒ Yes ☐ No

g. Does the law consider the public's interest in the disclosure of information when deciding whether to declassify information? *[Principle 19a]*

Please check one: ☒ Yes ☐ No

If you checked "Yes", please explain, in the terms provided by the law, what consideration is given to the public's interest:

Classified Information Act
Article 21a
Where the director of an agency considers, in accordance with the law governing access to public information, that justification of the prevailing public interest for disclosure should be assessed in connection with the request for access to public information relating to a piece of information determined as classified, he shall submit a proposal to the Government.
The Government shall decide on the justification of access to the piece of information referred to in the previous paragraph on the basis of the provisional opinion of the Commission.

Should the Government decide that the public interest concerning the disclosure is stronger than the public interest for limited access to the piece of information due to its confidentiality, it shall order the agency that classified the piece of information to declassify the classified piece of information. The agency shall declassify information no later than 15 days after the day it received the decision of the Government referred to in this paragraph and shall acquaint the applicant with the information.

5. Categories of Information that are Classifiable

a. Does the law list specific categories of information that may be classified on national security grounds?

Please check one: ☒ Yes ☐ No Cite: Article 5 of the Classified Information Act

If you checked "Yes":

i. What categories of information are included in this list? *[Principle 9]*

"a piece of information may be defined as classified if it is so important that its disclosure to unauthorised persons could or might obviously prejudice the security of the country or its political or economic interests, and is related to:
1. public security;
2. defence;
3. foreign affairs;
4. the intelligence and security activities of Government agencies of the Republic of Slovenia;
5. systems, appliances, projects and plans of importance to the public security, defence, foreign affairs and intelligence and security activities of Government
6. scientific, research, technological, economic and financial affairs of

importance to the public security, defence, foreign affairs and intelligence and security activities of public authorities.

ii. Is this list exhaustive?

Please check one: ☒ Yes ☐ No

b. Does the law prohibit any categories of information from being classified?

Please check one: ☒ Yes ☐ No Cite: Article 6 of the Classified Information Act

If you checked "Yes", please identify which categories: *[Principle 10]*

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.

In particular, does the law prohibit classification of:

i. human rights violations

Please check one: ☒ Yes ☐ No

ii. government corruption

Please check one: ☒ Yes ☐ No

iii. the existence of a government entity

Please check one: ☐ Yes ☒ No

iv. the budget or expenditures of a government entity

Please check one: ☐ Yes ☒ No

v. the existence of a law (or portion of a law)

Please check one: ☐ Yes ☒ No

vi. emergency response plans

Please check one: ☐ Yes ☒ No

If you checked "Yes" to any of the above, please provide additional detail:

Article 6 should be interpreted broadly. Even though it is not expressly mentioned in the Act the existence of a law could not be classified.

6. Review of a Denied Request for Information

a. Is there an opportunity for a speedy, low-cost review of a denied request for information by an independent authority? *[Principle 28a, 3e]*

Please check one: ☒ Yes ☐ No

b. Is there an opportunity for judicial review of a denied request for information? *[Principle 28a, 3e]*

Please check one: ☒ Yes ☐ No

7. <u>Judicial Proceedings</u>

a. Do courts have the authority to examine classified information that the government seeks to keep secret on national security grounds? *[Principle 29b]*

Please check one: ☒ Yes ☐ No

If you checked "Yes":

i. May a judge order the release of information if s/he determines that the information does not need to be kept secret, despite a public authority's assertion that national security justifies withholding the information? *[Principle 29d]*

Please check one: ☒ Yes ☐ No

ii. Do judges normally defer to the public authority's assessment that disclosure would harm national security? *[Principle 29c]*

Please check one: ☒ Yes ☐ No

b. Are judicial decisions required, according to the law, to be made available to the public (subject to redactions to protect privacy interests)? *[Principle 31b]*

Please check one: ☒ Yes ☐ No

If you checked "Yes":

i. May national security justify withholding part of a court decision?

Please check one: ☒ Yes ☐ No

ii. May national security justify withholding an entire court decision?

Please check one: ☐ Yes ☒ No

c. Are court hearings and trials presumptively open to the public? *[Principle 31c]*

Please check one: ☒ Yes ☐ No

d. Can a court case ever be kept entirely secret, such that it is not even recorded on the court's public docket? *[Principle 31b]*

Please check one: ☐ Yes ☒ No

e. Must all evidence that forms the basis of a criminal conviction be made available to the public? *[Principle 31c]*

Please check one: ☐ Yes ☒ No

What, if any, exceptions exist on the basis of national security?

Evidence is never automatically made public, it is available only to those who show a legitimate interest and to the convicted person. However, even for persons with interest, inspection and copying of individual criminal files may be refused if this is necessary on special

grounds of defense or national security or if the public was excluded from the trial. The appeal against such decision is possible, but it does not suspend the measure.

f. Must all evidence that forms the basis of a criminal conviction be shown to the accused, including in cases involving national security? *[Principle 32]*

Please check one: ☒ Yes ☐ No

If you checked "No":

i. What limitations exist on the disclosure of information to the accused on the basis of national security?

ii. What information, if any, must be provided to the accused in lieu of the classified evidence?

iii. Are there other safeguards to protect the accused's right to a fair trial? (*e.g.*, Can the accused hire special counsel who have access to all of the classified evidence, pursuant to security clearance?)

g. May the government refuse to disclose information to the opposing party in any of the following court proceedings, on the basis of national security?

i. A *habeas corpus* claim

Please check one: ☐ Yes ☒ No

ii. A claim of grave human rights violations (*e.g.*, torture) brought against a public authority *[Principle 33a]*

Please check one: ☐ Yes ☒ No

iii. A tort claim brought against a public authority *[Principle 33a]*

Please check one: ☐ Yes ☒ No

If you checked "Yes" for any of the above, please indicate what safeguards, if any, are in place to protect the fairness of the proceeding.

h. Can a judge dismiss a case, without reviewing the case on its merits, because reviewing the case would involve state secrets? *[Principle 29a]*

Please check one: ☐ Yes ☒ No Cite:

8. Autonomous Oversight Bodies

a. Is there an autonomous oversight body with authority to review classification decisions by security sector, defence, and intelligence agencies? *[Principle 34a]*

Please check one: ☒ Yes ☐ No

If you checked "Yes":

i. Identify the body. What are its mandates and powers? *[Principle 34a, 35]*

The Information Commissioner of Slovenia (see above & Article 21 and 27 of the Access to Public Information Act: https://www.ip-rs.si/index.php?id=324)

ii. What, if any, limitations are there on this body's ability to review classified information? *[Principle 7, 34b, 34c, 35]*

The Information Commissioner has, in connection with the discharge of her/his functions, access to classified information without permission to access. Employeed of this institution may aquire permission to access classified information in accordance with the Classified Information Act.

b. Can the public make requests for access to information held by the autonomous oversight body? *[Principle 36a]*

Please check one: ☒ Yes ☐ No

9. <u>Whistleblower Protections</u>

a. May public personnel who have authorized access to classified national security information be subject to criminal penalties if they disclose that information to the public? *[Principle 46]*

Please check one: ☒ Yes ☐ No <u>Cite</u>:

Article 260 of the Criminal Code (http://www.wipo.int/clea/docs_new/pdf/en/si/si045en.pdf)

If you checked "Yes":

i. What is the maximum penalty for this crime?

- imprisonment for not more than three years;
- imprisonment for not more than five years if the disclosure was committed out of greed or with a view to publishing or using the information concerned abroad;
- imprisonment for not more than one year if the offence has been committed through negligence

ii. What must the government prove in order to obtain a conviction?

- that the offence was commited by an official or any other person who had a duty to protect classified information
- that the perpetrator in non-compliance with his duties to protect classified information, communicated or conveyed information designated as classified information to another person, or otherwise provided him with access to such information or with the possibility of collecting such information in order to convey the same to an unauthorised person
- criminal intent or negligence

iii. Does the law take the public's interest in the disclosure of the information into consideration when deciding whether to penalize the disclosure? *[Principle 46b]*

Please check one: ☐ Yes ☒ No

If you checked "Yes":

1) Who bears the burden of proof in regard to whether the disclosure was in the public interest?

2) What factors must be present to meet this burden?

iv. Is a showing of either actual or probable harm to national security, resulting from the disclosure, required in order for a penalty to be imposed? *[Principle 46c]*

Please check one: ☐ Yes, actual ☐ Yes, probable ☒ No, neither

If you checked "No", is it a defence or mitigating circumstance that the disclosure did not harm national security?

Please check one: ☐ Yes ☒ No

v. Is it a defence or mitigating circumstance that the personnel making the disclosure had used, or tried to use, internal reporting procedures before making a disclosure to the public? *[Principle 46c]*

Please check one: ☐ Yes ☒ No

If you checked "Yes", what constitutes adequate exhaustion of the internal procedures?

vi. Is it a defence or mitigating circumstance that the personnel had a good faith belief that using the internal reporting procedure would be ineffectual, or would result in retaliation?

Please check one: ☐ Yes ☒ No

vii. Are there other defences or mitigating circumstances?

Not really, but there ia s general rule in the Criminal Code that could be used if the circumstances would allow it (eg the person did not know that information was classified):
Mistake of Fact
Article 30
(1) The perpetrator who, at the time of the committing of a criminal offence, was not aware of a statutory element of such an offence, shall not be held liable under criminal law.
(1) A criminal offence shall be deemed to be committed as a mistake of fact if the perpetrator at the time of committing of a criminal

offence was not aware of a statutory element of the circumstances, or he erroneously believed that the circumstances were present which, if they were true, would justify his conduct.
(3) For a criminal offence committed out of negligence, the guilt of the perpetrator shall not be excluded if he was in error regarding the circumstances, which he should and could have been aware of within the limits of required carefulness.

b. Have any public personnel been charged with a crime for disclosing classified national security information in the past two decades? *[Principle 46]*

Please check one: ☐ Yes ☐ No

If you checked "Yes":

i. Approximately how many prosecutions have there been?

No data available.

ii. Approximately how many convictions have there been, and what punishments were imposed, if any?

No data available.

If you checked "No", have any personnel been investigated or otherwise threatened with government sanction as a result of disclosing classified national security information in the past two decades?

Please check one: ☐ Yes ☐ No

If you checked "Yes", please explain what happened:

c. Do laws protect "whistleblowers" who disclose certain categories of classified information pertaining to government wrongdoing?

Please check one: ☒ Yes ☐ No Cite: Article 6 of the Classified Information Act.

If you checked "Yes":

i. What categories of information are covered by the whistleblower protection laws? *[Principle 39]*

Article 6 of the Classified Information Act.
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.

Do the protected categories vary depending on whether the information is disclosed publicly, internally, or to a designated independent body?

Please check one: ☐ Yes ☒ No

If you checked "Yes", please identify the type of disclosure that is protected for each listed category.

ii. Do these whistleblower protections apply to whistleblowers in the security sector, defence, and intelligence agencies?

Please check one: ☒ Yes ☐ No

iii. How do the protections afforded to whistleblowers in the security sector, defence, or intelligence agencies differ from whistleblowers in other government sectors, if at all?

/

d. Are public personnel prosecutable if they disclose classified national security information, in making a complaint *internally*, to someone within their own ministry, department, or unit, even if not a direct supervisor? *[Principle 39-41]*

Please check one: ☒ Yes ☐ No

e. Is there an *independent* body, expressly designated to receive complaints involving classified information from public personnel? *[Principle 42]*

Please check one: ☐ Yes ☒ No

If you checked "Yes":

i. Are public personnel prosecutable if they disclose classified national security information to the designated independent body? *[Principle 34d]*

ii. Must such personnel complain internally before approaching the independent body?

f. Are public personnel encouraged to make internal disclosures when they encounter information about government wrongdoing?

Please check one: ☐ Yes ☒ No

If you checked "Yes":

i. How are internal disclosures encouraged? *[Principle 47]*

ii. Do public personnel have a duty to disclose information of governmental wrongdoing to an internal or designated independent body? *[Principle 39]*

iii. What criminal, civil, and/or administrative penalties, if any, are there for retaliation (*e.g.*, firing, demotion, harassment) against personnel

who provide information concerning governmental wrongdoing to an internal or designated independent body? *[Principle 44]*

g. Are there criminal penalties for the unauthorized *possession* of classified information by a person who had authorized access to that information? *[Principle 50a]*

Please check one: ☐ Yes ☒ No

If you checked "Yes", do whistleblower protections apply to unauthorized possession of information?

Please check one: ☐ Yes ☐ No

10. <u>Media Protections</u>

a. May a person who does *not* have authorized access to classified national security information (such as a journalist) be subject to criminal penalties for disclosing this information to the public? *[Principle 50b]*

Please check one: ☒ Yes ☐ No <u>Cite</u>: Art. 260, Para 2 of the Criminal Code

If you checked "Yes":

i. What is the maximum penalty for this crime?

Imprisonment for not more than three years.

ii. What must the government prove in order to obtain a conviction?

The prosecution must prove:
- obtaining or publishing classified information with the intention of using it without authority

(The provision of the Criminal Code states: "Whoever, with the intention of using it without authority, obtains information protected as classified information or publishes such information publicly, shall be punished to the same extent." = imprisonment for not more than three years)

iii. Does the law take the public's interest in the disclosure of information into consideration in deciding whether to impose a penalty?

Please check one: ☐ Yes ☒ No

i. Who bears the burden of proof in regard to whether the information that was disclosed was in the public interest?

/

ii. What factors must be present to meet this burden?

/

iv. Is a showing of actual or probable harm to the national security, resulting from the disclosure, required in order for a penalty to be imposed?

Please check one: ☐ Yes, actual ☐ Yes, probable ☒ No, neither

If you checked "No", is it a defence or mitigating circumstance that the disclosure did not harm national security?

Please check one: ☐ Yes ☒ No

v. What other defences are available?

- no criminal intent (only negligence);
- mistake of fact (conviction, that the information is not classified);
- coercion;
- the information was really not classified in accordance with the provisions of the Act;
- information was classified in order to cover up a criminal offence, the exceeding or abuse of authority, or some other unlawful act or behaviour (such information is not considered to be classified).

b. Have any members of the media (journalists, editors, publishers, etc.) been charged with a crime for publishing government secrets in the past two decades? *[Principle 50b]*

Please check one: ☒ Yes ☐ No

If you checked "Yes":

i. Approximately how many times have charges been brought?

No data available

ii. Approximately how many convictions have there been, and what punishments were imposed, if any?

No data available

If you checked "No", have any member of the media been investigated or otherwise threatened with government sanction as a result of publishing government secrets in the past two decades?

Please check one: ☐ Yes ☐ No

If you checked "Yes", please explain what happened:

c. Are there criminal penalties for the *possession* of classified information by a person who did not have authorized access to that information (such as a journalist)? *[Principle 50a]*

Please check one: ☒ Yes ☒ No Cite:

If you checked "Yes":

i. What is the maximum penalty for this crime?

ii. What must the government prove in order to obtain a conviction?

iii. What are the defences?

d. May the government compel a member of the media to reveal a confidential source in the interests of national security? *[Principle 51]*

Please check one: ☒ Yes ☐ No

e. May the government prevent the media from publishing information on the basis of national security? *[Principle 52]*

Please check one: ☒ Yes ☐ No

If you checked "Yes":

i. What information must the government provide to justify a prior restraint on publication?

Such prevention is only possible in criminal proceedings - the prosecution must prove that, for example, a journalist obtained classified information with the intention of using it (elements of a criminal offence). If documents are needed as proof, they may be confiscated.

ii. To whom must this information be provided?

f. May the government prevent or sanction the dissemination of information even after that information has entered the public domain (*e.g.*, having been published on the Wikileaks website)?

Please check one: ☒ Yes ☐ No

If you checked "Yes", please explain what is required for the government to prevent or sanction dissemination of this information:

See above.

11. Record Maintenance

a. Is there a duty to archive classified documents? *[Principle 17]*

Please check one: ☒ Yes ☐ No

If you checked "Yes", does the duty to archive classified documents apply to the security sector, defence, and intelligence agencies?

Please check one: ☒ Yes ☐ No

b. Under what circumstances is classified information permitted to be destroyed? *[Principle 49]*

Classified information may only be destroyed under the conditions of the Decree on the protection of classified information, which states that when destroying classified information:
- the director of the agency or the person duly authorized by the director of the agency shall appoint at least a three-member commission for the destruction of classified information that shall include a person in the agency responsible for the protection of classified information;
- every agency shall, after the performed annual review of the received classified information, remove and, if necessary, destroy all classified information received for information purposes;
- reference number, date and classification level of the destroyed item of information contained on the original shall be entered in the record on the destruction of classified information
- the agency that assigned the level of classification shall be informed in writing on the destruction of information classified TOP SECRET.
- to the rest of classified information that are part of the current or permanent document database, the regulations governing document management by the public administration bodies shall be applied.

If classified information are archived under the provisions of Protection of Documents and Archives and Archival Institutions Act, they are kept permanently.

i. May classified information ever be destroyed before becoming declassified?

Please check one: ☒ Yes ☐ No

ii. What oversight is involved in the decision to destroy classified information?

Inspection proceedure of the Inspectorate of internal affairs.

iii. Are there certain categories of information that are not permitted to be destroyed (*e.g.*, information pertaining to human rights violations or corruption)?

Please check one: ☐ Yes ☒ No

If you checked "Yes", please indicate which categories of information are not permitted to be destroyed:

Note: If archived, classified information may not be destroyed at all.

c. Is each public authority that classifies information required to maintain a list of classified documents that it holds? *[Principle 16]*

Please check one: ☒ Yes ☐ No

If you checked "Yes":

i. What information must be included in this list?

There is no special rule for classified information, however, each public authority must keep a record of all documents emerging from its administrative operations.

ii. What information from this list, if any, must be made available to the public?

There is no rule regarding that. Such a record may be made available to the public if it is not itself classified or contain other exemptions from free access to public document (Article 6 of the Access to Public Information Act).

Sources: To the extent not already provided, please cite the key laws and regulations that provide the legal framework for allowing, and controlling, public access to information, including national security information. If you are aware of any useful secondary materials, please cite these resources as well. Please also note any significant case law or examples, exemplifying or contradicting the draft Principles.

Additional comments? (optional)

Follow-up questions for Rosana Lemut-Strle – SLOVENIA

1. For question (1)(b)(ii), are there any categories of information that are absolutely exempt from disclosure on the basis of national security? Or can the non-disclosure of all information be challenged and even though falling within one of the categories, still be determined to warrant disclosure?

Data marked with the highest classification level (top secret, secret), are absolutely exempt from disclosure. Data can also be classified on the grounds of national security. The data in this case can be disclosed only with the termination of classification (on a specified date, with the advent of a specified event, with the expiry of a specified time period, with declassification).

2. For question (9)(b), even though official statistics may not be available, please answer to the best of your knowledge, whether any personnel have been charged with a crime for disclosing classified national security information in the past two decades, and if so, approximately how many were convicted and what punishments were imposed. If not, please also indicate whether you are aware of any such persons being investigated or otherwise threatened with government sanction.

In the last twenty years in Slovenia we had three cases of criminal proceedings for disclosing classified information (to my knowledge). None ended with conviction. One was opened against the current Prime Minister (he was presumably acquainted with the recording of a meeting of presidents of parliamentary parties – when he was not authorized to be), second against MP (he presumably released classified information on the type of armaments used in the Slovenian Army) and third against two journalists (they supposedly published classified information from the court file).

3. For question (9)(c), do the protections afforded to whistleblowers in the security sector, defence, or intelligence agencies differ from the protections afforded to whistleblowers in other government sectors? If so, how?

Special protection of whistleblowers is not enacted. Article 6 of Classified Information Act applies to all, regardless of the sector they belong to. According to the cited Article an information shall not be considered as classified if it 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.

4. For question (10)(b), even though official statistics may not be available, please answer to the best of your knowledge, approximately how many members of the media have been charged in the past two decades for publishing government secrets, approximately how many were convicted, and what punishments were imposed, if any.

See the answer to the 2nd question.

5. For question (10)(c), please indicate what the maximum penalty is for possession of classified information by a person who did not have authorized access to that information. Please also indicate what the elements of this crime include and what potential defences may be raised against such a charge.

Article 260 (par II) of the Criminal Code Act says: Whoever, with the intention of using classified information without authority, obtains information protected as classified information or publishes such information publicly, shall be sentenced to

imprisonment for not more than three years.

If the offence has been committed out of greed, the perpetrator shall be sentenced to imprisonment for not more than five years.
If the offence has been committed through negligence, the perpetrator shall be sentenced to imprisonment for not more than one year.

Elements of criminal acts are possession or publication of classified documents. One might argue that such conduct was in the public interest, but the question is how successful one would be in this claim. The most recommended defense would be reliance on the Art 6 of Classified Information Act by claiming that there was no classified information (because it was designated as such for the sole purpose of covering up a criminal offence, the exceeding or abuse of authority, or some other unlawful act).

6. For question (10)(f), please explain in more detail how the government may prevent or sanction the dissemination of information obtained from the public domain. What criminal chares can be brought? Could these charges be brought against a journalist who disseminated information obtained on the Wikileaks website?

Government has no mechanism to prevent the publication of classified information. When it comes to it, government can initiate criminal proceedings. During the criminal procedure government may require destruction of objects with which the offense was committed (eg, newspapers, if the information was published in them), of course, this is inefficient when it comes to publishing on the Internet. Here the government has the same option as anyone else - asking the ISP to withdraw the document, citing the illegality of published content.