REGIONAL CONSULTATION ON
NATIONAL SECURITY AND THE RIGHT TO INFORMATION

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

Country analysed:

The Netherlands

Expert analyst:

Name of person completing this form:

Wouter Hins

Institutional or organizational affiliation:

Universiteit Leiden

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:

      State security

   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]*

      The law does not give a definition. Legal authors refer to the remit of the two national intelligence services 'AIVD' and 'MIVD', which are defined in articles 6 and 7 of the Act on the information and security services (Wet op de inlichtingen- en veiligheidsdiensten). Key elements are the maintenance of the democratic legal order and the efficient functioning of the military force..

      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:

The general Freedom of Information Act (Wet openbaarheid van bestuur) is not applicable in cases that are governed exclusively by another Act of parliament. An example is the disclosure of information that is processed by or on behalf of the intelligence services AIVD and MIVD. Disclosure of such information is governed by chapter 4 of the Act on the intelligence and security services (Wet op de inlichtingen- en veiligheidsdiensten).
The Freedom of Information Act also does not apply in cases that are governed by an international treaty that commands secrecy. Information about the events in Srebrenica, where Dutch forces had operated as part of the United Nations Protection Force UNPROFOR, could not be disclosed because the Convention on the Privileges and Immunities of the United Nations (1946) was applicable.

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?

Chapter 4 of the Act on the information and security services allows disclosure if there is no possibility of danger to State security. Under the Convention on the Privileges and Immunities of the United Nations (1946) the UN Secretary-General can allow disclosure.

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:

The Freedom of Information Act (FOIA) is only applicable to authorities of the executive branch of governent as defined in the General Act on administrative law. Parliament and the judiciary are exempt. In additon, some executive authorities also fall outside the scope of the General Act on administrative law and, therefore, the FOIA. For example, the Dutch Review Committee on the Intelligence and Security Services is explicitly excluded in article 1:1, paragraph 2 under h, of the General Act on administrative law. Therefore the FOIA is not applicable either.

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?

There is an exception to the exception. Auhorities that are excluded from the scope of the General Act on administrative law neverteless fall under this act when they take decisions concerning their relation

with a civil servant in their service. However, in relation to the FOIA this exception to the exception seems of little relevance.

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 Dutch Review Committee on the Intelligence and Security Services publishes Annual Reports. See the website http://www.ctivd.nl/?English

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?

In cases where confirming or denying the existence of a file would give insight in the working methods of an intelligence service and thus endanger the security of the State.

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 duty to specify the number of pages withheld, but if the interest of State security is sufficiently served by anonymising the requested document or by giving a resumé, the government should do so. The decision must explain why the complete document could not be given.

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]*

It is sufficient to convince the judge, e.g. by giving him the requested document confidentially, with the permission of the applicant. Naturally, this confidential information is not provided to the public. If the applicant refuses his consent, the judge will often find in favour of the government.

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 general FOIA says: 'as soon as possible, but ultimately within four weeks'. The authority can extend this term with another four weeks. The special Act on the intelligence and security services (Wet op de inlichtingen- en veiligheidsdiensten) has a much longer term. Article 51 of this Act says: 'as soon as possible, but ultimately within three months'. The competent Minister can extend this term with another four weeks.

3. Classification Procedures

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

Please check one: ☒ Yes ☐ No Cite:

Besluit voorschrift informatiebeveiliging rijksdienst - bijzondere informatie, Staatscourant 2004, 47 (a ministerial regulation)

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

Information is a State secret when the interests of the State or its allies are at stake and taking cognizance of the information by unauthorized persons might cause harm to these interests. Cf. Explanatory Memorandum to the Besluit voorschrift informatiebeveiliging rijksdienst - bijzondere informatie, Staatscourant 2004, 47

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:

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:

There are three levels of State secrecy: 1. Very secret 2. Secret and 3. Confidential (Article 5, paragraph 1, of the Besluit voorschrift informatiebeveiliging rijksdienst - bijzondere informatie, Staatscourant 2004, 47)

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

The classification is determined by the person that authorizes the document (Article 7, paragraph 2, of the Besluit voorschrift informatiebeveiliging rijksdienst - bijzondere informatie, Staatscourant 2004, 47). The classification authority may not be delegated. For each Ministry a Secrecy Officer supervises the classification procedures (Article 14).

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?

There is no such duty in general, but sometimes secrecy follows from a specific regulation, e.g. the Act on nuclear energy (Kernenergiewet).

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?

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?

The marking indicates the time during which the classification is valid. In addition, it may proscribe a specific treatment of the information. For example, the Ministry of Defence uses the marking 'NL/GE eyes only' for information that may be shared with Germany only (Article 5, paragraph 3, of the Besluit voorschrift informatiebeveiliging rijksdienst - bijzondere informatie, Staatscourant 2004, 47)

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]*

10 years (Article 6, paragraph 1, of the Besluit voorschrift informatiebeveiliging rijksdienst - bijzondere informatie, Staatscourant 2004, 47). Extension is possible in the circumstances described in Article 6, paragraph 2..

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?

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

There is no specific procedure for requesting the declassification of documents. However, everyone can submit a request under the FOIA, which will lead to reconsidering the legitimacy of maintaining secrecy.

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:

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: Specific laws, such as the Act on the intelligence and security services and the Act on nuclear energy.

If you checked "Yes":

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

Intelligence information, technological data about nuclear processes, etc.

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: Freedom of Information Act

If you checked "Yes", please identify which

categories: *[Principle 10]*

> The FOIA states that all documents in the possession of an administrative authority, as defined in the General Act on administrative law, are open to the public, subject to certain restrictions. If the security of the State cannot be at stake, disclosure should not be refused under that pretense.

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:

> The answers given are rather speculative, because it is the administrative court - interpreting the FOIA - that ultimately decides whether or not State security 'can' be at stake. However, it seems very unlikely that the court will allow the concealing of human rights violations or government corruption.

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. Judicial Proceedings

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?

Article 365, paragraph 5, of the Code of Criminal Procedure states that trial documents that are not attached to the judgment, will not be disclosed to the public. Therefore, there is no need for an exception based on national security.

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.

The answers given are rather speculative. The court will have to balance the conflicting interests, with due regard to the case law of the European Court of Human Rights.

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: Article 13 of the Act on general provisions (Wet Algemene bepalingen 1829)

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 Dutch Review Committee on the Intelligence and Security Services. See the website http://www.ctivd.nl/?English

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

The Committee has access to all relevant information of the intelligence and security services and may hear all the staff of the services. Furthermore the Committee has the right to hear witnesses (under oath) or experts. Finally, it may access all places which it deems necessary in the context of its task, with the exception of dwellings. The competences of the Committee are laid down in the articles 74 up to and including 77 of the Intelligence and Security Services Act (WIV) 2002.

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>: Articles 98-98c Criminal Code

If you checked "Yes":

i. What is the maximum penalty for this crime?

Under Article 98a, paragraph 1, the maximum is 15 years imprisonment. If the crime was committed in time of war, the maximum is imprisonment for life (paragraph 2).

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

As to Article 98a Criminal Code:
The secrecy of the information must be vital in the interest of the State or its allies. The suspect must have known or could reasonably have expected that the information had this character. The disclosure must be have been intentional.

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?

The Criminal Code itself does not mention this justification. However, under article 94 of the Dutch Constitution, Acts of Parliament, such as the Criminal Code, cannot be applied when this would violate a self-executing treaty. Therefore, the

suspect can submit that his conviction would violate Article 10 of the European Convention on Human Rights.

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

The factors mentioned in the case law of the European Court of Human Rights, such as ECHR (GC) 12 February 2008, Guja vs Moldova, par. 73-78.

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?

The first step is to report the wrongdoing to his superior, who informs the competent authority. If the civil servant does not agree with the decision of the authority or if this authority does not respond within eight weeks, he can address an independent advisory commission, the Commission integrity of government (Commissie integriteit overheid). The commission tenders an advice to the competent authority who finally decides what shall be done.
Cf. Staatsblad 2006, nos. 129 and 130

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?

A mitigating circumstance might be that the independent Commission shared the view that there was a case of serious wrongdoing, but the competent authority did not follow up this advice.

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?

Only a few.

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

Only a few. A recent case is a Supreme Court decision of 29 November 2011, which can be found on www.rechtspraak.nl under LJN no. BU6207. A former employee of the secret service was convicted on the basis of article 98c Criminal Code, that prohibits the possession of classified security information. The case started after the newspaper De Telegraaf appeared to have a copy of this document. The final verdict was one year and eleven months imprisonment.

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: No laws, only the direct effect of Article 10 ECHR

If you checked "Yes":

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

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]*

No

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

Yes, in principle. However, when there are 'weighty reasons' the civil servant may directly approach the Commission integrity of government (Commissie integriteit overheid).

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>: Articles 98-98c Criminal Code

If you checked "Yes":

i. What is the maximum penalty for this crime?

Under Article 98a, paragraph 1, the maximum is 15 years imprisonment. If the crime was committed in time of war, the maximum is imprisonment for life.

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

As to Article 98a Criminal Code:
The secrecy of the information must be vital in the interest of the State or its allies. The suspect must have known or could reasonably have expected that the information had this character. The disclosure must have been intentional.

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?

The Criminal Code itself does not mention this justification. However, under article 94 of the Dutch Constitution, Acts of Parliament, such as the Criminal Code, cannot be applied when this infringes a self-executing treaty. Therefore, the suspect can submit that his conviction would infringe Article 10 of the European Convention on Human Rights.

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

The factors mentioned in the case law of the European Court of Human Rights, such as ECHR (GC) 10 December 2007, Stoll vs Switzerland.

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?

All defences that are relevant under Article 10 ECHR, e.g.: the journalist did not actively provoke a crime, his acting in good faith and according to the ethices of journalism, the quality of the publication etc.

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?

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

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:

Journalists of the daily newspaper De Telegraaf had been systematically observed and phone-tapped after they had published government secrets. A complaint by De Telegraaf with the European Court of Human Righst is now pending and a judgment is expected in the autumn of this year (2012). The Chamber hearing was on 19 June 2012, case number 39315/06. See the webcast of the hearing on http://www.echr.coe.int/ECHR/EN/Header/Press/Multimedia/Webcasts+of+public+hearings/webcastEN_media?id=20120619-1&lang=en&flow=high

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: Article 98c Criminal Code

If you checked "Yes":

i. What is the maximum penalty for this crime?

6 years imprisonment

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

As to Article 98c Criminal Code:
The secrecy of the information must be vital in the interest of the State or its allies. The possession must be intentional.

iii. What are the defences?

The Criminal Code itself does not mention a justification. However, under Article 94 of the Dutch Constitution, Acts of Parliament, such as the Criminal Code, cannot be applied when this would violate a self-executing treaty. Therefore, the suspect can submit that his conviction would violate Article 10 of the European Convention on Human Rights.

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?

An injunction can only be ordered by a court. The government must specify which information exactly they want to be barred. There must be weighty reasons to justify such an injunction, in accordance with Article 10 ECHR.

ii. To whom must this information be provided?

To the court..

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:

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]*

Article 5 of the Archives Law states that documents may only be destroyed on the basis of a selection list, drafted by the authority that keeps the documents. The draft selection list is approved by the Minister of Culture, jointly with the Minister who is responsible for the subject-matter. Selection lists are published in the National Gazette (Staatscourant) and can be challenged by interested parties. A Royal Decree contains more detailed rules. However, article 9 of the Archives Law states that in extraordinary circumstances the Prime Minister can allow deviation from the normal rules on destruction.

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?

One can challenge the selection list in court. The practice of destructing documents is supervised by a General Archives Inspector (Algemene Rijksarchivaris) and his staff..

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:

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?

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

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.

At first sight, Dutch law seems to lag behind the draft Principles. For example, the Criminal Code prohibits any publication of state secrets that could potentially harm the interests of the State or its allies, without paying attention to the right of the public to be properly informed. The Criminal Code makes no distinction between a disloyal employee that sells documents for a profit and a journalist who publishes a leaked document, revealing corruption in the military. The Freedom of Information Act is not applicable to documents that are kept by the supervisory committee for the secret services. Finally, the Code of Criminal Procedure states that documents that were used during a criminal trial are not open to the public.
However, the real situation in the Netherlands is not as old-fashioned as the text of the laws might suggest. The reason for this is the direct applicability of Article 10 ECHR. Courts have the power to interpret domestic law in accordance with the case law of the Strasbourg court and not apply national laws that are in conflict with a self-executing treaty like the ECHR or the ICCPR.

Finally, I mention the Dutch names of the Acts of Parliament that were quoted most in the previous paragraphs:
Wet openbaarheid van bestuur (Freedom of Information Act)
Wet op de inlichtingen- en veiligheidsdiensten (Act on the intelligence and security services).
Wetboek van Strafrecht (Criminal Code)
Wetboek van Strafvordering (Code of Criminal Procedure)
Archiefwet (Archives Law)

Additional comments? (optional)