

**REGIONAL CONSULTATION ON
NATIONAL SECURITY AND THE RIGHT TO INFORMATION**

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

Country analysed:

Germany

Expert analyst:

Name of person completing this form:

Eric Töpfer

Institutional or organizational affiliation:

Deutsches Institut für Menschenrechte / German Institute for Human Rights

Supplementary information provided by:

Nils Leopold

Institutional or organizational affiliation:

Humanistische Union

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:

According to section 3 of the Federal Act on Freedom of Information (Informationsfreiheitsgesetz 2005, IFG) access to information can be restricted for a variety of reasons listed under the heading of "protection of special public issues" (Schutz von besonderen öffentlichen Belangen).

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*]

"Special public issues" are 'defined' by a list of issues for which the release of information could have "harmful effects" (nachteilige Auswirkungen), including among others a) international relations, b) military and other security-sensitive issues of the Federal Armed Forces, c) issues of internal or external security, d) tasks of control and supervision by the authorities for finance, competition and regulation, e) issues of external finance control, f) measures for the protection against illegal external economic transaction (section 3, para 1 IFG). In addition, access to information can be restricted if the release of information might threaten "public security" (section 3 para 2 IFG). However, this does not mean that these areas are exempt from FOI requests. Rather each individual request has to be examined.

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:

Any information that was classified in accordance with legal or general administrative provisions for the protection of secrecy or confidentiality or that is subject to professional or official secrecy (section 3, para 4 IFG).
Any information of other public authorities that is only temporarily processed without the purpose of becoming part of the files of the processing authority (section 3, para 5 IFG).
Any information that was collected or transferred confidentially as long as the third party is still interested in confidentiality (section 3, para 7 IFG)

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?

According to recent case law the simply formal classification of information is not sufficient to restrict access. Rather the classification has to be justified also in substantive respect which in effect means that older classifications have to be reassessed when access to information is requested. (2nd Report of the Federal Commissioner for Data Protection and Freedom of Information 2008/2009, pp. 19-20, referring to Federal Administrative Court decisions 7 C 21.08 and 7 C 22.08)

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:

Federal intelligence services (section 3, para 8 IFG), namely the foreign intelligence agency (Bundesnachrichtendienst), the federal

domestic intelligence service (Bundesamt für Verfassungsschutz) and the military intelligence agency (Militärischer Abschirmdienst) as such are exempted from FOI requests. The Federal Police, the Federal Criminal Police Office, the Federal Armed Forces and the Customs Criminological Office are not exempted as such from FOI requests but only when it comes to their "security-sensitive tasks" according to the Security Checks Act (Sicherheitsüberprüfungsgesetz 1994, SÜG), namely functions around 1) signal intelligence in support of the federal domestic secret service, 2) cooperation with the secret services for the purposes of combating terrorism, espionage, organised crime and arms trade.

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?

According to section 11 IFG public authorities do have to publish at least organisation charts and plans how they organise their file plans in "electronic form". The law does not provide for a specific routine of updating this information. As stated above, intelligence services are exempted from any obligations to publish information. If and how the Federal Ministry of Defence, the Federal Armed Forces, the Federal Ministry of Interior, federal law enforcement agencies and other security-related authorities could justify to classify certain sections of their file plans or organisational charts referring to the exemptions lists in 1.a.i is not known.

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?

[Empty box]

- 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]

Within the limits noted above, public authorities are required to grant access to information. However, they are not required to justify a denial of access in general. They only have to provide written justification for such a denial if the request was for written or electronic administrative acts. If citizens requests for access are vague public authorities are required to provide assistance to clarify requests, according to section 25 of the Administrative Procedure Law (Verwaltungsverfahrensgesetz).

- 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]

[Empty box]

- 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]

Public authorities shall answer FOI requests within one month (section 7, para 5 IFG). Every person can lodge a complaint with the Federal Commissioner for Data Protection and Freedom of Information if he or she believes his or her right to freedom of information violated. However, the Commissioner cannot enforce time limits, he can only issue non-binding reclamations (Beanstandungen), according to section 12 para 3 IFG.

3. Classification Procedures

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

Please check one: Yes No Cite:

For federal authorities most important is the General Administrative Order of the Federal Ministry of Interior on the Material and Organisational Protection of Classified Documents (Verschlussachen-Anweisung 2006, VSA) in relation with the Security Checks Act (Sicherheitsüberprüfungsgesetz 1994, SÜG)

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

According to section 4 SÜG and section 3 VSA following levels of classification exist:

TOP SECRET ("STRENG GEHEIM"): release of information may threaten the existence or the vital interests of the Federal Republic of Germany (FRG) or one of its Länder.

SECRET ("GEHEIM"): release of information may threaten the security of the FRG or one of its Länder or cause serious damage to its interests.

CONFIDENTIAL (VS-VERTRAULICH): release of information may be harmful ("schädlich") for the FRG or one of its Länder.

CONFIDENTIAL ONLY FOR USE DURING SERVICE ("VS-NUR FÜR DEN DIENSTGEBRAUCH"): release of information may be unfavourable ("nachteilig") for the FRG or one of its Länder

- 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:

VSA does not consider the public interest in disclosure but only the "public interest in the requirement for secrecy of facts" (section 2, para 1 VSA). Annex 1 of VSA calls on responsables, "to critically examine if a classification as confidential is really necessary" but points to the effects that a classification has for other persons who have to handle such information, namely the privacy-invasive security checks they have to pass.

- 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:

see 3.b

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

Section 8 of the VSA only states that the "function issuing confidential information decides the requirement for classification and the level of secrecy" and only if this is necessary. Thus, the Order only refers to "functions" (Dienststellen / Stellen) and does not specify a level of hierarchy. However, heads of functions may issue guidelines for classification to ease administrative work and harmonise practice which at least indicates that also other administrative staff than the head of function does classify documents in daily practice. In addition, section 5 VSA states that the head of function is in charge of the proper management of confidential documents, including recognition, production, copying, administration, electronic transfer, destruction and other use. For these purposes the head of functions may delegate these tasks to other staff. In larger functions and in higher levels of the federal administration these tasks are delegated to a Protection of Secrecy Commissioner (Geheimschutzbeauftragter).

- 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?

- 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?

According to section 16 and Annex 2 of VSO, the classification markings do only display the level of confidentiality. But all

classified documents need a date and file number, the total number of pages needs to be indicated, and all pages have to paginated.

- 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:

At least the available provisions do not explicitly prohibit the classification of information originating in the public domain.

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]*

30 years, which can be extended once for another 30 years. (section 9, para 3 VSA)

- 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?

Section 9 para 1 VSA states that classification has to be revised "as

soon as the reasons for the current level of classification change or expire" but periods for revision are not prescribed.

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

informal request towards the responsible author or function

- 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:

If you checked "Yes":

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

- 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:

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

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:

--

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 (answer provided by Nils Leopold)

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 (answer provided by Nils Leopold)

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 (answer provided by Nils Leopold)

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

Section 99 para 2 of the law of administrative court proceedings allows for an "in camera" proceeding so that the principle of publicity of court files as stated in section 100 para 1 is partially abandoned

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 (answer provided by Nils Leopold)

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 (answer provided by Nils Leopold)

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

Please check one: Yes No (answer provided by Nils Leopold)

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

Please check one: Yes No (answer provided by Nils Leopold)

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.

according to section 99 para 2 of the law of administrative court proceedings there has to be a formal decision of the court for admission which can be contested

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 19 para 4 of the German constitution

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 Federal Commissioner for Data Protection and Freedom of Information may examine citizens' complaints against administrative decisions to deny access to information. The Commissioner can issue non-binding opinions and publish reclamations if an administrative decision to withhold classified information is deemed to violate the FOI Act.

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

possible limitations apply regarding files under the security clearance act (SÜG)

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

Please check one: Yes No (answer provided by Nils Leopold)

9. Whistleblower Protections

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 Cite:

- for treason (Landesverrat) according to section 94 of the Penal Code;
- for publication of national secrets (Offenbaren von Staatsgeheimnissen), according to section 95 of the Penal Code;
- for the violation of official secrets and a special duty for secrecy

(Verletzung des Dienstgeheimnisses und einer besonderen Geheimhaltungspflicht), according to section 353b of the Penal Code

If you checked “Yes”:

i. What is the maximum penalty for this crime?

- For treason: not less than one year, and in "very serious cases" not less than five years with max. of "life-long sentence", i.e. 15 years of prison.
- For publication of national secrets: max. five years of prison
- For violation of official secrets: max. five years of prison or financial penalty.

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

unauthorized disclosure of respective material and endangerment of important public interest (353 b penal code)

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 (answer provided by Nils Leopold)

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 (answer provided by Nils Leopold)

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 (answer provided by Nils Leopold)

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

having followed the internal review procedure as stated in the administrative personnel laws, both federal and on Laender level which means addressing possible misbehaviour towards the next higher ranking officer (right of remonstrations)

- 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 (answer provided by Nils Leopold)

- vii. Are there other defences or mitigating circumstances?

- 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 (answer provided by Nils Leopold)

If you checked "Yes":

- i. Approximately how many prosecutions have there been?

there have been approx. 200 prosecutions acc. to section 353 b penal code

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

not known

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:

(answer provided by Nils Leopold)

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 (answer provided by Nils Leopold)

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

Please check one: Yes No (answer provided by Nils Leopold)

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 (answer provided by Nils Leopold)

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]

no

- 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]

none, see above (right to remonstrate/ complain provides protection)

- 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 (answer provided by Nils Leopold)

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

Please check one: Yes No

10. Media Protections

- 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 Cite:

Only in 2012 the Penal Code was amended (section 353b para 3a) to release journalists from the risk of being charged for aiding and abetting the "violation of official secrets" (see above) in case of publishing secret information. However it is still a crime to instigate a violation of official secrets for journalistic purposes.

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. 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
(answer provided by Nils Leopold)

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?

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 (answer provided by Nils Leopold)

If you checked “Yes”:

i. Approximately how many times have charges been brought?

presumably not more than a two-figure number since the overall number of charges for 353 b penal code was just 200. 17 persons were charged in 2007 for revealing secret service information but the accusations were dropped

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

only overall 28 convictions after 353 b of the penal code indicate that the unlikelihood that there was any conviction, there was no case ever made public

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:
(answer provided by Nils Leopold)

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 (answer provided by Nils Leopold)

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

Please check one: Yes No (answer provided by Nils Leopold)

If you checked “Yes”:

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

- 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 (answer provided by Nils Leopold)

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]*

Federal authorities "do offer" the Federal Archive their classified documents that are not required any more for archiving in the secret archive. If the Federal Archive does not archive the documents the classified information has to be destroyed. (sections 26, 27, 28 VSA) According to section 2 of the Federal Archive Act (Bundesarchivgesetz) federal authorities "have to offer" all documents not needed any more to the Federal Archive, and if these documents are considered to be of "lasting value for research and understanding of German history, for securing justified interests of citizens, or for the provision of information for legislation, administration or jurisdiction" they have to be handed over to the Federal Archive. The assessment whether documents are of "lasting value" is a decision made by the Federal Archive and the relevant federal authority.

- 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?

There is no specific oversight over decisions to destroy classified information but at least it has to be documented which documents have been destroyed when, and by whom the decision was taken. These information have to be signed by a witness. (section 28, para 3 VSA)

- 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.

--

Additional comments? (optional)

It is important to mention that only eleven of the 16 German states (Länder) have adopted freedom of information acts. The existence or non-existence of such acts are of particular relevance when it comes to police agencies and the domestic secret services at the Länder level but it was impossible to cover the individual provisions at the Länder level as well. However, a brief look at the Länder acts shows that access to information is restricted for the purpose of protecting "special public issues" in most cases.

==

A few brief remarks:

1) It is very important to note, that most of the information that I provided do only relate to the federal level and the relevant authorities! Similar provisions on classification procedures exist in the 16 German states, and eleven states have their own freedom of information acts but they might differ when it comes to the details. I could not check how much they differ. Thus, in particular the 16 domestic secret services are not covered by my answers to the questionnaire. Only the info on whistleblowing and media protection are applicable for both the federal and the state level as the scope of the Penal Code is nation-wide.

2) Regarding Number 7 on "judicial proceedings" where I did not find appropriate tick-boxes and space to explain the situation: Only the Federal Administrative Court can examine classified information of which the status is challenged by FOI requests in an in camera trial and assess public authorities' assertions whether this information is to be kept secret. Lower layers of the administrative court system are not authorized to do so. The verdict is not secret. However, the judges of the Federal Administrative Court may not refer to the content of the documents at stake. I was a bit surprised when I suddenly read about "criminal convictions" as I thought we are talking about FOI requests. Thus, I did not provide answers here.

3) Regarding Number 8 on "autonomous oversight bodies": The Federal Commissioner for Data Protection and Freedom of Information - Citizens can lodge complaints against administrative decisions to deny FOI requests with the Commissioner. However, I am not sure if and how the Commissioner's staff is entitled to assess the documents at stake. Though the FOI Act makes reference to the inspection rights of the Federal Data Protection Act I did not come across any information confirming that the Commissioner and staff have examined classified information themselves. However, the Commission does not have to power to declassify information. S/he can only issue a non-binding opinion and - sharpest sword - send a reclamation to the authority which is later published in the biannual report.

Follow-up questions for Eric Töpfer – GERMANY

1. When a public authority receives a request for information, may it ever refuse to acknowledge whether or not such information is even in its possession? If so, when?

Beyond the agencies and areas that are excluded from the scope of the Federal Freedom of Information Act (*Informationsfreiheitsgesetz*) no public federal authority may refuse to acknowledge whether information is in its possession, they may only deny access to information in certain cases. FOI Act Commentaries even suggest that section 7 FOI Act in relation with section 25 of the Administrative Proceedings Act (*Verwaltungsverfahrensgesetz*) provides for an obligation to guide citizens who can only vaguely formulate their request for information to the relevant information.

However, in practice public authorities may simply ignore requests, and it might require lengthy legal action to enforce access rights.

2. Can a judge dismiss a case, without reviewing the merits of the case, because reviewing the case would require consideration of state secrets?

No.

3. May a court case ever be kept entirely secret, such that it is not even recorded on the court's public docket?

According to sections 172 and 174 of the Constitution of Courts Act (*Gerichtsverfassungsgesetz*) the public can be excluded from trials when national security is at risk. In such cases media must not publish reports about the trial and about the content of relevant official documents. All persons present during such trials can be ordered by court to keep the details secret.

Another form of secret court proceedings were introduced in the 1990s by an amendment of the Administrative Courts Order (*Verwaltungsgerichtsordnung*, VwGO). Since then section 99 VwGO regulates 'in camera trials': in case that federal authorities refuse to submit documents to proceedings in administrative courts as this would allegedly harm the welfare of the Federal Republic or a German state, the opposing party may order an in camera trial reviewing the documents at stake to be held at the Federal Administrative Court. The opposing party is excluded from the in camera trial, all participants have to keep the details secret and the final verdict must not refer to kind and content of the classified documents.

However, the cases may not be kept entirely secret. Court verdicts are public documents in any case.

4. When handling a case that involves information that is classified on the basis of national security, will a judge normally defer to the public authority's evaluation regarding the sensitivity of the information?

This is an empirical question, and I do not have an overview about the actual outcomes of trials involving classified documents.

5. Can an accused ever be denied access to evidence that forms the basis of his conviction because the information is classified on grounds of national security? If so, what safeguards are there to ensure the fairness of the proceedings?

No, when we talk about criminal proceedings. But the defense lawyer can be excluded from trial if his or her participation might pose a risk to national security, according to section 138b of the Code of Criminal Procedure (*Strafprozessordnung*)

But when persons aims to contest administrative actions or decisions, for instance, their observation by secret services, they have to take the avenue of administrative law which means that the in camera trials mentioned above may come into play.

6. Are there any laws protecting “whistleblowers” who disclose classified information pertaining to government wrongdoing?

No laws protecting “whistleblowers” in general exist. Only specific sections in sectoral laws justify, for instance, the disclosure of information about cases of corruption in public administration (section 38 para 2 of the amended Public Servants Status Act, *Beamtenstatusgesetz*; and similarly the *Dienstrechtsneuordnungsgesetz* 2008)

7. In deciding whether to criminally penalize someone for disclosing national security information, does the court consider whether there was either actual or probable harm to the national security resulting from the disclosure?

Section 353b para 1 and 2 of the Penal Code states that those who reveal official secrets and “thereby threaten important public interests” will be penalised by prison term or punitive fine.

Similarly, sections 94 (and 95) of the Penal Code address a) the intention to cause harm to the Federal Republic of Germany and b) the outcome of the disclosure of national secrets (“thereby cause the threat of serious harm for external security”)

Thus, I would say that the actual or potential threat to important public interests should be considered by court.

8. In deciding whether to criminally penalize someone for disclosing national security information, does the court consider whether there was a public interest in having the information disclosed?

No general answer possible as the law is not explicit about this.

9. Are you aware of any people having been charged with a crime for disclosing classified national security information in the past 20 years? If so, please explain very briefly what happened in these cases.

According to the Police Crime Statistic published by the Federal Criminal Police Office on an annual basis, from 1998 to 2011 each year more than 100 cases (ranging from 130 in 1998 to 307 in 2009) of breaches of “official secrets” (*Dienstgeheimnisse*) according to section 353b of the Penal Code (*Strafgesetzbuch*) are registered. According to the same statistic in 2000 37 cases of treason and causing risks for national security were registered. Since then the statistic does not list the number of treason cases. I do not know to whom the classified information have been

disclosed in these cases and if they persons involved were eventually prosecuted and sentenced as the crime statistic only counts crimes investigated by the police.

The only specific case of which I am aware of is the search of the editors' office of the journal CICERO in 2005 in the wake of the publication of an article quoting classified documents (level "confidential") on finance networks of Islamist terrorism originating in the Federal Criminal Police Office. The editors' were charged with aiding the breach of official secrets, and the search aimed at identifying the source in the Federal Criminal Police Office. Eventually the regional court refused to open a trial due to lack of suspicion, and a constitutional complaint against the search of the editors' office was accepted by the Federal Constitutional Court, declaring that the search was illegal. But it is unknown if the source has been identified and if yes what happened to him or her.

10. Is there any kind of independent body where public personnel can bring complaints concerning classified information?

As already stated in my replies to the questionnaire, complaints against decisions of federal authorities to deny access to classified information can be lodged with the Federal Commissioner for Data Protection and Freedom of Information. The Commissioner can, however, only issue a non-binding opinion or reclamation (*Beanstandung*) based on their assessment of the case. In many cases authorities might defer to such reclamations as they are published in the biannual report to the Federal Parliament and might entail critical questions. But authorities are not obliged to as citizens' complaints to the Commissioner are not instruments of legal redress. Thus, the only independent institutions where the classification of documents could be reviewed are administrative courts.

11. Do public personnel have either a legal or professional duty to make internal disclosures when they encounter information about government wrongdoing?

In case that they know about the preparation or committing of crimes listed in section 138 Penal Code they are obliged to report these crimes as any other citizen. However, they are not obliged to report other kinds of "wrongdoing".

12. Can public personnel be prosecuted for disclosing classified national security information internally within their own ministry, department or unit?

Section 353b of the Penal Code refers to "revealing" official secrets in general without defining or limiting the reach of disclosure.

13. Is it a criminal offense for public personnel to have unauthorized possession of classified national security information? What about for members of the public to have unauthorized possession of classified national security information?

The unauthorised possession of "national secrets" (*Staatsgeheimnisse*) and the attempt to get in possession of national secrets is a criminal act, if done with the intention to disclose the information, according to section 96 of the Penal Code.

Aiding the "breach of official secrets" (*Dienstgeheimnisse*), according to section 353b para 1 Penal Code, is illegal when done by persons who are not journalists. However, as a "breach of official secrets" means the disclosure of information including the

effect of threatening important public interests, it might be debatable whether the simple possession of official secrets by members of the public is a criminal act.

14. May the government compel a member of the media to reveal a confidential source in the interests of national security?

No, journalists' rights to refuse to give evidence are guaranteed by section 53 of the Code of Criminal Procedure. In addition, the Federal Constitutional Court has confirmed the protection of journalists' sources in several cases as a cornerstone of press freedom.

15. May the government ever prevent the media from publishing classified national security information? If so, how?

In its landmark SPIEGEL-Decision the Federal Constitutional Court clarified that "journalistic treason", according to section 97 of the Penal Code, can be penalised under certain circumstances but if and how this is possible has to be decided on a case-by-base basis: "Here [when balancing press freedom and state security] it has to be considered on an individual basis the relevance of disclosed facts both for the potential enemy and the political judgement of the people; the threat against national security that may result from publication have to be balanced against the requirement to be informed about important developments in the area of security policy." (Federal Constitutional Court Decision BVerfGE 20, 162)

16. Once classified national security information has been published in the public domain, may the further dissemination of that inform be sanctioned?

No.

Additional comments

In addition, one important clarification which was highlighted by a colleague today. In criminal trials defense lawyers may be excluded from trial when they pose a threat to national security, as I have written in my answers. But this does not mean that the prosecuted person cannot appoint another defense lawyer; only the contested person has to be changed.

Follow-up questions for Nils Leopold – GERMANY

1. For question number (7)(h) ("Can a judge dismiss a case, without reviewing the case on its merits, because reviewing the case would involve state secrets?"), you have checked both Yes and No. I suspect, since you cite the German constitution, that you meant only to check No. Is that correct?

Correct, it is a No.

2. In regard to questions (9)(b) and (10)(b), do I understand correctly that Section 353ba applies both to public personnel who disclose classified national security information and other persons (who did not have authorized access to that information but otherwise come upon it) who disclose this information?

Correct, prosecutions are possible regarding all personnel engaged in handling public service "secrets". Journalists can become involved either by aiding and abetting (which was abandoned most recently) or by instigating the public disclosure of these secrets.

And that in the last 20 years, there have been 200 charges, but only 28 convictions, under this section?

SORRY, that figure was just in 2010.

But that it is not possible to determine (without a close case study) how many were public personnel and how many were other persons who somehow gained access to the information without authorization? But that you suspect the 28 convictions were most likely all public personnel, since there has not been any news otherwise?

Yes, because we have no knowledge of journalists which are the only "external group" outside public service that could be covered by this foreskrift actually being convicted

And, in any event, in 2012, the provision was revised to exclude the possibility of prosecuting journalists? I also take it that we know at least 17 who were not public personnel were charged in 2007, but that the charges against these people were dropped.

Is all of that correct, or have I misunderstood anything?

Well, you can still get journalists for instigating a 353 b. That is why my party presented an alternative draft regulation also dropping the possibility of charging for instigating. Unfortunately we did not succeed in parliament.

3. In denying a request for information, is a public authority required to provide written reasons for the denial?

No, this has not been regulated. But in cases of denial there is an explicit right to go to court, see Art. 9 para 4 of the federal FOI-Law. So by filing a suit you can force an explanation

4. What requirements, if any, are there for a public authority to describe information responsive to a request that it withholds? (e.g., do they have to indicate the amount withheld or the category?)

The requirement will derive from general administrative procedure law. So yes, in case that information is being withheld there should be an abstract description of what is being withheld. Limits to this of course in cases where even this mere info would fulfill the definition of the exception clause which justifies withholding the info.

5. What information or documentation must support an assessment that disclosure would cause harm to national security? Is this information provided to the public?

As you might already know in German administrative courts the instrument of "in-camera-procedure" offers the possibility to open up possible proof or documentation. Art 99 para 2 of the German administrative court procedure law regulates this. There is an ongoing discussion whether this article can be applied to FOI-laws but some courts have already decided to do so

6. Does the duty to archive classified documents apply to the security sector, defence, and intelligence agencies?

Any public authority is obliged to keep documentations according to the specific regulations of each sector

7. Is each public authority that classified information required to maintain a list of classified documents that it holds? If so, what information is contained in this list? Is any of the information in this list made available to the public?

To my knowledge there has to be list which does not hold any more info than dates and level of classification, size and responsible officer carrying out the classification.

Each public authority according to an internal administrative regulation has to keep a list

8. Regarding the 200 prosecutions of people who publicly disclosed information.

I'd be interested to know more about those prosecutions since it's such a startling number. Did most of them relate to the 1989 changes? And were they all public disclosures? What kind of info was disclosed? How many convictions? Would a person be likely to be prosecuted, and convicted, today for disclosing classified info to the media which he reasonably believed showed that serious human rights violations or crimes had been, or were likely to be, committed?

Any information you can provide would be a great help. Among the other countries surveyed, the highest number of prosecutions reported over the past 20 years was about a dozen. Otherwise, there were only one or two cases, so Germany stands out as the exception.

Please do not work with those figures regarding penalties for disclosure of government secrets. Our statistics never indicate a real prosecution but simply the fact that there was an investigation being started, no more, no less. I know of not a single journalist actually having been charged and prosecuted, there probably are only a few top spies, who where prosecuted after 89. The fact that we have like up to 200 cases of investigations a year has a number of reasons, amongst them intensified

investigations around police corruption, but also cases of secret committee disclosures or data protection/ data security investigations. The whole thing covers all kinds of disclosures and is by no means focused on human rights violation disclosures. We have an ongoing discussion whether the leading article 353 b of our penal code is actually worthless because all investigations seem to be in vain. As I have explained before the loophole of using the disclosure regulation via aiding and abetting in order to search offices etc. has been closed due to regulation two years ago.