REGIONAL CONSULTATION ON
NATIONAL SECURITY AND THE RIGHT TO INFORMATION

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

Country analysed:

Sweden

Expert analyst:

Name of person completing this form:

Iain Cameron

Institutional or organizational affiliation:

Law Faculty, Uppsala University

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:

      Rikets säkerhet (security of the realm) is used in Sweden, but I will in this questionnaire use the term national 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]*

      Not defined in the Public Access to Information and Secrecy Act 2009:400 (PAIS Act) or other legislation. Crimes against national security are defined in the Criminal Code. International relations is a separate category of secret information under PAIS and so there is no need to interpret national security widely to encompass this. In the travaux preparatoires to the former Secrecy Act (1980:100) it is stated that defence secrecy covers all the different activities which are of significance to the defence of the country, not simply purely military components of defence but also such matters as the economic aspects of defence preparedness, essential supplies for the civilian population, and psychological defence (prop. 1979/80:2 Del A s. 132). The term "total defence" is defined in section 1 of the Act on Total Defence as activities which are necessary to prepare Sweden for war. In the travaux preparatoires it is stated that civil defence encompasses all the preparations for armed conflict which inter alia civil authorities take in peacetime and all the preparations during armed conflict which are necessary to support the defence forces, protect and save life, maintain essential supplies and important societal functions ((prop. 1994/95:7 s. 50 f.).

      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:

There are several categories of information which are to be kept secret for reasons of national security, but no category is totally "exempt" from disclosure. However, there is a persumption of secrecy of regarding certain national security information; eg police intelligence files (PAIS Act 18:2) and regarding information on people collected in the course of military/signals intelligence operations (PAIS Act 38:4). This presumption can be rebutted.

ii. Is exemption of these categories absolute?

Please check one: ☐ Yes ☒ No

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

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

Please check one: ☐ Yes ☒ No

If you checked "Yes":

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

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

Please check one: ☐ Yes ☐ No

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

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

Please check one: ☐ Yes ☒ No

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

Please check one: ☒ Yes ☐ No

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

The Security Police publish an annual report, as do the oversight bodies monitoring the police/security police and the signals intelligence organisation.

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?

All authorities are required to maintain publicly accessible registers of all official information, however, there are exceptions for inter alia military, signals and security police intelligence registers (PÄIS Act 5:3 and 5:4, PAIS Ordinance section 2).

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 a general duty on administrative authorities to motivate a decision (Administration Act, sections 20 and 21), but an exception applies if this is necessary with regard to national security.

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]*

As regards official information covered by secrecy provisions which an individual requests access to and which is denied by reference to the secrecy, the extent of the motivation given, and the extent to which this is made available to the individual in question will depend upon the circumstances. A simple reference to the legislation may be

the only motivation given to the individual. As regards very secret information (eg is there a file on a given person), it may be that even confirmation of its existence or non-existence would itself damage national security. All decisions are, however, capable of being appealed against, ultimately to the courts. As regards favouring disclosure, this is the general rule, see answer to 3.a below but see also answer to 1.b above.

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]*

No set time limits. The Administration Act section 7 requires all administrative decisions affecting individuals to be taken as speedily as it is possible to do, without thereby risking legal security. The Ombudsman monitors this.

3. Classification Procedures

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

Please check one: ☒ Yes ☐ No Cite:

The detailed guidelines regarding classification used by the government, the security police, the defence forces and the signals intelligence organisation are not available. Classification has only an administrative function, warning people handling the information to show special care in this. It does not determine the issue of whether the information is, in fact, entitled to be kept secret. Public access to all information is the rule and secrecy the exception. Thus, the public interest in disclosure is built into the system of disclosure, but is not (necessarily) a factor in the classification decision. And there is no possibility to (or need for) appeal against a classification decision.

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

Each administrative authority has its own routines for classification of official information as secret. Most often, classification is done by the desk officer responsible for receiving or drafting the document in question. When access is requested to a particular document, these requests tend to go through a specialist official, who contacts the desk officer responsible for having drafted, or received, the document in question, to discuss and determine whether or not it can be released.

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:

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

Generally speaking, the authority in possession of the information. This authority also decides applications from individuals to have access to this information. However, an exception exists for information of considerable significance to national security, where the government can specify that only a certain authority, or a certain group within the authority, may decide on such applications (PAIS Act 15:3, PAIS Ordinance section 1).

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?

Excessive classification can draw criticism from the Ombudsman or even, in theory, prosecution for misuse of office. In practice however, prosecutions for any form of misuse of office are very rare. Reasons for classification - albeit brief - must be given to the courts if and

when an individual requests access to the information, and a negative decision is taken which is then appealed to the administrative courts.

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 words "secrecy classification" and a reference to the authority which took the decision to classify and the date.

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:

On the same basis as other information which is to be kept secret, eg topological information can be classified. There appear to be differences of opinion amongst the leading authorities as to whether systematic gathering of publicly available information (eg military port traffic) can mean that the information becomes secret (contrast Ulväng et al, p. 247 with Axberger, p. 262). See also RÅ 1989 ref. 111 and JO 2001/02 s. 478. But it is clear that this - if it applies at all - would be very exceptional. In general, a great deal of personal information given voluntarily to administrative authorities (eg on a patient's health) can be said to originate in the "public domain". A special rule applies to inventions made by private companies or individuals which are of significance to national security (Act on Defence Inventions, 1971:1078). These can be classified.

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]*

Forty years (PAIS 15:2). Yes if there are exceptional reasons the government may prescribe a longer period (150 years for certain military information of long-duration, 70 years for intelligence information, PAIS Ordinance section 4)..

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?

See g below.

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:

It is not possible to appeal against the classification as such. Instead, the appeal is that the information does not, in fact, fall under one of the exceptions in the law on freedom of information and so, is not, in fact, secret. The court has to determine if the information genuinely should be kept secret or not, and thus takes into account this particular individual's interests in obtaining the information.

5. Categories of Information that are Classifiable

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

Please check one: ☐ Yes ☒ No Cite:

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

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?

See Code of Judicial Procedure 5:1. If information subject to secrecy is to be provided or adduced at a court hearing, the court may generally hold a hearing behind closed doors (in camera). However, in the general courts (district/city courts, courts of appeal and the Supreme Court) strong reasons are usually required to be able to hold a hearing in camera. The possibilities for holding hearings in camera are greater in administrative courts (county administrative courts, courts of administrative appeal and the Supreme Administrative

Court) than in the general courts. If a court hearing has been held in camera, the court may impose a duty of confidentiality on those who have been in attendance. If secret information is presented in open court, the secrecy for the information as a main rule ceases to apply

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?

PAIS 10:3 para. 1 allows keeping information secret if this is of particular importance (synnerlig vikt).

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

PAIS 10:3 para. 2 specifies that secrecy can never apply for a judgment or a decision. Nor may secrecy limit a party's rights under the Code of Judicial Procedure to have access to information on all the factors which are of significance to the decision or judgment. This is not the same as having access to all documentation underlying the decision or judgment.

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?)

Special counsel do not exist in Swedish procedural law, except as regards proceedings to grant warrants for interception of communications and bugging.

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.

See PAIS 10:3 in (g) above. See also Administration Act section 20.

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

Please check one: ☐ Yes ☒ No Cite:

8. Autonomous Oversight Bodies

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

Please check one: ☐ Yes ☒ No

If you checked "Yes":

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

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

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

Please check one: ☐ Yes ☒ No

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:

If you checked "Yes":

i. What is the maximum penalty for this crime?

Aggravated revealing of very secret national security information (CC 18:8) 4 years imprisonment, otherwise 2 years (revealing CC:18:7) or six months (grossly careless revealing CC 18:9). Revealing of otherwise secret information (CC 20:3) 1 year.

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

Intent and actus reus depend on how the offences are fomulated. obehörig befattning med hemlig uppgift" (unauthorised dealing with secret information, CC 18:7,8,9) means "A person who, without intent to aid a foreign power, without authority obtains, transmits, gives or reveals information concerning matters of a secret nature, the disclosure of which to a foreign power can cause harm to the defence of the Realm or to the maintenance of necessary supplies to the people during war or during extraordinary conditions caused by war, or otherwise to the security of the Realm". The court must therefore determine if the information in question can cause the requisite harm.

According to case law, NJA (Nytt Juridisk arkiv, Supreme Court Reports) 1988 s. 118, this should mean information of real significance.
For the aggravated offence of unauthorised dealing with secret information 4 years imprisonment, otherwise 2 years (ordinary offence) or six months (offence committed through carelessness). Revealing of otherwise secret information (CC 20:3) means "A person who discloses information which he is duty-bound by Law or other statutory instrument or by order or provision issued under a Law or statutory instrument to keep secret, or if he unlawfully makes use of such secret, he shall, if the act is not otherwise specially subject to punishment, be sentenced for breach of professional confidentiality to a fine or imprisonment for at most one year. A person who through carelessness commits an act described in the first paragraph shall be sentenced to a fine. In petty cases, however, punishment shall not be imposed."

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 right of access to all official information is the rule. However, both "yes" and "no" are misleading answers, as the prosecution need show that the information falls properly within the exception and that "damage" to national security has ocurred.

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

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

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

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

Please check one: ☐ Yes ☐ No

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

Please check one: ☐ Yes ☒ No

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

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

Please check one: ☐ Yes ☒ No

vii. Are there other defences or mitigating circumstances?

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?

A few, perhaps one every two years. Usually the issue has been negligent handling of secret information.

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

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: TF 1:1

If you checked "Yes":

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

There is a "right" to leak "ordinary" secret information to the press. Leaking of "qualified" secret information is a criminal offence (for a person who has a duty to keep this secret), but made deliberately difficult to investigate. There are no limits on investigation of the leaking of very secret national security information, but this category of information is very limited.

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.

Only leaking to the press is protected.

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?

There is more qualified secret information and very secret national security information in these sectors, meaning that the room for whistleblowing is less. But most defence and police information will still fall under the ordinary secrecy protection (CC 20:3).

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

Please check one: ☒ Yes ☐ No

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

Please check one: ☐ Yes ☒ No

If you checked "Yes":

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

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

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

Please check one: ☐ Yes ☒ No

If you checked "Yes":

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

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

iii. What criminal, civil, and/or administrative penalties, if any, are there for retaliation (*e.g.*, firing, demotion, harassment) against personnel who provide information concerning governmental wrongdoing to an internal or designated independent body? *[Principle 44]*

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

Please check one: ☒ Yes ☐ No

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

Please check one: ☒ Yes ☐ No

10. <u>Media Protections</u>

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

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

If you checked "Yes":

i. What is the maximum penalty for this crime?

See 9.a.i

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

See 9.a.ii

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?

For the crimes of revealing very secret security information, the prosecution must show that "damage" to national security has occurred.

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

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

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

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

Please check one: ☐ Yes ☐ No

v. What other defences are available?

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:

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

Please check one: ☒ Yes ☐ No Cite:

If you checked "Yes":

i. What is the maximum penalty for this crime?

See 9.a.i and ii

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

See 9.a.i and ii. Information has to be of real significance in order to

fall under the crime of "obehörig befattning med hemlig uppgift". Most defence and police information will only fall under the ordinary secrecy protection (CC 20:3).

iii. What are the defences?

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

Please check one: ☒ Yes ☐ No

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

Please check one: ☐ Yes ☒ No

If you checked "Yes":

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

ii. To whom must this information be provided?

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

Please check one: ☒ Yes ☐ No

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

Government may never prevent dissemination of information, but in principle may prosecute for revealing secret national security information which has previously entered the public domain. However, in most such cases, the courts would be likely to rule that no further damage to national security has occurred by the subsequent publication, and so acquit.

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]*

Archives Act 1990:782, section 10 allows destruction, however, sufficient material must be retained for the purpose of the public's right of access to official documents, to the need for administration and the courts and for the purpose of research (section 3).

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?

Security and Integrity Board monitors security police data banks.

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.

JO 1995/96:29, Axberger, H.G, Tryckfrihetens gränser, Liber, 1984. Ulväng, M, Jareborg, J, Friberg, S, Asp, P., Brotten mot allmänheten och staten, Iustus, 2012, Bring, T., Sekretss i brottsbekämpande och dömande verksamhet, Norstedts, 2012.

Additional comments? (optional)

1.d If a company or individual has been by law delegated authority to exercise public power, it is covered by PAIS. If an administrative authority determines that an

individual or company may be given secret information, it can do so subject to a condition that this information not be revealed. Thus, the individual or company can, with its consent, be made subject to PAIS.
7.a Courts most often agree with the assessment of the security police that information should be kept secret. The Supreme Administrative Court has annulled a judgment of a lower court on the basis that it did not examine the information itself and make an objective assessment of whether or not information should be kept secret but simply accepted the reasons given by the security police (mål nr 4123-07, 12 Mars 2008)
8. There is an autonomous oversight body, with competence to oversee certain aspects of the work of the Security Police, the Security and Integrity Board. This can review security screening decisions, but not decisions to classify documents. It exercises a general supervision over security police files, particularly personal information in these files.
9.g Information has to be of real significance in order to fall under the crime of "obehörig befattning med hemlig uppgift". Most defence and police information will fall under the ordinary secrecy protection (CC 20:3) and there is no penalty for simply possessing this information, or even, for a journalist or another person who does not have a duty to keep it secret, for publishing this information.
10.a.iii Where secret information has been revealed, and there is a public interest in it being revealed, the public interest in disclosure will be taken into account in determining whether "harm" to the nation has ocurred.
10.d Journalists can be compelled to reveal their sources only as regards very secret information i.e. that falling under the crimes of espionage or of "obehörig befattning med hemlig uppgift". This has not happened in the last thirty years.

Follow-up questions for Iain Cameron – SWEDEN

1. For question (2)(f), can the authority to classify information be delegated to subordinate officers, or is it limited to heads or bodies or specified authorities?

Normally, the classification decision is taken by the desk officer responsible for dealing with the specific matter in question. Only a small category of classification decisions are taken by higher authority.

2. For question (4)(d), are decisions to classify information reviewed periodically to ensure that the original reason for the classification is still valid? If so, how often are classification reviews performed?

No. As already explained, the Swedish system is not built around classification, which is a purely administrative measure. Whenever a request is made by a journalist or member of the public for access to a specific document, the official who receives the request must decide whether the document should be released or not in accordance with the criteria set out in the law, notwithstanding whether or not it has been classified. Thus, a "review" is performed, whenever a request is made. Eg a decision can have been made to classify a document but for reasons which are only valid for a very short period. The first time a request is received for access, the official can determine that the reasons for not releasing outweigh the reasons for releasing. The next time, some weeks or months later, the same or another official can determine the opposite.

3. For question (5)(b)(i-vi), do I understand correctly that Swedish law does not prohibit the classification of human rights violations, government corruption, the existence of a government entity, the budget or expenditures of a government entity, the existence of a law, or emergency response plans?

The law is not constructed in the way that there is a wide competence to refuse access, conditioned by absolute prohibitions on the classification of human rights violations, government corruption, the existence of a government entity, the budget or expenditures of a government entity, the existence of a law, or emergency response plans. Instead, these factors would be weighed into the decision on whether or not to release on request. Information eg indicating a HR violation might well be classified properly for foreign policy reasons but when a request is made for its release, the public interest in release is seen to be stronger. An example here is the Swedish ambassador's opinion that Egyptian authorities had, in fact, tortured the two people deported by Sweden to Egypt during the "war against terror", contrary to the assurances they had given Sweden. This, like most diplomatic correspondence with a potential to damage good foreign relations, was classified by the Swedish foreign office. But when the parliamentary committee on the constitution, and journalists, requested to see it, it was released to them.

4. For question (7)(h), you have indicated that a judge may not dismiss a case without reviewing it on its merits because the case involves state secrets. Is there any law that specifically states this?

Security reasons are not listed in the Code of Judicial Procedure (42:18) as justifying dismissing a case without a hearing.

5. For question (9)(b)(ii), approximately how often have prosecutions of public personnel for disclosing classified national security information resulted in convictions? What punishments have been imposed?

No convictions to my knowledge.

6. For question (10)(a)(iii)(ii), how is the burden of showing that "damage" to national security has occurred lifted? Is such a showing required in cases involving secret (but not "very secret") information? Given your answer to question (3)(e) (that the law does not specify levels of classification), what makes some information "very secret"?

It is not lifted. The prosecution must prove it, where it is an element of the offence, which is the case inter alia for espionage and aggravated and ordinary revealing of very secret national security information in CC 19 [I may have written CC 18 in my reply – if so, please correct this]. Whether or not there is a "damage" criterion for "ordinary" secret information depends on how the specific provision in OSL is formulated. The difference between "very secret" and secret is not a formal difference: it is simply that, according to both the travaux preparatoires and case law, only a very limited category of secret information is regarded as being sufficiently important to be covered by the relevant paragraphs in CC 19. The legal basis for punishing the revealing of all other secret information is OSL in conjunction with CC 20:3.

7. For question (11)(c), what information must be included in the list of classified documents that each classifying authority holds? Is any information from this list required to be made available to the public?

In principle, the titles of all documents must be registered. There are criteria determining at which stage a "document" comes into being. For certain highly secret bodies, such as the military intelligence agency, the signals intelligence agency, the security police – and the independent oversight bodies established to monitor these – the register itself can be kept secret from the public (but not the oversight body).