

# **National Security and the Right to Information in Europe**

**Amanda L. Jacobsen**  
**April 2013**

**University of Copenhagen, Department of Political Science,  
Centre for Advanced Security Theory**

## Table of Contents

### **Introduction**

### **Sources of Information**

#### **I. National Security Exceptions to the Right to Information**

- a. The Definition of “National Security”*
- b. A Presumption in Favor of Secrecy*
- c. Exemption of Certain Information, Offices or Officials*

#### **II. Disclosure Obligations**

- a. The Right to Information*
- b. Affirmative Disclosure Obligations*
- c. Time Limits for Responding to Requests for Information*
- d. Requests for Classified Information*
- e. Segregation of Non-exempt Information*
- f. Confirming or Denying the Existence of Requested Information*
- g. Written and Substantiated Explanations for Denied Requests for Information*
- h. Review of Denied Requests for Information*

#### **III. Classification Procedures**

- a. Classification Rules*
- b. Classification Levels and Markings*
- c. Classification Authority*
- d. Classification Duties*

#### **IV. Declassification Procedures**

- a. Time Limits on the Duration of Classification*
- b. Periodic Classification Reviews*
- c. Automatic Declassification*
- d. Requests for Declassification by the Public*

#### **V. Classifiable Information**

- a. Consideration of the Public Interest in Disclosure during Classification*
- b. Classification of Information in the Public Domain*
- c. Categories of Classifiable Information*

#### **VI. Judicial Review**

- a. Authority of the Court to Review and Order the Release of Classified Information*
- b. Public Access to Court Decisions*
- c. Public and Defendant Access to Evidence in Criminal Cases*
- d. Access to Information in Other Proceedings*

*e. Dismissal on the Basis of the State Secrets Privilege*

**VII. Autonomous Oversight Bodies**

**VIII. Criminal Prosecutions of Public Personnel**

- a. Criminal Penalties for Unauthorized Disclosure*
- b. Disclosures Made Internally or to an Independent Oversight Body*
- c. Information in the Public Domain*
- d. Defenses against Criminal Penalties*
- e. Criminal Penalties for Disclosure by Persons without Authorized Access*
- f. Criminal Penalties for Unauthorized Possession*

**IX. Whistleblower Protections**

**X. Media Protections**

- a. Prior Restraints on Publication*
- b. Media Privileges*
- c. Prosecution of the Media*

**XI. Record Maintenance**

- a. The Duty to Archive and the Duty to Destroy*
- b. Oversight of Document Destruction*
- c. Maintenance of Classified Document Lists*

**Annex A:** *National Questionnaire from the European Consultation on National Security and the Right to Information*

**Annex B:** *February 2012 Draft of the Principles on National Security and the Right to Information (which accompanied the National Questionnaire)*

## **Introduction**

This report was commissioned by the Centre for Advanced Security Theory (CAST) at the University of Copenhagen's Department of Political Science. The objective of the report is to identify trends within Europe related to national security and the right to information by surveying national laws and practices within the region.

This report was undertaken in connection with the Open Society Justice Initiative and seeks to inform its ongoing efforts, together with 15 other organizations and academic centres and in consultation with leading UN and regional experts, to develop a set of Global Principles on National Security and the Right to Information. More information about that project may be found at the Justice Initiative's website: <http://www.right2info.org/exceptions-to-access/national-security>.

This report is based upon information collected from national security and transparency experts from twenty European countries who completed an extensive questionnaire (attached at Annex A). The questionnaires for each of the twenty countries, although not attached to this report, may also be found at the Justice Initiative's website. The questionnaire took outset in an early draft of the Global Principles (attached at Annex B) and covered a broad cross-section of security and transparency issues addressed by the draft Principles.

After completing the questionnaire, the experts consulted for this report were convened in Copenhagen, Denmark on 20-21 September 2012, along with approximately thirty other regional and national experts, for a regional consultation on this topic. This event, which was co-hosted by the Justice Initiative and the Centre for European Constitutionalization and Security (CECS) at the University of Copenhagen's Faculty of Law, was one in a series of regional and national consultations hosted by the Justice Initiative and its partner organizations.

A special thanks is owed to the national experts who completed the questionnaire, regarding the laws and practices in their states. These experts were chosen, in part, for their unique ability to address a range of issues related to national security and transparency. The twenty European countries included in this study were chosen with the aim of providing a representative sample of current national laws and practices within the region, including both Eastern and Western Europe. In selecting these countries, consideration was given to the countries' international and regional influence, reputation for best practices, and emerging law in this field.

## **Sources of Information**

The following experts were consulted in preparing this report and completed the attached national questionnaire.

### ***Albania***

*Illir Gjoni*, Albanian Parliament, National Security Committee

### ***Belgium***

*Frankie Schram*, Professor, KU Leuven, Public Management Institute; University of Antwerp, Faculty of Political and Social Science

### ***Czech Republic***

*Oldřich Kužílek*, Otevřená společnost o.p.s., Open Society Foundations

### ***Denmark***

*Pernille Boye Koch*, Associate Professor in Constitutional Law, University of Southern Denmark

### ***France***

*Bertrand Warusfel*, Professor of Law, University of Lille2 (Paris)

### ***Germany***

*Eric Töpfer*, Researcher Reporting to the European Union Agency for Fundamental Rights, German Institute for Human Rights

*Nils Leopold*, Board of Directors, Humanistische Union; Officer, Data Protection Commission

### ***Hungary***

*Adam Foldes*, Executive Director, Transparency International of Hungary

### ***Italy***

*Arianna Vendaschi*, Associate Professor of Comparative Public Law, University of Bocconi

### ***Netherlands***

*Wouter Hins*, Associate Professor of Constitutional and Administrative Law, University of Amsterdam; Professor of Media Law, Leiden University

### ***Norway***

*Ole Henrik Brevik Førland*, Norwegian Parliamentary Intelligence Oversight Committee

### ***Moldova***

*Viorel Cibotaru*, Director, European Institute for Political Studies of Moldova

***Poland***

*Adam Bodnar*, Secretary, Helsinki Foundation for Human Rights

***Romania***

*Codru Vrabie*, Steering Committee Member, Freedom of Information Advocates Network

***Russia***

*Ivan Pavlov*, Chairman, Freedom of Information Foundation

***Serbia***

*Marko Milošević*, Researcher, Belgrade Centre for Security Policy

***Slovenia***

*Rosana Lemut Strle*, Deputy Information Commissioner of Slovenia

***Spain***

*Susana Sánchez Ferro*, Associate Professor of Constitutional Law, Autònoma University of Madrid

***Sweden***

*Iain Cameron*, Professor of Public International Law at Uppsala University.

***Turkey***

*Yaman Akdeniz*, Professor of Law, Human Rights Law Research Center, Faculty of Law, Istanbul Bilgi University

***United Kingdom***

*Adam Tomkins*, John Millar Chair of Public Law, University of Glasgow

## I. National Security Exceptions to the Right to Information

### a. *The Definition of “National Security”*

All twenty of the surveyed countries (100%) report that the public’s access to information may be restricted on the basis of national security.<sup>1</sup> Despite this seeming consensus, however, considerable variation exists among these countries regarding what, exactly, is meant by “national security.”<sup>2</sup> Foremost, there is notable inconsistency in the terminology itself, with national laws referring (often interchangeably) not only to “national security,”<sup>3</sup> but also to “state security,”<sup>4</sup> “public security,”<sup>5</sup> “public safety,”<sup>6</sup> “national defense,”<sup>7</sup> “national interests,”<sup>8</sup> “state secrets,”<sup>9</sup> and various other similar and related terms, including, *e.g.*, “security of the realm,”<sup>10</sup> “security of [the country] or its allies,”<sup>11</sup> “defense of the country,”<sup>12</sup> “national safety,”<sup>13</sup> and other “special public issues.”<sup>14</sup>

The difficulty in identifying a universal definition of national security as an exception to government disclosure obligations is compounded by the fact that in well over half of the countries surveyed, national law does not provide an express definition of national security (or the similar term) for the purpose of justifying the non-disclosure of

---

<sup>1</sup> Question (1)(a) asked: “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? Please check one: Yes / No.” *Yes* was selected for all 20 of the 20 surveyed countries: Albania, Belgium, the Czech Republic, Denmark, France, Germany, Hungary, Italy, Moldova, the Netherlands, Norway, Poland, Romania, Russia, Serbia, Slovenia, Spain, Sweden, Turkey, and the United Kingdom.

<sup>2</sup> Question (1)(a)(i) asked: “How is “national security” (or the similar term) defined for purposes of justifying non-disclosure of information?” See responses to Question (1)(a)(i).

<sup>3</sup> Question (1)(a) also asked: “If your answer refers to a similar term, please state that term here.” The experts for 17 of the 20 surveyed countries (85%) indicated that their answer to Question (1)(a) referred to a “similar term”: Albania, Belgium, the Czech Republic, France, Germany, Italy, Moldova, the Netherlands, Norway, Poland, Romania, Russia, Serbia, Slovenia, Spain, Sweden, and Turkey.

<sup>4</sup> See responses to Question (1)(a) for the Czech Republic, the Netherlands, and Russia.

<sup>5</sup> See responses to Question (1)(a) for Belgium and Slovenia.

<sup>6</sup> See responses to Question (1)(a) for the Czech Republic and Serbia.

<sup>7</sup> See responses to Question (1)(a) for France, Romania, Serbia, and Spain.

<sup>8</sup> See response to Question (1)(a) for Poland (“harm to Poland’s interest”) and Romania (“vital national/public interests”).

<sup>9</sup> See response to Question (1)(a) for Albania and Turkey.

<sup>10</sup> See response to Question (1)(a) for Sweden (“security of the realm”); *see also* response to Question (1)(a) from Italy (“security of the Republic”).

<sup>11</sup> See response to Question (1)(a) for Norway.

<sup>12</sup> See response to Question (1)(a) for Belgium.

<sup>13</sup> See response to Question (1)(a) for Serbia.

<sup>14</sup> See response to Question (1)(a) for Germany (“protection of special public issues” – where special public issues is defined to include having harmful effects on international relations, military and other security sensitive issues, internal or external security, finance, competition and regulation, external finance control, and other identified areas).

government-held information.<sup>15</sup> In several countries, despite the lack of such a definition in a law concerning government disclosure obligations, the meaning of national security as applied in this context can be, at least partially, deduced by looking to definitions provided in other legal sources.<sup>16</sup> However, in at least some of the surveyed countries, there is no useful guidance regarding how national security should be understood, despite its express inclusion as a basis for non-disclosure.<sup>17</sup>

In general, where a definition of national security has been provided in the law, the term tends to be broadly defined to encompass any threats to the independence, sovereignty, or territorial integrity of the nation, as well as to its internal safety or constitutional order.<sup>18</sup> Although the questionnaire results do not suggest one universally understood definition of national security,<sup>19</sup> it is clear that in the majority of the surveyed countries national security is understood to encompass both international relations and protection against domestic security threats (*e.g.*, law enforcement). Nonetheless, it must be noted that international relations is understood to be a separate concept from national security in approximately 30% of the surveyed countries,<sup>20</sup> and protection against domestic security threats is understood to be a separate concept from national security in approximately 15% of the surveyed countries.<sup>21</sup>

---

<sup>15</sup> In response to Question (1)(a)(i), the experts for 12 of the 20 surveyed countries (60%) expressly stated that *no definition* is provided in the national law for the purposes of justifying the non-disclosure of government-held information. These 12 countries are Belgium, Denmark, Hungary, Italy, the Netherlands, Norway, Russia, Serbia, Slovenia, Spain, Sweden, and the United Kingdom. The provision cited by the expert for Turkey states only that national security information should be exempt from disclosure, but does not provide a definition of national security, thus suggesting that no definition of national security is provided in the law for the purposes of justifying non-disclosure in Turkey either. The experts for the remaining 7 countries – Albania, the Czech Republic, France, Germany, Moldova, Poland, and Romania – provide a definition, although some of these may be drawn from related legal sources, rather than from a law concerning public access to information.

<sup>16</sup> *See, e.g.*, responses to Question (1)(a)(i) for Italy (“Italian law does not provide for an explicit definition of ‘Security of the Republic.’ However, specifically regarding the state secrets privilege, this definition can be easily and clearly deduced from article 39.1 of Law 124/2007”), Sweden (referring to a definition for crimes against national security provided in the Criminal Code), Hungary (referring to a definition of national security provided in Act CXXV of 1995 on National Security Services “for purposes of that act”), Spain (referring to a definition of national defense contained in the National Defense Act of 2005), and the United Kingdom (noting that there is an incomplete definition of national security reflected in the Security Service Act 1989).

<sup>17</sup> *See, e.g.*, responses to Question (1)(a)(i) for Denmark (“The term ‘national security’ is actually not defined in the law and there is no further guidance in theory or practice”), Belgium (“no definition available”), and Russia (“there is no such definition in current Russian law”).

<sup>18</sup> *See, e.g.*, responses to Question (1)(a)(i) for Albania, the Czech Republic, and France.

<sup>19</sup> For example, several countries expressly include protection of the national economy as part of their definition, *see, e.g.*, the Czech Republic and Moldova, whereas others do not.

<sup>20</sup> Question (1)(a)(ii) asked: “Does the definition of ‘national security’ include international relations? Please check one: Yes / No.” *No* was selected for 6 out of 19 responsive countries: Belgium, Denmark, the Netherlands, Russia, Sweden, and the United Kingdom. No answer was provided for Hungary due to the lack of a uniform definition for national security in each of the acts referenced in the Hungarian FOI Act.

<sup>21</sup> Question (1)(a)(iii) asked: “Does the definition of ‘national security’ include protection against domestic security threats (*e.g.*, law enforcement). Please check one: Yes/No.” *No* was selected for 3 out of 19

*b. A Presumption in Favor of Secrecy*

In the vast majority of the surveyed countries (80%), where there is doubt about whether disclosure of information would harm national security, the law does not favor disclosure.<sup>22</sup> Those countries that do favor disclosure are Belgium, Norway, Slovenia, and Sweden. Note, however, that according to the expert for Belgium, there is a presumption in favor of disclosure, only until the information is classified.<sup>23</sup> As explained by the expert for Sweden, public access to all information is the rule and secrecy the exception.<sup>24</sup> Nonetheless, in Sweden, there is a rebuttable presumption of secrecy regarding certain national security information, such as police intelligence files and information collected in the course of military/signals intelligence operations.<sup>25</sup>

*c. Exemption of Certain Information, Offices or Officials*

The majority of the surveyed countries (65%) do not provide exemption from disclosure obligations to any public offices or officials.<sup>26</sup> Nonetheless, a significant number of the surveyed countries (35%) report that certain offices or officials are exempt.<sup>27</sup> Thus, for example, in the Netherlands, the Freedom of Information Act (FOIA) is only applicable to authorities of the executive branch of government; whereas parliament, the judiciary, and also certain executive authorities, such as the Dutch Review Committee on the Intelligence and Security Services, are not expected to respond

---

responding countries: Belgium, Denmark, and Russia. No answer was provided for Hungary due to the lack of a uniform definition for national security in all relevant acts.

<sup>22</sup> Question (2)(f) asked: “Where there is doubt about whether disclosure would harm national security, does the law favour disclosure? Please choose one: Yes/No.” *No* was selected for 16 of the 20 surveyed countries: Albania, the Czech Republic, Denmark, France, Germany, Hungary, Italy, Moldova, the Netherlands, Poland, Romania, Russia, Serbia, Slovenia, Spain, Turkey, and the United Kingdom. *Yes* was selected for the remaining four countries.

<sup>23</sup> See “feedback on draft report” for Belgium.

<sup>24</sup> See response to Question (3)(a) for Sweden.

<sup>25</sup> See response to Question (1)(b)(i) for Sweden.

<sup>26</sup> Question (1)(c) asked: Are there any public offices of officials (e.g., military branches, intelligence agencies, police) that are exempt from disclosure obligations? Please check one: Yes/No.” *No* was selected for 13 out of 20 countries (65%): Belgium, Denmark, France, Hungary, Moldova, Norway, Poland, Romania, Russia, Serbia, Slovenia, Spain, and Sweden.

<sup>27</sup> For Question (1)(c), *Yes* was selected for 7 out of 20 countries (35%): Albania, the Czech Republic, Germany, Italy, the Netherlands, Turkey, and the United Kingdom. *But see also* responses to Question (8)(b) (“Can the public make requests for access to information held by the autonomous oversight body?”). Of the 12 countries that have an autonomous oversight body, experts for 6 of the 12 (i.e., half of the responding countries) selected *No* in response to this question: France, Italy, the Netherlands, Norway, Poland, and Spain. Notably, the experts for 4 of these countries (France, Norway, Poland and Spain) indicated in response to Question (1)(c) that no offices or officials are exempt from disclosure obligations. The inconsistency in these answers suggests that the experts may have been primed by the examples provided in question in (1)(c) to think only of security agencies in responding to that question: if this is the case, the total number of surveyed countries that exempt offices or officials may be higher than indicated in response to (1)(c). See “feedback on draft report” for Spain (“there is no law regulating access to information held by the legislative branch for example”).

to requests for information.<sup>28</sup> Moreover, most of the countries that allow for exemption of certain offices or officials also provide that these offices or officials are absolutely exempt.<sup>29</sup>

In most of these countries, exemption is limited specifically to offices or officials working in the national security sector. Thus, in the United Kingdom, all information that relates to specified national security agencies (including MI5, MI6, and the Government Communication Headquarters) are exempt from disclosure obligations.<sup>30</sup> Likewise, in Germany, federal intelligence services (namely the foreign intelligence agency, the federal domestic intelligence service, and the military intelligence agency) are exempt from Freedom of Information (FOI) requests, whereas the Federal Police, Federal Criminal Police Office, Federal Armed Forces, and Customs Criminology Officer are exempt when it comes to their “security-sensitive tasks.”<sup>31</sup> In Albania, the activity of the Internal Control Service and Military Intelligence Service are excluded from the obligations flowing from the Law on Access to Official Information.<sup>32</sup> In Turkey, civil and military intelligence units are out of the scope of the public’s Right to Information law,<sup>33</sup> and in the Czech Republic, exempt officials include the intelligence services in fulfilling their tasks, the police in areas of ongoing investigation, and the ministry of finance in the areas of money laundering and terrorism.<sup>34</sup>

In addition, even where exemption is not expressly provided by the law, some countries report that these agencies may be exempt in practice. In Norway, for example, although there are technically no public offices or officials that are exempt from disclosure requirements, information generated by some authorities (such as the intelligence services) is automatically classified as a matter of practice.<sup>35</sup> In practice, release of information by these agencies depends on the exercise of these agencies’ discretion.<sup>36</sup> Likewise, in Romania, while there is no exemption as such: practice may

---

<sup>28</sup> See response to Question (1)(c)(i) for the Netherlands. Question (1)(c)(i) asked: “If you checked Yes [to Question (1)(c)], Please list the offices or officials that are exempt.”

<sup>29</sup> Question (1)(c)(iii) asked: “If you checked yes [to Question (1)(c)], is exemption of these offices or officials absolute? Please check one: Yes/No.” Of the 7 countries that exempt some offices or officials from disclosure obligations, 5 of the 7 (71%) reported that the exemption was absolute: Albania, the Czech Republic, Germany, Italy, and the United Kingdom. In the two countries where the exemption was reported not to be absolute, the office or official may often be exempt from disclosure obligations: see response to Question (1)(c)(iii) for Turkey (allowing that disclosure is required where the information affects the professional working life of persons) and the Netherlands (allowing that disclosure is required for decisions concerning the government’s relation with a civil servant in their service).

<sup>30</sup> See response to Question (1)(c)(i) for the United Kingdom.

<sup>31</sup> See response to Question (1)(c)(i) for Germany.

<sup>32</sup> See response to Question (1)(c)(i) for Albania.

<sup>33</sup> See response to Question (1)(c)(i) for Turkey.

<sup>34</sup> See response to Question (1)(c)(i) for the Czech Republic.

<sup>35</sup> See follow-up comment to Question (1)(c) for Norway.

<sup>36</sup> See response to Question (1)(c)(iii) for Norway.

differ from the letter of the law because decision-making authority is bestowed on heads of institutions with very little oversight or accountability: indeed, in Romania, the decision to classify information is itself very often classified as an official secret.<sup>37</sup>

In addition to specific offices, exemptions from disclosure are also often provided for specific categories of information.<sup>38</sup> In Poland, for example, information that leads to the identification of officers, soldiers, or other persons who participated or assisted in operational activities can be withheld indefinitely.<sup>39</sup> In Norway, relations with foreign powers, critical infrastructure, and sources and intelligence measures are exempt.<sup>40</sup> However, in the majority of the surveyed countries, no categories of information are absolutely exempt from disclosure.<sup>41</sup>

## II. Disclosure Obligations

### a. *The Right to Information*

All of the surveyed countries recognize a public right of access to government-held information. However, the disclosure obligations of public authorities vary from country to country. Notably, Spain does not have a Freedom of Information Act, and the right to information provided by the Spanish Constitution provides access to information collected in administrative archives and registries only: otherwise, there is no disclosure duty.<sup>42</sup> To the contrary, in the vast majority of the surveyed countries, the disclosure

---

<sup>37</sup> See comment to Question (1)(c) for Romania.

<sup>38</sup> Question (1)(c) asked: “Are there any public offices of officials (e.g., military branches, intelligence agencies, police) that are exempt from disclosure obligations? Please check one: Yes/No.” Answers to this question varied depending on whether classified information, broadly, was taken to be category. In several of the surveyed countries, more specific descriptors are not provided. Nonetheless, experts for the majority of the surveyed countries listed specific categories of information that are exempt from disclosure on the basis of national security. See, e.g., response to Question (1)(c) for Norway, Poland, Sweden, and the United Kingdom, which list specific categories; see also responses to Question (5)(a). Compare with responses for Denmark, Hungary, and Turkey, which do not exempt any categories, and Belgium, France, and Germany, which refer broadly to classified national security information.

<sup>39</sup> See response to Question (1)(b) for Poland. See also responses to Question (1)(b) for the United Kingdom and the Netherlands. In the United Kingdom, all information that was supplied to or relates to any of the national security agencies listed in FOIA is absolutely exempt from disclosure. Likewise, in the Netherlands, the FOIA does not apply to information that is processed by or on behalf of the intelligence services. In the Netherlands, the FOIA also does not apply to information that is governed by an international treaty that commands secrecy. See also responses to Question (1)(c) regarding the exemption of certain officials and offices from disclosure obligations.

<sup>40</sup> See response to Question (1)(b) for Norway.

<sup>41</sup> Question (1)(b)(ii) asked “Is exemption of these categories absolute?” *Yes* was selected by 6 of the surveyed countries: Belgium, the Czech Republic, France, Romania, Spain, and the United Kingdom. The other countries either selected *No*, or indicated in response to Question (1)(b) that no categories of information are exempt at all. Accordingly 14 (or 70%) of the surveyed countries do not absolutely exempt any categories of information. Moreover, as explained by the expert for Belgium, such exemption is for classified information generally.

<sup>42</sup> See “additional comments” for Spain.

obligations are much broader. Moreover, in the majority of the surveyed countries (60%), disclosure obligations apply not only to government authorities, but also to non-state actors that are serving as agents or contractors for the government.<sup>43</sup> Where disclosure obligations are not automatically extended by law to government agents or contractors, such obligations may nonetheless be expressly included in the government contract terms.<sup>44</sup>

### *b. Affirmative Disclosure Obligations*

Fifteen of the twenty surveyed countries (75%) report that, beyond any obligation to disclose information upon request, public authorities also have an obligation to affirmatively publish information for the public.<sup>45</sup> However, in many of the surveyed countries, the scope of information that is expected to be disclosed by the security sector, defense, and intelligence agencies is quite limited.<sup>46</sup> In Turkey, for example, although affirmative disclosure obligations exist for public authorities in general, these obligations do not apply to the security sector, defense and intelligence agencies, nor, as a matter of practice, do these agencies ever affirmatively publish the information that they hold.<sup>47</sup> Likewise, in Germany, while public authorities generally have an affirmative obligation

---

<sup>43</sup> Question (1)(d) asked: “Do disclosure obligations apply to non-state actors that are serving as agents or contractors for the government? Please check one: Yes/No.” *Yes* was selected for 12 countries: Albania, Belgium, France, Germany, Hungary, Italy, Moldova, Norway, Poland, Serbia, Slovenia, and Turkey. *No* was selected for 7 countries: the Czech Republic, Denmark, the Netherlands, Russia, Spain, Sweden and the United Kingdom. The expert for Romania did not select either Yes or No, but answered similarly to Sweden, by indicating that the answer depends on the specific contract at issue. The given percentage is based, therefore, on a Yes answer from 12 out of 20 countries.

<sup>44</sup> Experts for two countries indicated that whether disclosure obligations apply to a non-state actor depends on the terms of each contract. In Romania, although when public money is involved, information should generally be disclosed, this obligation reportedly lies more with the state than with its private sector agents or contractors. As such, whether a non-state actor will be subject to disclosure requirements depends on the specific contract. *See* response for Romania to Question (1)(d). Likewise, in Sweden, although such obligations do not normally apply to non-state actors, a private company can, with its consent, be made subject to disclosure obligations. *See* response for Sweden to Question (1)(d).

<sup>45</sup> Question (1)(e) asked: “Beyond any obligation to disclose information upon request, do public authorities have an affirmative obligation to public information? Please check one: Yes/No.” *Yes* was selected for 15 of the 20 surveyed countries: Albania, the Czech Republic, France, Germany, Hungary, Moldova, the Netherlands, Poland, Romania, Russia, Serbia, Slovenia, Sweden, Turkey, and the United Kingdom. *No* was selected for 5 of the 20 surveyed countries: Belgium, Denmark, Italy, Norway, and Spain. As explained by the expert for Italy, disclosure obligations only follow targeted requests for information. *See* response to Question (2)(a) for Italy.

<sup>46</sup> Question (1)(e)(i) asked: “If you checked ‘Yes’ [for Question (1)(e)] what information do security sector, defence, and intelligence agencies have an affirmative obligation to publish? How often is this information affirmatively published by these agencies in practices?” *See, e.g.,* responses to Question (1)(e)(i) for the United Kingdom (the publication obligations of the authorities is very limited; in the national security context, fuller but still limited information is published in annual reports by the oversight bodies), Russia (not in detail), and Germany (organizational charts).

<sup>47</sup> *See* response to Question (1)(e)(i) for Turkey (“None and Never”). *See also* response to Question (1)(e)(i) for Hungary (noting that, although disclosure obligations technically apply to national defense agencies, the scope of such disclosure obligation is determined by government decree, and the government has failed to adopt such a decree since 2009).

to at least publish organizational charts, even this minimal requirement does not apply to intelligence agencies.<sup>48</sup> Nonetheless, in the majority of the surveyed countries, at least some affirmative disclosure obligations do apply to these agencies and/or their oversight bodies.<sup>49</sup> Thus, for example, in Russia, each government body is expected to publish its official name, official symbols, address and other contact information, the names of head officials, and forms and procedures for applications made to the body.<sup>50</sup>

Notably, in Slovenia, the positive publication requirements include not only agency programs, strategies, opinions and regulations, but also all public information that has been requested at least three times.<sup>51</sup> In Romania, publication requirements also include a list of “public interest documents” and a list of categories of documents produced and/or managed by the specific institution.<sup>52</sup>

In other countries, while there are affirmative publication requirements, these requirements are not specifically enumerated. In Albania, for example, the outset is simply that, unless information is classified or protected, it ought to be affirmatively disclosed.<sup>53</sup> Likewise, in Moldova, all official information (*i.e.*, information developed, selected, processed, systematized, or adopted by official bodies) should be affirmatively disclosed, except where certain exceptions (such as the protection of national security) are implicated.<sup>54</sup>

How often information is expected to be affirmatively published by government agencies varies considerably. In Belgium, for example, the requirement is to publish “continuously,” in Serbia, every three months, in Romania, at least once a year, and in Germany, the law does not provide any specific time period for updating the required information.

### *c. Time Limits for Responding to Requests for Information*

All of the surveyed countries require public authorities to respond to requests for information in a timely manner. The vast majority of the surveyed countries have set

---

<sup>48</sup> See response to Question (1)(e)(i) for Germany.

<sup>49</sup> See response to Question (1)(e)(i) for the United Kingdom and Sweden (both requiring annual reports to be published by the security oversight bodies).

<sup>50</sup> See response to Question (1)(e)(i) for Russia. See also responses for the Czech Republic (required to publish annual reports, containing main information about the agency’s purpose, location, contacts, procedures, budget, and so forth) and Serbia (required to publish an information booklet, including organizational structure, important contacts, scope of work, legal framework, budget, data on public procurement).

<sup>51</sup> See response to Question (1)(e)(i) for Slovenia (However, while some agencies in Slovenia are quite proactive in publishing, all of the agencies do not provide information for all enumerated categories).

<sup>52</sup> See response to Question (1)(e)(i) for Romania.

<sup>53</sup> See response to Question (1)(e)(i) for Albania.

<sup>54</sup> See response to Question (1)(e)(i) for Moldova.

time limits for responding to requests.<sup>55</sup> In those countries that do not have set time limits, there is instead a requirement to respond “without undue delay”<sup>56</sup> or “as quickly as possible.”<sup>57</sup> The set time limits for responding to requests for information range from 10 days to two months, with most set at 15 or 30 working days, and possibilities to extend these deadlines, where available, are likewise limited.<sup>58</sup> While some of these time limits are regularly deviated from in practice,<sup>59</sup> most are enforced or enforceable.<sup>60</sup>

#### *d. Requests for Classified Information*

In slightly more than half (55%) of the surveyed countries, the classification status of information is conclusive in determining whether a request for that information will be denied.<sup>61</sup> Notably, in Belgium, the legislation on Freedom of Information simply does not apply to classified information.<sup>62</sup> To the contrary, in Germany, the simple formal classification of information is not sufficient to restrict access: rather, the classification has to be justified in substantive respect, which means that classifications must be reassessed when access to information is requested.<sup>63</sup>

#### *e. Segregation of Non-exempt Information*

The vast majority of the surveyed countries (80%) provide that public authorities are required to segregate and disclose non-exempt information within a document if those

---

<sup>55</sup> Question (2)(h) asked: “What time limits exist for a public authority to respond to a request for information? Are these time limits enforced in practice?” *See, e.g.*, responses to Question (2)(h) for Albania (40 days), Belgium (30 working days; 15 in the Flemish region); Czech Republic (15 days with option to extend for 25 additional days in defined circumstances); Denmark (10 days, but not as an absolute time limit); France (two months, followed by one month for appeal); Hungary (15 calendar days that can be extended once by 15 days); Italy (30 days); Moldova (15 days with the possibility to extend by 5 days), the Netherlands (4 weeks), Poland (14 days, or with reason, up to 2 months), Romania (30 days in practice), Russia (30 days), Serbia (up to 40 days), Slovenia (30 working days), Turkey (15 working days); and the United Kingdom (20 days). Notably, since in Spain there is no specific legislation dealing with access to information, the time to respond (3 months) is a general one to respond to any request directed to the public administration.

<sup>56</sup> *See* response to Question (2)(h) for Norway.

<sup>57</sup> *See* response to Question (2)(h) for Sweden.

<sup>58</sup> *See* responses to Question (2)(h) above.

<sup>59</sup> *See, e.g.*, responses to Question (2)(h) for Albania, Denmark, and Russia.

<sup>60</sup> *See, e.g.*, responses to Question (2)(h) for Serbia (usually enforced, but not always), Slovenia (strictly enforced), Turkey (enforced), and the United Kingdom (enforceable).

<sup>61</sup> Question (3)(c) asked: “Is the classification status of information conclusive in determining whether a request for that information will be denied? Please choose one: Yes/No” *Yes* was selected by 11 out of the 20 surveyed countries: Belgium, the Czech Republic, France, Italy, Moldova, Norway, Poland, Russia, Serbia, and Spain. *No* was selected by the remaining 9 countries: Albania, Denmark, Germany, Hungary, the Netherlands, Romania, Slovenia, Sweden, and the United Kingdom.

<sup>62</sup> *See* follow-up responses for Belgium

<sup>63</sup> *See* response to Question (1)(b)(i) and (ii) for Germany. *See also* response to Question (1)(b)(i) and (ii) for the Czech Republic (classified information is absolutely exempt from disclosure, but it is possible that a court decides to disclose some classified information on principle of public interest test).

portions of the document are reasonably segregable.<sup>64</sup> Notably, in Italy, this also means that every single part of a document must be individually classified, so that the public authority receiving a request for information is better placed to decide which portions of the document may be segregated and disclosed.<sup>65</sup> Those countries that do not require segregation, even where possible, are Norway, Romania, Spain, and the United Kingdom. As noted by the expert for the United Kingdom, however, while there is no such requirement under FOIA, such requirement does exist in the context of civil litigation.<sup>66</sup>

*f. Confirming or Denying the Existence of Requested Information*

In approximately one-third of the surveyed countries, public authorities are always required to confirm or deny whether they hold requested information.<sup>67</sup> However, in the majority of surveyed countries, confirmation or denial is not always required.<sup>68</sup> In several countries, this is because the existence of classified information may itself be classified.<sup>69</sup> In Slovenia, for example, if the mere affirmation or denial would itself disclose protected information, that confirmation or denial is not required.<sup>70</sup>

In Germany, although most public authorities are not permitted to refuse to acknowledge whether information is in their possession, in practice, these authorities may effectively avoid acknowledgement by simply ignoring requests for information and requiring lengthy legal action to enforce access rights.<sup>71</sup> In Romania, although

---

<sup>64</sup> Question (2)(g) asked: “Is a public authority required to segregate and disclose non-exempt information within a document if those portions of the document are reasonably segregable. Please check one: Yes/No.” *Yes* was selected by 16 out of 20 countries: Albania, Belgium, the Czech Republic, Denmark, France, Germany, Hungary, Italy, Moldova, the Netherlands, Poland, Russia, Serbia, Slovenia, Sweden, Turkey. *No* was selected by 4 out of 20 countries: Norway, Romania, Spain, and the United Kingdom. Notably, however, in Belgium, although there is generally a principle of segregation of non-exempt information, classification extends to the whole document. See “feedback on draft report” for Belgium.

<sup>65</sup> See response to Question (2)(g) for Italy. See also responses to Question (3)(j)(ii) (regarding classification markings).

<sup>66</sup> See response to Question (2)(g) for the United Kingdom.

<sup>67</sup> Question (2)(a) asked: “Upon receipt of a request for information, is a public authority always required to confirm or deny whether it holds the requested information? Please check one: Yes/No.” *Yes* was selected by 7 out of 19 responding countries: Albania, Moldova, Romania, Russia, Serbia, Spain, and Turkey always require confirmation or denial. No answer was provided by Germany. The other 12 countries (Belgium, the Czech Republic, Denmark, France, Hungary, Italy, the Netherlands, Norway, Poland, Slovenia, Sweden, and the United Kingdom) reported that they do not always require confirmation or denial. Notably, for Spain, although *Yes* was selected, the right of access to information (and likewise the requirement to answer requests) is limited only to archives and public registries.

<sup>68</sup> See responses to Question (2)(a)(i) (“If you checked No [to Question (2)(a)], under what circumstances may a public authority refuse to confirm or deny whether it holds the requested information?”)

<sup>69</sup> See, e.g., responses to Question (2)(a)(i) for the Czech Republic and Norway.

<sup>70</sup> See response to Question (2)(a)(i) for Slovenia. See also responses for the United Kingdom (when required for the purposes of safeguarding national security) and France (any national defense secret).

<sup>71</sup> See response to Question (2)(a)(i) for Germany. Notably, although *No* was selected for Question (2)(a) for Germany, there are some public authorities in Germany that are excluded from the scope of the

confirmation or denial is said to be required, in practice, the rate of silent denials is reportedly often as high as 40%.<sup>72</sup> In addition, as mentioned above, several of the countries that require confirmation or denial nonetheless exempt certain offices or officials from this requirement.<sup>73</sup>

*g. Written and Substantiated Explanations for Denied Requests for Information*

In the vast majority of the surveyed countries (85%), public authorities are required to provide written reasons for denying a request for information.<sup>74</sup> As pointed out by the expert for Italy, however, this requirement is only applicable if an express denial is provided: as discussed above, in some circumstances, a public authority may refuse to even confirm or deny whether it holds the requested documents.<sup>75</sup> In Germany, although public authorities are not required to provide a written explanation for a denied request, it is noted that there is a right to challenge the denial in court and thereby compel explanation.<sup>76</sup>

In most of the surveyed countries, the written explanation that is required to be provided is very minimal and does not require any supporting documentation.<sup>77</sup> In Italy and Serbia, for example, in denying a request for information, the requirement is merely to state the level of classification.<sup>78</sup> In Spain and Poland, it would be enough to merely

---

Freedom of Information Act, and therefore are not required to acknowledge what information is in their possession.

<sup>72</sup> See response to Question (2)(a)(i) for Romania.

<sup>73</sup> Compare responses to Question (2)(a) and (1)(c) for Albania and Turkey.

<sup>74</sup> Question (2)(b) asked: "In denying a request for information, is a public authority required to provide written reasons for the denial? Please choose one: Yes/No." *Yes* was selected by 17 of the 20 surveyed countries: that is, all except Denmark, France, and Germany. In France, there is generally such a requirement; however, no such requirement exists where secrecy is invoked in defense of the national security.

<sup>75</sup> See response to Question (2)(b) for Italy. See also section II.f. of this report, regarding the obligation to confirm or deny the existence of requested information. In addition, in Sweden, although there is a general duty on administrative authorities to motivate a decision, an exception applies if this is necessary with regard to national security. See response to Question (2)(c) for Sweden. Likewise, in Belgium, no motivation is required when that motivation could have a negative influence on the national security or infringe public order. See "feedback on draft report" for Belgium.

<sup>76</sup> See follow-up explanations from Nils Leopold for Germany.

<sup>77</sup> Question (2)(e) asked: "What information or documentation must support an assessment that disclosure would cause harm to national security?" See, e.g., responses for Denmark (only brief reasons and no comprehensive documentation), France (no information or documentation must support an assessment), Italy (no information or explanation is obliged to be provided to the public), Norway (information or documentation is not required), Romania (no specific standards or requirements), Russia (no such requirements), Spain (no obligation to support the assessment with any documentation or additional information), Sweden (a simple reference to the legislation may be the only motivation given to the individual), and Turkey (none).

<sup>78</sup> See follow-up response to Question (2)(c) for Italy (the public authority has only to say only the level of classification of the document) and response to Question (2)(e) for Serbia (the level of confidentiality).

say that the information is classified or that it affects national defence or national security.<sup>79</sup> In Moldova, such an explanation will include the date, the name of the officers in charge, the grounds for refusal with reference to the normative act, and the procedure for contesting the refusal.<sup>80</sup> In Romania, as a matter of practice, this requirement is fulfilled by merely referring to the applicable exemption: in denying a request for information, the authorities do not provide support for why a particular exemption is applicable.<sup>81</sup> As explained by the expert for Norway, information or documentation is not required because the public authority exercises discretionary powers when defining “national security.”<sup>82</sup>

Notably, in Slovenia, a written assessment of possible adverse effects must support a determination that information is withheld in the interests of national security. Moreover, access to the assessment of harm may not be restricted, but should be provided to the public upon request.<sup>83</sup> To the contrary, in Albania, an assessment must be supported by classified information, and as a result the public does not have a right to access that information, but learns only the fact that an assessment of harm has been made and that it is based on classified information.<sup>84</sup> In Belgium, an assessment that disclosure of information would cause harm to national security must be supported by concrete elements of that information, unless this information itself unveils information that is protected. In addition, a public interest test must be carried out to balance whether the specific public interest in disclosure of the information is more important than the national security interest in nondisclosure.<sup>85</sup> However, if the information is classified, classification need merely be invoked.<sup>86</sup>

In denying a request for information, public authorities in most of the surveyed countries are not obliged to provide any description of the information that is withheld, such as the number of pages or the category of information withheld.<sup>87</sup> To the contrary, in

---

<sup>79</sup> See response to Question (2)(c) for Spain (the public authority is obliged to give a very brief general explanation of the reasons for withholding the information) and response to Question (2)(e) for Poland (although the authorities are obliged to provide “basic justification” for denying a request, in practice, the government justification might state only that information cannot be disclosed because it is classified, without providing any further explanation, in particular, regarding what kind of damage may be caused).

<sup>80</sup> See response to Question (2)(c) for Moldova.

<sup>81</sup> See response to Question (2)(b) for Romania. See also, e.g., response to Question (2)(c) for Hungary (the FOI law only requires that there should be some reasoning if the request is denied; the mere citation of the above legal provisions without substantive explanation usually satisfies the court in case of litigation).

<sup>82</sup> See response to Question (2)(e) for Norway.

<sup>83</sup> See response to Question (2)(e) for Slovenia.

<sup>84</sup> See response to Question (2)(e) for Albania.

<sup>85</sup> See response to Question (2)(e) for Belgium.

<sup>86</sup> See “feedback on draft report” for Belgium.

<sup>87</sup> Question (2)(c) asked: “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?)” See, e.g., responses for Albania (no specifications in the law),

the Czech Republic, the authority must very precisely describe which information is refused.<sup>88</sup> In Germany, pursuant to general administrative procedure law, there should be an “abstract description” of what is being withheld, unless even this mere information would fall within an exception that justifies withholding.<sup>89</sup> As explained by the expert for Slovenia, although there is no general obligation to describe information that is withheld, it must be clear upon which request the authority is deciding.<sup>90</sup> In addition, in Slovenia, if the authority allows partial access to documents, it must specify exactly which part of the information is restricted, and that may mean specifying pages and other descriptive information.<sup>91</sup> To the contrary, the other countries do not require indication of how much information is extracted.<sup>92</sup> In Belgium, this requirement exists only where environmental information is concerned: the environmental authority should insofar as possible indicate where information is left out, but the same requirement is not imposed on other public authorities.<sup>93</sup>

Nonetheless, in the majority of the surveyed countries, a declaration or certification by the relevant public authority, in denying a request for information, that disclosure would cause harm to national security is not in and of itself conclusive on the matter.<sup>94</sup> In German administrative courts, the instrument of "in-camera-procedure"

---

Denmark (no such requirements), Hungary (no such requirement, although the requestor can ask about these details as well), Norway (no requirements), Romania (no specific requirements in the law), Spain (no duty to specify the number of pages withheld or identify the category), and the United Kingdom (no such requirements). *See also* responses to Question (2)(c) for Serbia (the obligation is only to provide reasons for not providing information, be it classified or personal data), the Netherlands (the decision must explain why the complete document could not be given), and Turkey (the response should provide reasons behind withholding information; in practice, detailed information such as page number is rarely provided).

<sup>88</sup> *See* response to Question (2)(c) for the Czech Republic. It seems that this information must be provided in the denial; however, the answer may also apply to judicial review. *See also* response to Question (2)(d) for the Czech Republic (support must be included in the decision of refusal of request for information. The courts require a very detailed justification).

<sup>89</sup> *See* follow-up explanation from Nils Leopold for Germany.

<sup>90</sup> *See* response to Question (2)(c) for Slovenia.

<sup>91</sup> *See* response to Question (2)(c) for Slovenia.

<sup>92</sup> *See* responses to Question (2)(c) for the Netherlands and Serbia (both noting that partial documents may be provided, along with reasons why the complete document could not be given, but that there is no duty to specify the number of pages withheld).

<sup>93</sup> *See* response to Question (2)(c) for Belgium.

<sup>94</sup> Question (2)(e) asked: “Is a declaration or certification by the public authority, denying a request for information, that disclosure would cause harm to national security conclusive? Please choose one: Yes/No.” *Yes* was selected for 8 out of 19 (or 42% of the) responding countries: Albania, the Czech Republic, France, Italy, Moldova, Norway, Turkey, and the United Kingdom. *No* was selected for 11 out of 19 (or 58% of the) responding countries: Belgium, Denmark, Germany, Hungary, the Netherlands, Romania, Russia, Serbia, Slovenia, Spain, and Sweden. No answer was provided by Poland. Compare with responses to Question (3)(c), which provide that in the majority of the surveyed countries, the classification status of information is conclusive in determining whether a request for information will be denied. *See also* section VI of this report, regarding the availability of judicial review for denied requests. Notably, although the expert for Denmark answered *No* in response to this question, in response to Question (2)(e), it is stated that in practice the assessment of, *e.g.*, Intelligence Services or Armed Forces is always respected because the control organs do not have the qualifications to challenge this specialist

offers the possibility to open up proof or documentation.<sup>95</sup> Likewise, in the Netherlands, in order to convince a judge, the documents themselves may be provided to the judge confidentially.<sup>96</sup>

#### *h. Review of Denied Requests for Information*

All of the surveyed countries provide an opportunity for judicial review of a denied request for information.<sup>97</sup> Moreover, the majority of the surveyed countries also provide an opportunity for a speedy, low-cost review of a denied request for information by an independent authority.<sup>98</sup> Notably, however, in France, while both administrative and judicial review is technically available, such process is irrelevant if the information requested is classified, because in France no judge is authorized to access classified documents; moreover, the independent body that can access classified documents does not have the authority to order their declassification.<sup>99</sup> In Belgium, while judges have the authority to see classified information,<sup>100</sup> the legislation on freedom of information does not apply to classified information,<sup>101</sup> and judges are not able to order the release or declassification of classified documents.<sup>102</sup> To the contrary, in the vast majority of the surveyed countries, a judge may 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

---

opinion: moreover, in the one and only court decision on this issue in Denmark, the Supreme Court denied insight only because the Minister of Justice declared it would harm national security; accordingly, the relevant authorities normally only give brief reasons and no comprehensive documentation in support of an assessment that disclosure would harm national security.

<sup>95</sup> See follow-up explanation from Nils Leopold for Germany (There is an ongoing discussion in Germany regarding whether this article can be applied to FOI-laws but some courts have already decided to do so.)

<sup>96</sup> See response to Question (2)(e) for the Netherlands.

<sup>97</sup> Question (6)(b) asked: "Is there an opportunity for judicial review of a denied request for information? Please choose one: Yes/No." *Yes* was selected by 19 out of 19 responding countries. France left this question blank, but noted that the answer would depend of the type of information which is denied:

if the information is not classified (like a business secret or personal data, for example), it will be possible to go to the administrative court in order to examine the justification for denying the request of information and maybe to oblige the administration to disclose the information, but if the information denied is classified, it is impossible in France for a court to reverse the classification decision and to oblige the administration to declassify the information. Only an independent body (the CCSDN, which is not a court) can have access to the classified information; moreover, this CCSDN can provide only non-mandatory advice regarding the declassification of that information.

<sup>98</sup> Question (6)(a) asked: "Is there an opportunity for a speedy, low-cost review of a denied request for information by an independent authority? Please choose one: Yes/No." *Yes* was selected for 11 of the 20 surveyed countries (55%): France, Germany, Hungary, the Netherlands, Norway, Poland, Serbia, Slovenia, Sweden, Turkey, and the United Kingdom. *No* was selected for the remaining 9 countries (45%): Albania, Belgium, the Czech Republic, Denmark, Italy, Moldova, Romania, Russia, and Spain. However, in Belgium, such opportunity exists in regard to environmental information and FOI requests in the Flemish region. See "additional comments" for Belgium.

<sup>99</sup> See follow-up explanation provided for France.

<sup>100</sup> See response to Question (7)(a) for Belgium.

<sup>101</sup> See follow-up explanation provided for Belgium.

<sup>102</sup> See response to Question (7)(a)(i) for Belgium.

national security justifies withholding the information.<sup>103</sup> In the Czech Republic, for example, although classified information is exempt from disclosure, it is possible that the court will decide to order its release in accordance with the public interest or in keeping with constitutional principles.<sup>104</sup>

### **III. Classification Procedures**

#### *a. Classification Rules*

In the vast majority of the surveyed countries, the classification of information is governed by rules that are publicly available.<sup>105</sup> Indeed, the only surveyed country that reported that classification rules are not publicly available is Turkey, where this issue is currently subject to Parliamentary debate.<sup>106</sup>

Notably, however, in the United Kingdom, there is no system for the classification of official information, other than a wholly informal, non-legal system of marking the sensitivity of internal Government documents.<sup>107</sup> As a result, the expert for the United Kingdom has abstained from answering survey questions pertaining to classification. As explained in the questionnaire response for the United Kingdom, the basic legal position in the United Kingdom is that the Government is not under any legal obligation to make public the information it holds. Rather, in the United Kingdom, the Government's information becomes public (1) because the Government chooses to publish it, (2) because of a successful Freedom of Information request, or (3) because it is archived. Absent these three conditions, the default position is that the Government's information remains unpublished. The fact that such information is not published does

---

<sup>103</sup> Question (7)(a)(i) asked: "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? Please choose one: Yes/No." Only Albania, Belgium, and Norway responded No. Notably, in Spain, only the Spanish Supreme Court can reverse a classification decision. See additional comments for Spain.

<sup>104</sup> See response to Question (1)(b)(ii) for the Czech Republic.

<sup>105</sup> Question (3)(a) asked: "Are classification rules publicly available? Please choose one: Yes/No." *Yes* was selected for 18 out of 19 responding countries. No answer was provided by the United Kingdom because there is no system of classification of official information in the United Kingdom, other than a wholly informal system of marking the sensitivity of internal government documents. The only country to answer *No* was Turkey. Note, however, in Spain, in addition to the Official Secrets Act, which is publicly available, there is a parallel development of rules regulating the classification of information that is not contained in the law and therefore is not known by the majority of the public: in Spain, questions have been raised about the legitimacy of this regulation, which creates new categories of classified information outside the scope of the law. See "additional comments" from Spain regarding section (3).

<sup>106</sup> See response to Question (3)(a) for Turkey. According to the questionnaire for Turkey, there is currently no publicly available information regarding classification procedures in Turkey; however, if the proposed State Secrecy Bill is adopted, classification procedures would be clarified.

<sup>107</sup> See response to Question (3)(a) for the United Kingdom. According to the questionnaire for the United Kingdom, this internal classification system has no basis in law and no legal consequences other than, potentially, for the handling of archived material.

not necessarily mean, however, that the information is being kept as a “secret”, strictly speaking. Non-published information is informally classified within the Government, but the scheme for doing so is non-legal, and its purpose is merely to highlight how that information must be handled within the Government: the classification does not determine whether the information can be released publicly.

Likewise, in Sweden, classification serves only the administrative function of warning government officials handling the information that they should show special care. Classification does not determine whether the information is entitled to be kept secret.<sup>108</sup> Unlike in the United Kingdom, however, in Sweden, public access to all information is the rule and secrecy the exception. Notably, in Sweden, although classification rules are generally available, the detailed guidelines regarding classification used by the government, the security police, the defense forces, and the signals intelligence organization are not available. As explained by the Swedish expert, there is no possibility to appeal a classification decision, nor is there a need: the public interest in disclosure is otherwise built into the system, and is not necessarily a factor in the classification decision.

Nonetheless, for the vast majority of the surveyed countries, the classification system serves to identify information to be kept from the public, because such disclosure could harm or threaten national interests.<sup>109</sup>

#### *b. Classification Levels and Markings*

In virtually all of the surveyed countries, the law specifies varying levels of classification (*e.g.*, “Top Secret”, “Secret”, “Confidential” and “Restricted”).<sup>110</sup> Moreover, when classifying documents, all of the surveyed countries require that the documents bear classification markings.<sup>111</sup> However, what is included in the

---

<sup>108</sup> See response to Question (3)(a) for Sweden.

<sup>109</sup> Question (3)(b) asked: “What criteria are used to determine whether information may be classified?” See responses to Question (3)(b).

<sup>110</sup> Question (3)(e) asked: “Does the law specify levels of classification (*e.g.*, ‘Top Secret’, ‘Secret’, ‘Confidential’)? Please choose one: Yes/No.” Notably, even in Turkey, where classification rules are not publicly available, it was noted that certain classification levels are known to exist. The only country to respond *No* that the law does not specify levels of classification is Sweden, where classification serves a purely administrative function. In the United Kingdom, where classification is also purely administrative, although no answer was provided to this question, it was noted in follow-up answers provided for the United Kingdom, that there are four classifications (top secret, secret, confidential and restricted) in the U.K. system.

<sup>111</sup> Question (3)(j) asked: “When documents are classified, must the documents bear classification markings? Please choose one: Yes/No.” The United Kingdom did not respond to this question. All 19 of the remaining 19 countries reported that classification markings are required.

classification markings varies considerably from country to country.<sup>112</sup> In several of the countries, all that is required is the classification level.<sup>113</sup> Several also have administrative requirements, such as a reference number,<sup>114</sup> the number of pages,<sup>115</sup> the number of copies,<sup>116</sup> citation of the law authorizing classification,<sup>117</sup> official emblems,<sup>118</sup> and other identifying symbols. Notably, in Russia, the marking is required to contain the reason for classification.<sup>119</sup> Several of the countries require the marking to contain the date of classification,<sup>120</sup> and several also require the date of declassification.<sup>121</sup>

Another common requirement is identification of the classifying agency or administrative origin of the document.<sup>122</sup> More specifically, several countries also require the name (and signature) of the individual responsible for the classification decision.<sup>123</sup> The majority of the surveyed countries, *i.e.*, 11 out of 19 (or 58% of the) responding countries, provide that the identity of the person responsible for a classification decision must be indicated on the document, or otherwise easily traced, to ensure accountability.<sup>124</sup> As noted for Russia, however, this information is available only to the person having access to the classified document: there may be no easy way for a person not having access to the document to learn who is responsible for the document's classification.<sup>125</sup>

---

<sup>112</sup> Question (3)(j)(i) asked: "If you checked 'Yes,' What information is contained in the classification marking?"

<sup>113</sup> See responses to Question (3)(j)(i) for Turkey, Norway, Moldova, Belgium, Denmark, and Italy.

<sup>114</sup> See responses to Question (3)(j)(i) for Italy (as concerns state secrets), Romania, France, and the Czech Republic.

<sup>115</sup> See responses to Question (3)(j)(i) for Germany and Romania.

<sup>116</sup> See responses to Question (3)(j)(i) for Poland, Romania, and Slovenia.

<sup>117</sup> See responses to Question (3)(j)(i) for Belgium and Norway.

<sup>118</sup> See response to Question (3)(j)(i) for Albania.

<sup>119</sup> See response to Question (3)(j)(i) for Russia.

<sup>120</sup> See responses to Question (3)(j)(i) for the Albania, Czech Republic, France, Germany, Italy (as concerns state secrets), Poland, and Romania.

<sup>121</sup> See responses to Question (3)(j)(i) for Albania, France, Hungary, the Netherlands, and Serbia.

<sup>122</sup> See responses to Question (3)(j)(i) for the Czech Republic, France, Poland, Romania, Serbia, Slovenia, and Sweden.

<sup>123</sup> See responses to Question (3)(j)(i) for Albania, Hungary, Romania, and Serbia.

<sup>124</sup> Question (3)(k) asked: "Is the identity of the person responsible for a classification decision indicated on the document, or otherwise easily traced, to ensure accountability? Please choose one: Yes/No." Eleven countries, Albania, Hungary, Italy, Moldova, Poland, Romania, Serbia, Slovenia, Spain, and Sweden, responded *Yes* (that the identify of the person responsible for a classification decision is indicated on the document, or otherwise easily traceable, to ensure accountability). Although Russia left this question blank, it is also included in the count, due to the follow-up explanation that the signatory (*i.e.*, the person responsible) is indicated on the document itself. Notably, although France marked *No* (that the person responsible for the classification is not indicated or easily traceable), the responsible administrative service is indicated.

<sup>125</sup> See response to Question (3)(k) for Russia.

In half of the surveyed countries, *i.e.*, 10 out of 19 (or 53% of the) responding countries, a separate classification marking is required for each section of a document.<sup>126</sup> In Poland, however, it was noted that this requirement is only triggered if the material is separable: otherwise, separate classification markings are not needed.<sup>127</sup> In Romania, on the other hand, each page must bear a separate marking.<sup>128</sup> Furthermore, as explained by Spain, while a document may be comprised of various levels of classified information, the document as a whole will bear the marking of and be handled according to whichever is the highest of these classification markings.<sup>129</sup>

### *c. Classification Authority*

In most of the surveyed countries, classification authority belongs to the agency that originally produced, acquired, or created the document at issue.<sup>130</sup> However, in several of the countries, classification authority is limited to specifically authorized persons.<sup>131</sup> In Serbia, for example, the authorized persons are as follows: 1) the President of the National Assembly; 2) the President of the Republic; 3) the Prime Minister; 4) the head of the public authority; 5) an elected, appointed or nominated official of the public authority authorized to determine classified information by law or by the regulation adopted on the grounds of law, or who has been authorized to do so in writing by the head of the public authority; and 6) a person employed by the public authority who has been authorized in writing by the head of the public authority. In Russia, beyond the Presidential administration and executive government bodies, the bodies with classification authority are defined by a “List of Information Related to State Secret.”<sup>132</sup> Likewise, in Moldova, information may only be referred for state secret classification by heads of the state administration bodies, according to a list of responsible persons who are authorized to refer the information to state secret.<sup>133</sup>

---

<sup>126</sup> Question (3)(j)(ii) asked: “Is a separate classification marking needed for each section of a document? Please choose one: Yes/No.” *Yes* was selected for Albania, Belgium, Denmark, Germany, Italy, Poland, Romania, Slovenia, Spain, and Turkey. *No* was selected for the Czech Republic, France, Hungary, Moldova, the Netherlands, Norway, Russia, Serbia, and Sweden. No answer was provided for the United Kingdom.

<sup>127</sup> See response to Question (3)(j)(ii) for Poland. Notably, the same clarification was also provided by Hungary, which had answered *No* to the question. As such, the requirements in Hungary and Poland should be considered similarly.

<sup>128</sup> See response to Question (3)(j)(ii) for Romania.

<sup>129</sup> See “additional comments” for Spain regarding Question (3)(j)(ii).

<sup>130</sup> Question (3)(f) asked: “Who has the authority to classify information? May this authority be delegated?” See responses to Question (3)(f) for Belgium (the authority that produced the information), Czech Republic (the authority that produced the information), Denmark (the authority with possession of the information), Germany (the function that issues the information), Netherlands, Norway, Poland (or that is entitled to sign), and Turkey.

<sup>131</sup> See, *e.g.*, response to Question (3)(f) for Serbia.

<sup>132</sup> See response to Question (3)(f) for Russia.

<sup>133</sup> See response to Question (3)(f) for Moldova.

Several of the surveyed countries limit classification authority, in particular, for higher level classification.<sup>134</sup> In Romania, for example, classification authority for Top Secret information of the utmost importance is limited to certain ministers, whereas classification authority for ordinary Top Secret information may be exercised by vice-ministers, and for Secret information, may also be exercised by under-secretaries, secretary generals, or directors.<sup>135</sup> Likewise, in Slovenia, classification authority at the Top Secret level may only be assigned by certain persons (*e.g.*, the President of the Republic, the President of the National Assembly, the Prime Minister, and certain ministers and directors of agencies, military commanders, and diplomatic heads); whereas the director of an authority, elected or appointed officials of the authority with written authorization from the director, and employees of the authority with written authorization from the director are authorized to designate information with lower levels of classification.<sup>136</sup>

While some of the surveyed countries allow classification authority to be delegated,<sup>137</sup> several place restrictions on the delegation of such authority, such as the requirement that delegation be made in writing.<sup>138</sup> In Hungary, classification authority for Top Secret classification can only be delegated to a deputy, and for other levels of classification, can only be delegated in writing to senior officials, entrusted with the exercise of public authority.<sup>139</sup> Moreover, many of the surveyed countries do not allow classification authority to be delegated at all.<sup>140</sup> In Albania, classification authority may only be delegated up to the Secret level, and not for Top Secret information.<sup>141</sup> Note

---

<sup>134</sup> See, *e.g.*, response to Question (3)(f) for Italy (the state secrets privilege may only be invoked by the President of the Council of Ministers; whereas for other classification, the authority is vested in the function that creates the information).

<sup>135</sup> See response to Question (3)(f) for Romania (Art. 19 of Law 182/2002 defines the authority to classify information, as follows: a) for top secret of utmost importance: President of Romania, Chairs of the 2 Chambers of Parliament, members of the CSAT—Supreme Council for National Defence, Prime-Minister, members of Government (ministers and secretary general), Governor of the BNR—Central Bank, directors of the intelligence services (SRI, SIE, SPP and the STS—Service for Special Telecommunications), secretary generals of the 2 Chambers of Parliament, president of the INS—National Institute of Statistics, director of the National Administration of State Reserves, other authorities mandated by the President or the Prime-Minister; b) for top secret: all of the above, as well as public officials ranking as secretaries of state (vice-ministers), according to their material competencies/attribution; c) for secret: all of the above, as well as public officials ranking as under-secretaries of state, secretary generals or director generals, according to their material competencies/attribution.)

<sup>136</sup> See response to Question (3)(f) for Slovenia.

<sup>137</sup> See, *e.g.*, response to Question (3)(f) for Belgium (to another with the same security clearance level), Germany, Hungary, Italy, and Serbia (in writing).

<sup>138</sup> See, *e.g.*, response to Question (3)(f) for Albania (delegation is permitted up to the Secret level, but not for Top Secret classification authority); Germany (delegation is permitted to staff); Denmark (The relevant official has to be specially authorized by superior to classify).

<sup>139</sup> See response to Question (3)(f) for Hungary.

<sup>140</sup> See responses to Question (3)(f) for the Czech Republic, Poland, the Netherlands, Norway, Russia, Slovenia, and Spain.

<sup>141</sup> See response to Question (3)(f) for Albania.

also, in Italy, although classification authority may be delegated, the ability to invoke the state secrets privilege can only be exercised by the President of the Council of Ministers and cannot be delegated.<sup>142</sup> As explained by the expert for Sweden, however, classification decisions are normally taken by the desk officer responsible for dealing with the specific matter in question: only a small category of classification decisions of considerable significance to national security are taken by higher authority.<sup>143</sup>

*d. Classification Duties*

More than half of the countries surveyed, *i.e.*, 11 out of 18 (or 61% of the) responding countries, reported that classification authorities have a duty to classify information.<sup>144</sup> In Romania, the duty to classify information is triggered whenever the classifier encounters information “susceptible” of being classified; in Denmark, the duty is triggered “when there are reasons to believe that the information needs to be classified,” and in Russia, the duty occurs “upon foundation of an authority.”<sup>145</sup> To the contrary, in Slovenia, the law states only that authorized persons “may” classify information. Accordingly, there is no duty to classify information, but rather only an obligation to assess the security importance of information and make proposals based thereon.<sup>146</sup> Likewise, in Spain, the government must perform a test to determine whether the disclosure of information to a non-authorized person could threaten or harm national security or defense, and if the test is positive, the government can classify the information, but it is not obliged to do so.<sup>147</sup>

Slightly less than half of the countries surveyed, *i.e.*, 9 out of 19 (or 47% of the) responding countries, reported that there is a duty for public authorities to state reasons for classifying information.<sup>148</sup> As explained in the questionnaire response for Italy,

---

<sup>142</sup> See response to Question (3)(f) for Italy.

<sup>143</sup> See response to Question (3)(f) for Sweden.

<sup>144</sup> Question (3)(g) asked: “Do classification authorities have a duty to classify information? Please choose one: Yes/No.” *Yes* was selected by 11 out of 18 responding countries: Albania, the Czech Republic, Denmark, France, Italy, Moldova, the Netherlands, Norway, Poland, Romania, Russia. Notably, in the Netherlands, in general, there is no such duty, but such a duty may follow from a specific regulation, *e.g.*, the Act on Nuclear Energy. *No* was selected by 7 out of 18 responding countries: Belgium, Germany, Hungary, Serbia, Slovenia, Spain, or Sweden. It is unknown whether any such duty exists in Turkey and the question is, as explained above, not applicable in the United Kingdom.

<sup>145</sup> See response to Question (3)(g) for Romania, Denmark, and Russia. See also response for Poland (In Poland, this duty is triggered when information “may lead to harm to Poland’s interests”) and Italy (In Italy, as concerns state secrets, the duty to classify is triggered whenever the information is “at least potentially” harmful for national security.).

<sup>146</sup> See response to Question (3)(g) for Slovenia.

<sup>147</sup> See response to Question (3)(g) for Spain.

<sup>148</sup> Question (3)(h) asked: “Is there a duty for public authorities to state reasons for classifying information? Please choose one: Yes/No.” *Yes* was selected for 9 out of 19 responding countries: Albania, Hungary, Italy, Moldova, Romania, Russia, Serbia, Slovenia, Spain. *No* was selected for 10 countries: Belgium, Czech Republic, Denmark, France, Germany, Netherlands, Norway, Poland, Sweden, and Turkey. No

however, such reasons are often formulaic; detailed or substantiated reasons are not often provided to the public.<sup>149</sup> Moreover, in the countries that do not have such a duty, the relevant authorities may still be required to provide reasons for classification when the classification is challenged and/or information requests are made. As noted in the response for Sweden (where classification is purely an administrative function), for example, reasons for classification – albeit brief – must be given to the courts if and when an individual requests access to information and a negative decision is taken which is then appealed to the administrative courts.<sup>150</sup>

At least seven of the surveyed countries also impose penalties on government officials for improperly classifying information.<sup>151</sup> In particular, several of these countries use monetary fines to punish the improper classification of information.<sup>152</sup> In Moldova, deliberate violation by a public person of the legal procedure for ensuring and enforcement of the right to access to information, which caused a considerable damage to the legally protected rights and interests of the person who requires information regarding public health protection, public security or environmental protection, shall be punished with a jail sentence of up to 3 years or forfeiture of the right to hold certain positions or to carry on a certain activity for a term up to 5 years.<sup>153</sup> Other countries, while not specifically penalizing the improper classification of information, note that such offense may be penalized as an abuse of office.<sup>154</sup> As explained by the Swedish expert, excessive classification can draw criticism from the Ombudsman or even, in theory, prosecution for

---

answer was provided for the United Kingdom. According to the expert for Spain, although, in theory, there is such a duty in Spain, this duty is not complied with in most cases involving classified information.

<sup>149</sup> See response to Question (3)(h) for Italy.

<sup>150</sup> See response to Question (3)(h) for Sweden.

<sup>151</sup> Question (3)(i) asked: “Are there any penalties for improperly classifying information? Please choose one: Yes/No.” *Yes* was selected for 7 of the surveyed countries: the Czech Republic, Moldova, Poland, Russia, Serbia, Slovenia, and Sweden. In addition, various penalties are available in Romania, although not explicitly for the improper classification of information. *No* was selected for 10 of the surveyed countries: Albania, Belgium, Denmark, France, Germany, Hungary, Italy, the Netherlands, Norway, and Spain. For Italy, one should note, however, that an improper classification – on a case by case basis – could be deemed an offence of abuse of public officer under article 323 of the Italian Code of Criminal Law and punishable with detention from six months to a maximum of three years. Likewise, in Belgium, under Article 151 of the Penal Code, civil servants can be sentenced with imprisonment up to one year for arbitrarily infringing constitutionally guaranteed rights, although this provision has not been used to penalize improper classification to date. In Turkey, the answer was reported to be unknown; however, it was also reported that there is no reason to suspect that penalties are imposed. The United Kingdom provided no answer.

<sup>152</sup> See responses for Russia (1,000 to 3,000 rubles, *i.e.*, 25- 75 EUR), Serbia (5,000-50,000 RSD, *i.e.*, 50-500 EUR), and Slovenia (417- 12,519 EUR). See also response for Romania (On a case-by-case determination, penalties may be labour-related, career-related, disciplinary, administrative or criminal. The range of administrative penalties is quite steep, and varies from Lei 500K to 100M (roughly €100K to 20 million, but it may be the case that the wording in the legislation was not adapted to the denomination by 10,000 of the Romanian Leu, in 2005)).

<sup>153</sup> See response to Question (3)(i) for Moldova.

<sup>154</sup> See response to Question (3)(i) for Italy and Romania.

misuse of office: in practice, however, in Sweden, prosecutions for any form of misuse of office are very rare.<sup>155</sup>

#### **IV. Declassification Procedures**

##### *a. Time Limits on the Duration of Classification*

In slightly more than half of the surveyed countries, when information is classified, the classifier is expected to specify a time (date or event) that triggers the declassification of the information.<sup>156</sup> Moreover, in the majority of the surveyed countries, the classification period is subject to a maximum duration.<sup>157</sup> The maximum duration of classification varies from state to state, but the most commonly prescribed (and median) time limit is thirty years.<sup>158</sup> Notably, however, in the Netherlands, the maximum duration is set at 10 years; whereas, in Romania, for top secret information of “utmost importance” the maximum is set at 100 years.<sup>159</sup> In both of these countries, as in the majority of the surveyed countries, the maximum is subject to extension.<sup>160</sup> In some countries, the ability to extend the classification period is itself limited. For example, in

---

<sup>155</sup> See response to Question (3)(i) for Sweden.

<sup>156</sup> Question (4)(a) asked: “When information is classified, does the classifier specify a time (date or event) that triggers the declassification of the information? Please choose one: Yes/No.” *Yes* was selected for 10 out of 19 responding countries: Albania, France, Hungary, Moldova, the Netherlands, Romania, Russia, Serbia, Slovenia, and Spain. Notably, however, in Spain, there is no absolute obligation to specify a date or event that triggers declassification: the law states that “whenever possible” the classifier will specify the duration of the classification. *No* was selected for 9 countries: Belgium, the Czech Republic, Denmark, Germany, Italy, Norway, Poland, Sweden, and Turkey. No answer was provided for the United Kingdom, since the basic legal position in the U.K. is that the Government is not under any legal obligation to make public the information it holds.

<sup>157</sup> Question (4)(b) asked: “What is the maximum duration of classification? Can this time period be extended?” See response to Question (4)(b) for Albania (no maximum and the time period specified at the time of classification can be extended); Belgium (no time limit); Czech Republic (no maximum, but once the time period provided at the time of classification expires, the classification expires); Denmark (75 years and can be extended); France (50 years); Germany (30 years, which can be extended for another 30 years); Hungary (30 years for Top Secret information; 20 years for Restricted; 10 years for Confidential and can be extended subject to limits); Italy (15 years for state secrets with possibility of extension up to 30 years); Moldova (25 years for Top Secret information; 10 years for Secret, but possible to establish longer); Netherlands (10 years and can be extended); Norway (30 years and can be extended, with review every 10 years after 40 years); Poland (no maximum, but review every 5 years); Romania (100 years for Top Secret information of utmost importance, except when needs longer protection); Russia (30 years and can be extended); Serbia (30 years and can be extended); Slovenia (no maximum, but once time period that has been marked expires, the classification expires, and if not then law governing archival information provides limit of 40 years); Spain (no maximum); Sweden (40 years, but may be 150 years for certain military information and 70 years for intelligence); Turkey (no max).

<sup>158</sup> See responses to Question (4)(b) for Germany, Hungary, Norway, Russia, and Serbia.

<sup>159</sup> See responses to Question (4)(b) for the Netherlands and Romania; *see also* response to Question (4)(b) for Sweden: in Sweden, the maximum duration is normally set at 40 years; however, 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).

<sup>160</sup> See responses to Question (4)(b) for Albania, Denmark, Germany, Hungary, Italy, Moldova, the Netherlands, Norway, Romania, Russia, and Serbia.

Italy, the President of the Council of Ministers may, by stating reasons, extend the state secret privilege beyond the ordinary 15 year limit, but the privilege may not by extension exceed 30 years (*i.e.*, the extension itself is limited to 15 years).<sup>161</sup> Likewise, in Germany the 30 year maximum may be extended only once for an additional 30 years,<sup>162</sup> and in Hungary, while Top Secret and Secret information can be extended only once by 30 years, Restricted and Confidential information can be extended only once by 5 years.<sup>163</sup>

In Romania, Top Secret information may, by extension, be classified for up to 200 years: while there is no legal text in Romania that allows for outright indefinite classification, where the proscribed maximum is for such a lengthy time period, it might just as well be considered to be indefinite.<sup>164</sup> Nonetheless, in the majority of the surveyed countries, information may not be classified indefinitely, either in law or in practice.<sup>165</sup>

Notably, although there is no prescribed maximum duration of classification in the Czech Republic, the classification is still time limited because once the time period for the classification of the information that has been marked on the document has expired, the classification expires.<sup>166</sup> The same is also true in Slovenia. In addition, several of the countries that do not have a maximum duration, require periodic review of the classification decision.<sup>167</sup> Indeed, in Poland, a law passed in 2010 removed automatic declassification and replaced it with non-automatic declassification based on a five-year review.<sup>168</sup> In general, it may be said, therefore, that the trend in the surveyed countries has been to establish declassification procedures that provide a time limit, trigger event, or mandatory period of review to ensure that publicly-held information does not remain indefinitely classified.

---

<sup>161</sup> See response to Question (4)(b) for Italy.

<sup>162</sup> See response to Question (4)(b) for Germany.

<sup>163</sup> See response to Question (4)(b) for Hungary. Note also, regarding Hungary, “With regard to defence, national security, law enforcement, or judiciary interests in relation to the rightful interest of a private person Top Secret/Secret classification can be extended twice by 30+30 years and the Restricted and Confidential twice by 20+20 years.”

<sup>164</sup> See response to Question (4)(c) for Romania (I might as well have answered Yes. Who is to know what happens in 200 years?)

<sup>165</sup> Question (4)(c) asked: “May information ever be classified indefinitely (in law or in practice)? Please choose one: Yes/No.” *No* was selected for Albania, France (except regarding information related to mass destruction weapons), Germany, Italy, the Netherlands, Norway, Serbia, Slovenia, and Sweden. *No* was also selected for Romania; however, it should be noted that certain information may be classified in Romania for up to 200 years. *Yes* was selected for Belgium, Czech Republic, Hungary, Moldova, Poland, Russia, Spain, and Turkey. The expert for Denmark did not select either *Yes* or *No*, noting that no information could be found on this issue: as such, in Denmark, the possibility of indefinite classification could only be said to be theoretical.

<sup>166</sup> See response to Question (4)(b) for the Czech Republic.

<sup>167</sup> See responses to Question (4)(b) for Poland (every 5 years), Norway (every 10 years after the first 30), and Moldova (every 5 years).

<sup>168</sup> See response to Question (3)(b) for Poland.

### *b. Periodic Classification Reviews*

In the majority of the surveyed countries, the decision to classify information is reviewed periodically to ensure that the original reasons for the classification are still valid.<sup>169</sup> In most of these countries, a specific time period for review is prescribed.<sup>170</sup> Most commonly, this period of review is set at five years.<sup>171</sup> Notably, in Serbia, information classified at the Restricted level must be reviewed annually, whereas Confidential information must be reviewed every three years, and Top Secret information every five years.<sup>172</sup> To the contrary, in Slovenia, the classification of information as Top Secret must be reviewed every year and other classification levels must be reviewed every three years.<sup>173</sup> In Sweden, although there are not periodic reviews, review of the classification level is performed whenever a request for disclosure of that information is made: consideration of whether a document is properly withheld from the public must be carried out *de novo* every single time a request is received by a journalist or member of the public for access to that document, even if it has only been some months or weeks since the last request.<sup>174</sup>

### *c. Automatic Declassification*

In the majority of the surveyed countries, classified information does not automatically lose its classified status if it becomes widely available in the public

---

<sup>169</sup> Question (4)(d) asked: “Are decisions to classify information reviewed periodically to ensure that the original reason for the classification is still valid? Please choose one: Yes/No.” *Yes* was selected for 13 out of 18 (or 72% of the) responding countries: Albania, Czech Republic, Denmark, France, Germany, Hungary, Italy, Moldova, Poland, Romania, Serbia, Slovenia, and Spain. However, in Germany, periods for review are not prescribed, and review is only prompted by change or expiration of the reason for classification: accordingly, Germany does not appear to have periodic review, but rather only occasional review, bringing the percentage to 67%. *No* was selected for 5 out of 18 responding countries: Belgium, the Netherlands, Norway, Russia, and Turkey. Neither *Yes* nor *No* was selected for Sweden or the United Kingdom, where classification is purely administrative.

<sup>170</sup> To the contrary, *see* responses for Albania (the law stipulates that review should occur “time after time” after the period of classification has expired); Denmark (in principle the public authority has to review classified information regularly, but it is very uncertain if this actually happens); Germany (periods for revision are not prescribed; review is only prompted by change or expiration of the reason for classification); Romania (the law provides that there shall be “periodic checks” but it is not clear how often this should occur); and Spain (to avoid excess accumulation of classified material, the authority in charge of classifying information is expected to establish a procedure to determine, periodically, the convenience of declassifying or lowering the classification of information; also the director of the National Intelligence Centre provides that the users of classified information should carry out a “continuous” review; however, there is not systematic review). *See also* response for France (a new instruction recommends revision at least every 10 years, but it is not yet the general practice).

<sup>171</sup> *See* response to Question (4)(d) for Czech Republic (5 years); Hungary (5 years); Italy (15 years for state secrets privilege, but 5 years for other classified information); Moldova (5 years); Poland (5 years).

<sup>172</sup> *See* response to Question (4)(d) for Serbia.

<sup>173</sup> *See* response to Question (4)(d) for Slovenia.

<sup>174</sup> *See* response to Question (4)(d) for Sweden.

domain.<sup>175</sup> In Romania, for example, the law provides only one method for declassification of state secrets, namely the active decision of the Government or Cabinet of Ministers: unless the Government has acknowledged by Government Decision that information is irreversibly lost as a consequence of a formal investigation, the information is presumed to be actively protected by its classification status.<sup>176</sup> In the Czech Republic, the law requires the originator to immediately revoke or amend the security classification once he learns that the reason for the secrecy has disappeared, and failure to do so may result in penalties (such as fines) for violation of this duty.<sup>177</sup> In Serbia, on the other hand, the law proscribing time limits on information classification explicitly states that the classification of information shall terminate if the information is made available to the public: indeed, the public availability of information is listed as a trigger of declassification akin to passage of an expiry date or revocation of classification status. According to the Serbian expert, although this law has not been further elaborated, as a matter of practice, once “secret” information (such as the number of soldiers in the army) has been publicly stated, that data can be used, interpreted, and broadcast without legal consequence.<sup>178</sup> Likewise, in Italy, several rulings by the Italian Supreme Court have affirmed that when a classified piece of information becomes widely available in the public domain, the classification should cease to exist; however, the Italian Constitutional Court has found otherwise as concerns the state secrets privilege.<sup>179</sup>

Notably, in Italy, as concerns classified information, the level of classification will automatically be downgraded five years after the date of its original application, and all classification restrictions must be lifted after a further five year term, unless reasons are provided for an extension of the original classification date. Moreover, in the case of extensions beyond 15 years, such explanation must be provided by the President of the Council of Ministers.<sup>180</sup>

#### *d. Requests for Declassification by the Public*

In the majority of the surveyed countries, declassification requests can be made by the public.<sup>181</sup> In several of these countries, however, no specific procedures are

---

<sup>175</sup> Question (3)(l) asked: “Does classified information lost its classified status if it becomes widely available in the public domain? Please choose one: Yes/No.” *No* was selected for Belgium, Denmark, France, Germany, Hungary, Italy, the Netherlands, Norway, Poland, Romania, Russia, Slovenia, Spain, Sweden, and Turkey.

<sup>176</sup> *See* response to Question (3)(l) for Romania.

<sup>177</sup> *See* response to Question (3)(l) for Czech Republic.

<sup>178</sup> *See* response to Question (3)(l) for Serbia.

<sup>179</sup> *See* response to Question (3)(l) for Italy.

<sup>180</sup> *See* response to Question (4)(b) for Italy.

<sup>181</sup> Question (4)(f) asked: “Can declassification requests be made by the public? Please choose one: Yes/No.” *Yes* was selected for 15 out of 19 responding countries: Albania, Belgium, Czech Republic, France, Hungary, Italy, Moldova, the Netherlands, Norway, Romania, Russia, Slovenia, Spain, Sweden,

provided for declassification requests, and consideration of such requests by the relevant agency is purely discretionary.<sup>182</sup> For example, in Spain, although there is no specific procedure for the public to ask for the declassification of information, under the Petition's Right Act, any person has the right to make a formal request of any public institution.<sup>183</sup> In Slovenia, on the other hand, if an applicant holds that information is denoted classified in violation of the Act governing classified data, he can request the withdrawal of the classification: such application must be decided by the director of the agency concerned and can be appealed to the Information Commissioner.<sup>184</sup> Likewise, in Serbia, the user of classified information may propose that the authorized persons revoke classification, and the authorized person is obliged to consider the proposal, which can be appealed to the Commissioner for Information of Public Importance.<sup>185</sup> In Romania, either the under-assessment or the over-assessment of the classification level and the duration for which it has been stored may be contested by any Romanian person in the administrative courts.<sup>186</sup> Notably, in both Moldova and Russia, declassification requests must be examined within three months of receipt.<sup>187</sup>

Nonetheless, while declassification requests can be made by the public, in the majority of the surveyed countries, the law does not require consideration of the public's interest in the disclosure of information when the relevant agency is deciding whether to declassify information.<sup>188</sup> Still, as explained by the expert for Romania, although there is not an explicit public interest test provided by the law, information shall only be classified in the first instance if it needs protection, and classification periods shall apply only so long as the unauthorized disclosure or dissemination of the information may damage the national security and defense, public order, or the interests of public or

---

and Turkey. *No* was selected for 4 countries: Denmark, Germany, Poland, and Serbia. No answer was provided by the U.K.

<sup>182</sup> Question (4)(e) asked: "What is the procedure for requesting the declassification of documents?" *See* responses to Question (4)(e) for Belgium (no procedure); Czech Republic (not specified by law, but anyone can submit an informal complaint, and the originator may consider it); Denmark (no specific procedure); Hungary (such a request can be made, though the law does not provide such right to the public, nor any procedure); Italy (a specific procedure does not exist); Netherlands (no specific procedure, but everyone can submit a request under FOIA, which will lead to reconsidering the legitimacy of maintaining secrecy); Spain (no specific procedure); Turkey (only through freedom of information requests).

<sup>183</sup> *See* response to Question (4)(f) for Spain

<sup>184</sup> *See* response to Question (4)(e) for Slovenia.

<sup>185</sup> *See* response to Question (4)(e) for Serbia.

<sup>186</sup> *See* response to Question (4)(g) for Romania.

<sup>187</sup> *See* responses to Question (4)(e) for Moldova (requiring a motivated answer to declassification requests received from citizens, enterprises, institutions, organizations and state bodies) and Russia.

<sup>188</sup> Question (4)(g) asked: "Does the law consider the public's interest in the disclosure of information when deciding whether to declassify information? Please choose one: Yes/No." *No* was selected for 14 countries: Albania, Belgium, Czech Republic, Denmark, Germany, Hungary, Italy, the Netherlands, and Norway. *Yes* was selected for 5 countries: France (but only, under the defense code, to the interests of the judicial process and the accused's right), Moldova, Serbia, Slovenia, and Sweden.

private legal persons.<sup>189</sup> Moreover, as noted by Sweden, in adjudicating a freedom of information challenge, the court has to determine if the information genuinely should be kept secret and, thus, takes into account the individual's expressed interests in obtaining the information.<sup>190</sup>

## V. Classifiable Information

### a. *Consideration of the Public Interest in Disclosure during Classification*

The vast majority of the surveyed countries reported that the law does not take the public's interest in the disclosure of information into consideration when deciding whether to classify information.<sup>191</sup> In Slovenia, although there is no specific mention of the public interest when deciding to classify, only the lowest level of classification necessary to ensure protection of the protected interest is permitted.<sup>192</sup> Similarly, in Hungary, the right of access to information can be restricted only in line with the general principles of necessity and proportionality, which dictate that information of public interest may only be restricted by the level of classification needed for the protection and for the time period absolutely necessary.<sup>193</sup> Likewise, in Germany, the law calls on the responsible authorities to critically examine if a classification is really necessary.<sup>194</sup> Nonetheless, in Germany, the concept of public interest is invoked only as concerns the public interest in safeguarding the secrecy of information, and not as concerns the public interest in information disclosure. To the contrary, according to Italian legislation, the concept of "public interest" applies both to justify broader disclosure obligations and also

---

<sup>189</sup> See response to Question (4)(g) for Romania.

<sup>190</sup> See response to Question (4)(g) for Sweden.

<sup>191</sup> Question (3)(d) asked: "Does the law consider the public's interest in the disclosure of information when deciding whether to classify information? Please choose one: Yes/No." *No* was selected for 16 out of 19 (or 84% of the) responding countries: Albania, Belgium, the Czech Republic, Denmark, France, Italy, the Netherlands, Norway, Poland, Romania, Russia, Serbia, Spain, Sweden, and Turkey all selected "No" (that the law does not consider the public's interest in the disclosure of information when deciding whether to classify information). Although the expert for Germany left this question blank, Germany should also be included in this count: as the Germany expert explained, the law "does not consider the public interest in disclosure but only the public interest for the requirement of secrecy." *Yes* was selected for Hungary, Moldova, and Slovenia; however, at least as far as Hungary and Slovenia are concerned, it is not clear that the consideration given to the public interest in disclosure is markedly different than that provided by those countries answering No. No answer provided for the United Kingdom.

<sup>192</sup> See response to Question (3)(d) for Slovenia.

<sup>193</sup> According to the answer to question 3(b) of the Hungarian questionnaire, "There are three conjunctive criteria for a valid classification: 1) classification has to protect one of six categories of public interest defined by law, 2) disclosure of, unauthorized obtaining of, manipulation or use of information, providing access to unauthorized person or rendering it inaccessible to authorized persons harms public interest that can be protected by classification, and therefore 3) openness of and accessibility by persons excluding the authorized ones is needed for a certain time period."

<sup>194</sup> See response to Question (3)(d) for Germany.

to justify a stricter segregation of information for the purpose of protecting the security of the Republic.<sup>195</sup>

A few countries, such as Moldova, on the other hand, lists specific categories of information, the disclosure of which is in the public interest, that may not be classified: these include any violations of human and citizen rights and freedoms, emergencies and catastrophes that threaten the health of people, real situations in education, health, ecology, agriculture, trade and the legal order, and illegal activity or inactivity by the state. Moreover, in Moldova, classification is not allowed if it negatively affects the implementation of governmental and sartorial programs or social, economic, and cultural development, or if it restricts the competition of economic agencies.<sup>196</sup>

*b. Classification of Information in the Public Domain*

In the majority of the surveyed countries, information that originated in the public domain can be classified, or at least is not expressly prohibited from being classified.<sup>197</sup> For example, in Norway, such information might be classified if it is included along with classified information in a report or collection and would by its inclusion expose the working methods of the security service.<sup>198</sup> Likewise, as explained by the Hungarian expert, intelligence services collect and compile information from publicly available sources and the result of such collection may be classified.<sup>199</sup> In Serbia, information generated through the consolidation or linking of information which is not inherently classified shall be classified, if the information is consolidated or linked in such a manner

---

<sup>195</sup> See response to Question (3)(d) for Italy.

<sup>196</sup> See response to Question (5)(b) for Moldova; see also response to Question (1)(b)(ii) for Russia (The following categories of information should not be classified: on accidents and disasters threatening security and health of citizens, as well as of natural disasters, their official prognoses and consequences; on state of environment, health care, sanitary, demography, education, culture, agriculture, and crime; on privileges, benefits, and social warranties provided by the state to citizens, officials, enterprises, institutions, and organizations; on facts of violations of human and civil rights and freedoms on volumes of gold stock and state currency reserves of the Russian Federation; on state of health of top state officials of the Russian Federation; on facts of law violation by government bodies and their officials).

<sup>197</sup> Question (3)(m) asked: "Can information be classified if it originated in the public domain? Please choose one: Yes/No." *Yes* was select for 10 countries: Albania, the Czech Republic, Hungary, Italy, Norway, Poland, Russia, Serbia, Spain and Sweden. Notably, some of these, *e.g.*, Spain and Russia, base this answer on the fact that there is no prohibition against doing so. Neither *Yes* nor *No* was selected for Germany, Denmark, Romania, or the United Kingdom. As noted in Germany, the available provisions do not explicitly prohibit the classification of such information. As noted in Denmark, because there have been no such cases and there are no rules, practices, or discussion in jurisprudence, the state of the law is unclarified. As noted by the expert for Romania, it is imaginable that this information could be classified, but there is no explicit provision to that effect. The experts for 6 countries (Belgium, France, Moldova, the Netherlands, Slovenia, and Turkey) report that *No*, information that originated in the public domain cannot be classified.

<sup>198</sup> See response to Question (3)(m) for Norway.

<sup>199</sup> See response to Question (3)(m) for Hungary.

that it constitutes information that needs to be protected.<sup>200</sup> Leading authorities in Sweden, on the other hand, appear to disagree as to whether the systematic gathering of publicly available information can mean that the information becomes secret; however, it is clear that – if classification applies to this information at all – it would be very exceptional.<sup>201</sup>

Some of the surveyed countries note that while classification of such information is theoretically possible, it is unlikely.<sup>202</sup> As explained by the experts for the Czech Republic and Spain, for example, classification of such information would be difficult because classification of information is only permissible if knowledge of that information by unauthorized persons could cause harm or threaten the national security or defense, and this would not likely be the case if the information originated in the public domain.

### *c. Categories of Classifiable Information*

Half of the surveyed countries, *i.e.*, 10 out of 19 (or 53% of the) responding countries, list specific categories of information that can be classified on national security grounds.<sup>203</sup> In some countries, the lists provided by the law or implementing regulations are also exhaustive.<sup>204</sup> In the other countries, however, the law only provides broad terms and not subcategories of national security.<sup>205</sup> Notably, in Spain, although the Official Secrets Act itself does not contain categories of classifiable information, such a list can be constructed by compiling relevant legislative decisions and government agreements.<sup>206</sup>

In a little less than half of the surveyed countries, the law also prohibits certain categories of information from being classified.<sup>207</sup> In particular, some countries

---

<sup>200</sup> See response to Question (3)(m) for Serbia.

<sup>201</sup> See response to Question (3)(m) for Sweden.

<sup>202</sup> See response to Question (3)(m) for the Czech Republic and Spain.

<sup>203</sup> Question (5)(a) asked: “Does the law list specific categories of information that may be classified on national security grounds? Please choose one: Yes/No.” *Yes* was selected for Albania, Czech Republic, Italy, Moldova, the Netherlands, Romania, Serbia, Slovenia, and Spain. The expert for Russia did not provide an answer to this question, but should also be considered as a *Yes*. See response to Question (1)(b)(i) for Russia. *No* was selected for Belgium, Denmark, France, Germany, Hungary, Norway, Poland, Sweden, and Turkey. No answer was provided for the United Kingdom.

<sup>204</sup> Question (5)(a)(ii) asked: “Is this list exhaustive? Please choose one: Yes/No.” *Yes* was selected for the Czech Republic, Moldova, Romania, Russia, Serbia, and Slovenia. *No* was selected for Albania, Italy, the Netherlands, and Spain.

<sup>205</sup> See response to Question (1)(b)(i) for Hungary (both the Secrecy Act and the National Security Act apply very broad terms and don’t use subcategories).

<sup>206</sup> See “additional comments” for Spain regarding Question (5)(a). Notably, in Spain, while the government must perform a test of whether the disclosure of information to an unauthorized person could threaten or harm national security or defense, the legislature does not need to perform such a test, but rather can classify information directly, and has done so in some occasions.

<sup>207</sup> Question (5)(b) asked: “Does the law prohibit any categories of information from being classified? Please choose one: Yes/No.” *Yes* was selected for 8 out of 19 (or 42% of the) responding countries: Albania, Italy, Moldova, the Netherlands, Romania, Russia, Serbia, and Slovenia. *No* was selected for 11

explicitly prohibit classification of human rights violations,<sup>208</sup> government corruption,<sup>209</sup> the existence of a government entity,<sup>210</sup> the budget or expenditures of a government entity,<sup>211</sup> the existence of a law (or portion of a law),<sup>212</sup> emergency response plans,<sup>213</sup> accidents and disasters threatening the health and security of the citizens,<sup>214</sup> and the state of the environment.<sup>215</sup> In some countries, although not explicitly prohibited, the ability to classify information such as human rights violations is reported to be unlikely.<sup>216</sup> In Sweden, for example, although such information may be properly classified for purely administrative purposes, it is noted that, upon receipt of a request for such information, it may nonetheless be determined that the public interest in disclosure warrants its release.<sup>217</sup> In addition, in several countries, information shall not be considered to be

---

out of 19 (or 58% of the) responding countries: Belgium, Czech Republic, Denmark, France, Hungary, Norway, Poland, Spain, Sweden, and Turkey. No answer was provided for the United Kingdom. Notably, in Italy, as concerns the state secrets privilege, information pertaining to acts of terrorism, mass murder, mafia-style criminal organization, subverting the constitutional order, and devastation and ransacking cannot be protected.

<sup>208</sup> See responses to Question (5)(b)(i) for Albania (prohibiting classification, though not explicitly), Moldova, the Netherlands (speculating what the administrative court would rule), Romania, Russia, and Slovenia

<sup>209</sup> See responses to Question (5)(b)(ii) for Albania (prohibiting classification, though not explicitly), Moldova, the Netherlands (speculating what the administrative court would rule), Romania, Russia, and Slovenia

<sup>210</sup> See responses to Question (5)(b)(iii) for Albania (prohibiting classification, though not explicitly), Moldova, Romania, and Russia. Contrast response to Question (5)(b) for Serbia (the classification of a government entity might be allowed if part of a secret service's operational team or a similar unit currently employed in an investigation).

<sup>211</sup> See responses to Question (5)(b)(iv) for Albania (prohibiting classification, though not explicitly), Moldova, and Romania. Contrast response to Question (5)(b) from Serbia (some budget expenditures may qualify as "secret procurements").

<sup>212</sup> See responses to Question (5)(b)(v) for Albania (prohibiting classification, though not explicitly), Italy, Moldova, Romania, Russia, Serbia, and Spain. Note, however, that in Italy regulations issued by the government concerning national security topics can be either partially or totally classified. In Serbia, after it was discovered that a secret bylaw was used, the Ombudsman reacted, asserting that all laws should be accessible.

<sup>213</sup> See responses to Question (5)(b)(vi) for Moldova and Russia.

<sup>214</sup> See response to Question (1)(b)(ii) for Russia. ("The following categories of information should not be classified: on accidents and disasters threatening security and health of citizens, as well as of natural disasters, their official prognoses and consequences, on state of environment, health care, sanitary, demography, education, culture, agriculture, and crime; on privileges, benefits and social warranties provided by the state to citizens, officials, enterprises, institutions, and organizations; on facts of violations of human and civil rights and freedoms; on volumes of gold stock and state currency reserves of the Russian Federation; on state of health of top state officials of the Russian Federation; on facts of law violation by government bodies and their officials.")

<sup>215</sup> See response to Question (1)(b)(ii) for Russia.

<sup>216</sup> See responses to Question (5)(b) for the Netherlands and Slovenia. As explained by the expert for the Netherlands, it seems very unlikely that the administrative court, interpreting the Freedom of Information Act, would allow the concealing of human rights violations or government corruption.

<sup>217</sup> See, e.g., response to Question (5)(b)(vi) for Sweden ("Information, e.g., indicating a Human Rights 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

classified if it has been designated as classified in order to conceal a criminal offense, abuse of power, or other unlawful behavior.<sup>218</sup> Nonetheless, in the majority of the surveyed countries such information can be classified.

## **VI. Judicial Review**

### *a. Authority of the Court to Review and Order the Release of Classified Information*

In nearly all (95%) of the surveyed countries, the courts have the authority to examine classified information that the government seeks to keep secret on national security grounds.<sup>219</sup> Notably, however, in some countries, only certain courts or judges with special clearance may examine classified information.<sup>220</sup> The one country that responded that courts do not ever have the authority to examine classified information was France.<sup>221</sup> According to the French expert, it is impossible for a French judge to examine classified information.<sup>222</sup> Some judges in France (both from the administrative court and the criminal court) tried to examine classified information in the past, but failed to gain access. In France, in order to limit the effect of this prohibition, the law of 1998 created the CCSDN commission, which can access classified information requested by the judge in order to evaluate whether it could be reasonable to declassify it.

---

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.”)

<sup>218</sup> See responses to Question (5)(b) for Romania, Serbia, and Slovenia. In Albania, the law also expressly prohibits classification to obstruct or delay the release of information, which does not require protection for the interest of national security.

<sup>219</sup> Question (7)(a) asked: “Do courts have the authority to examine classified information that the government seeks to keep secret on national security grounds? Please choose one: Yes/No.” *Yes* was selected for 18 of the surveyed countries: Albania, Belgium, Czech Republic, Denmark, Germany, Hungary, Italy, Moldova, the Netherlands, Norway, Poland, Russia, Serbia, Slovenia, Spain, Sweden, Turkey, and the United Kingdom. The expert for Romania left the question blank, but says that in principle, any court has the authority to examine classified information, but only judges with ORNISS clearance may actually examine a piece of classified information. Note also, in Italy, the *Yes* answer does not apply to the state secrets privilege, whose release could follow a ruling by the Constitutional Court.

<sup>220</sup> See responses to Question (7)(a) for Germany (only the Federal Administrative Court can examine classified information) and Romania (above). See also response to Question (7)(g) for Spain (although the Official Secrets Act does not contemplate access for judges, as it does for Congress and the Senate, the Spanish Supreme Court has determined that it, and only it, has the power to review the classification of information by the Government). Compare response for Poland (There is no need for special clearance for judges to have access to such type of information).

<sup>221</sup> See response to Question (7)(a) for France.

<sup>222</sup> See follow-up explanation for France. As further explained by the French expert: This is a specificity of the French situation, based on the history of the French State and of the French concept of “national defence.” Sometimes, it is also justified by the need to strictly respect the equality of information between the different parties in the court: in other words, the judge shall not be permitted to know the contents of a document that the accused is not allowed to see.

Nonetheless, in the vast majority of surveyed countries, judges are not only able to review classified information, but also are able to order the release of that information if they determine that information does not need to be kept secret, despite a public authority's assertion that national security justifies withholding the information.<sup>223</sup> As a matter of practice, however, in the majority of countries, judges normally defer to the public authority's assessment that disclosure would harm national security.<sup>224</sup> In Sweden, although courts most often agree with the assessment of the security police, it is noted that the Supreme Administrative Court has annulled the judgment of a lower court on the basis that the lower court did not examine the information and make an objective assessment of whether or not information should be kept secret, but simply accepted the reasons given by the security police.<sup>225</sup>

*b. Public Access to Court Decisions*

All (100%) of the surveyed countries require, by law, that judicial decisions be made available to the public.<sup>226</sup> In the vast majority of the surveyed countries, 16 out of 19 (or 83% of the) responding countries, national security may not justify withholding an entire court decision from the public.<sup>227</sup> Moreover, half (50%) of the surveyed countries

---

<sup>223</sup> Question (7)(a)(i) asked: "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 justified withholding the information? Please choose one: Yes/No." *Yes* was selected for 16 of the 20 surveyed countries: the Czech Republic, Denmark, Germany, Hungary, Italy, Moldova, the Netherlands, Norway, Romania, Russia, Serbia, Slovenia, Spain, Sweden, Turkey, and the United Kingdom. *No* was selected for the remaining 4 countries: Albania, Belgium, France, and Poland. As mentioned, however, in France, judges are not even permitted to review classified information.

<sup>224</sup> Question (7)(a)(ii) asked: "Do judges normally defer to the public authority's assessment that disclosure would harm national security? Please choose one: Yes/No." *Yes* was selected for 13 out of 16 responding countries: Belgium, the Czech Republic, Denmark, Hungary, Italy, Moldova, the Netherlands, Poland, Russia, Serbia, Slovenia, Turkey, and the United Kingdom. *No* was selected for Albania, Spain, and Sweden. Neither answer was selected for France, Germany, Norway, or Romania. According to the Romanian expert, there are not enough cases to infer judicial practice. The German expert, likewise, replied that he lacked sufficient information to support an empirical answer. As noted by the expert for Norway, although there have been very few cases, a judge normally will be very careful in overruling the public authority. In France, no answer was provided because judges cannot evaluate classified information.

<sup>225</sup> See response to Question (7)(a)(ii) for Sweden.

<sup>226</sup> Question (7)(b) asked: "Are judicial decisions required, according to the law, to be made available to the public (subject to redactions to protect privacy interests)? Please choose one: Yes/No." All 20 of the surveyed countries selected *Yes*.

<sup>227</sup> Question (7)(b)(ii) asked: "May national security justify withhold an entire court decision? Please choose one: Yes/No." *Yes* was selected for 3 countries: Norway, Russia, and the United Kingdom. No answer was provided for Serbia. *No* was selected for the remaining countries. As noted by the Polish expert, however, because there is no public interest exception that would allow disclosure in the public interest when the information is properly classified, there is the possibility that when a case covered by state secrecy (such as the investigation concerning Poland's involvement in the CIA's extraordinary rendition program) is considered by the court, the court's hearing will not be open to the public, and the justification of the court's judgment will be classified too.

reported that national security may not even justify withhold part of a court decision.<sup>228</sup> As explained by the expert for Italy, no part of the reasoning of the Court, which underlies a judgment, can be withheld; although due to national security reasons, the copies of the decision that are disclosed to the public can omit personal names, company names, and geographic references.<sup>229</sup> The vast majority also report that it is not possible for a court case to be kept entirely secret, such that it is not even recorded on the court's public docket.<sup>230</sup> Only Russia and the United Kingdom reported to the contrary.<sup>231</sup> In all twenty (100%) of the surveyed countries, court hearings and trials are presumptively open to the public.<sup>232</sup> Despite this presumption, however, it may be possible to close specific hearings on national security grounds.<sup>233</sup>

*c. Public and Defendant Access to Evidence in Criminal Cases*

In France, Italy, and Romania, all evidence that forms the basis of a criminal conviction must be shared with the public.<sup>234</sup> To the contrary, in the vast majority of the surveyed countries, all evidence that forms the basis of a criminal conviction does not need to be shown to the public.<sup>235</sup> As explained by the expert for Serbia, although the court, in its judgment must briefly elaborate all evidence that has led to the conviction, the public may only find out about the existence and role of this evidence in the proceedings through the written judgment, and may not have access to the evidence itself.<sup>236</sup> As explained by the expert for the Netherlands, the Code of Criminal Procedure states that trial documents that are not attached to the judgment will not be disclosed to

---

<sup>228</sup> Question (7)(b)(i) asked: "May national security justify withholding part of a court decision? Please choose one: Yes/No." *Yes* was selected for 10 of the 20 surveyed countries: Denmark, Hungary, Moldova, Norway, Poland, Russia, Serbia, Slovenia, Turkey, and the United Kingdom. *No* was selected for 10 of the 20 countries: Albania, Belgium, the Czech Republic, France, Germany, Italy, the Netherlands, Romania, Spain, and Sweden. Notably, in France, although the court decisions are always public, the judge also never has access to any information which could be classified.

<sup>229</sup> See response to Question (7)(b)(i) for Italy.

<sup>230</sup> Question (7)(d) asked: "Can a court case ever be kept entirely secret, such that it is not even recorded on the court's public docket. Please choose one: Yes/No." Only Russia and the United Kingdom answered *Yes*. The experts for the remaining countries selected *No*.

<sup>231</sup> See, e.g., response to question (7)(d) for Russia and the United Kingdom.

<sup>232</sup> Question (7)(c) asked: "Are court hearings and trials presumptively open to the public? Please choose one: Yes/No." The experts for all 20 of the surveyed countries selected *Yes*.

<sup>233</sup> See, e.g., response to Question (7)(c) for Italy and follow-up explanations provided by the expert for France.

<sup>234</sup> See response to Question (7)(e) for France, Italy, and Romania.

<sup>235</sup> Question (7)(e) asked: "Must all evidence that forms the basis of a criminal conviction be made available to the public? Please choose one: Yes/No." *No* was selected for 17 of the 20 surveyed countries: Albania, Belgium, the Czech Republic, Denmark, Germany, Hungary, Moldova, the Netherlands, Norway, Poland, Russia, Serbia, Slovenia, Spain, Sweden, Turkey, and the United Kingdom. *Yes* was selected for France, Italy, and Romania.

<sup>236</sup> See response to Question (7)(e) for Serbia.

the public: accordingly, there is no need for an exception based on national security.<sup>237</sup> Likewise, the Slovenian expert explains, evidence in criminal cases is never automatically made public: it is available only to those who show a legitimate interest and to the convicted persons; however, if inspection and copying of individual criminal files is refused for persons of interest, *e.g.*, on the basis of national security concerns, it is possible to appeal that decision.<sup>238</sup> In Belgium, on the other hand, access to criminal records is only possible with authorization of the official prosecutor, and there are no legal criteria for this decision, nor any possibility for appeal; however, after 30 years, all records must be laid down in the General Archives and for that reason become accessible to the public.<sup>239</sup>

In Spain, although hearings and trials are presumptively open to the public, and evidence that forms the basis of criminal conviction is presented and discussed during the oral trial, the press and public may be excluded from all or part of the trial in the interests of morals, public order, the protection of rights or the owed respect for the person offended or his/her family. Notably, the courts have extended the notion of public order to also include national security reasons. Accordingly, on a case-by-case basis, the judge will weigh the right of the public against the other values that must be protected, such as national security.<sup>240</sup> In Sweden, if strong reasons are provided for the court to hold a hearing in camera, the court may impose a duty of confidentiality on those who have been in attendance; however, if secret information is presented in open court, the secrecy for the information as a main rule ceases to apply.<sup>241</sup>

To the contrary, in the majority of the surveyed countries, all evidence that forms the basis of a criminal conviction must be shown to *the accused*.<sup>242</sup> Notably, in Romania, the defense lawyer must have a security clearance in order to effectively represent a defendant in a criminal trial that involves national security.<sup>243</sup> In Spain, on the other hand, there is no procedure for disclosing secret information just to the opposing party, so either the information is kept secret and the party and the judge do not have access to the

---

<sup>237</sup> Question (7)(e) also asked: “What, if any, exceptions exist on the basis of national security?” See response to Question (7)(e) for the Netherlands.

<sup>238</sup> See response to Question (7)(e) for Slovenia.

<sup>239</sup> See response to Question (7)(e) for Belgium.

<sup>240</sup> See response to Question (7)(e) for Spain (giving case examples where the court rules that closing the trial to the public was justified because very important issues for Spain and its allies were at stake and the witnesses could reveal information that would have a very negative impact on the highest interests of the State).

<sup>241</sup> See response to Question (7)(e) for Sweden.

<sup>242</sup> Question (7)(f) asked: “Must all evidence that forms the basis of a criminal conviction be shown to the accused, including in cases involving national security? Please choose one: Yes/No.” *Yes* was selected for 13 of the 20 surveyed countries: the Czech Republic, France, Germany, Hungary, Italy, Moldova, the Netherlands, Romania, Russia, Serbia, Slovenia, Spain, and the United Kingdom. *No* was selected for the remaining 7 countries: Albania, Belgium, Denmark, Norway, Poland, Sweden, and Turkey.

<sup>243</sup> See response to Question (7)(f)(i) for Romania.

evidence, or the information is declassified by order of *the* Supreme Court and is incorporated into the case and becomes public.<sup>244</sup> In Sweden, although the accused may not have access to all documents underlying the judgment or decision, secrecy can never apply to the judgment or a decision itself, nor may secrecy limit a party's right to have access to information on factors which are of significance to the judgment or decision.<sup>245</sup>

There has been extensive European Court of Human Rights case law on this issue from the United Kingdom, and as a result, in the U.K., “enhanced judicial trial management” is compulsory in terrorism trials.<sup>246</sup> According to case law from the U.K. House of Lords, sufficient material must be disclosed to the party to enable him to give effective instructions to his legal representative.<sup>247</sup> In cases involving liberty or property interests, if these disclosure obligations cannot be satisfied, the charges must be dropped. However, in “mere” equality or non-discrimination cases, this degree of disclosure will not always be required.<sup>248</sup> Notably, in the United Kingdom, there is also the possibility of utilizing non-criminal alternatives, such as control orders and TPIMS (Terrorism Prevention and Investigation Measures), and disclosure obligations in these circumstances are lesser.<sup>249</sup> Likewise, in Poland, there are no procedural guarantees akin to the accused's right to see classified documents in an administrative proceeding. In a deportation hearing, for example, the court has upheld that the document that constituted the basis for the deportation was unseen by both the defendant and his attorney.<sup>250</sup>

#### *d. Access to Information in Other Proceedings*

In almost half of the surveyed countries, the government may refuse to disclose information to the opposing party on the basis of national security in a *habeas corpus* case.<sup>251</sup> In slightly more than half of the surveyed countries, the government may refuse

---

<sup>244</sup> See response to Question (7)(g) for Spain.

<sup>245</sup> See response to Question (7)(f)(ii) for Sweden.

<sup>246</sup> See response to Question (7)(f)(i) for the United Kingdom (citing the Criminal Procedure and Investigations act 1996; the Terrorism act 2006, s 16, and European Court of Human Rights case law on Article 6).

<sup>247</sup> See response to Question (7)(f)(iii) for the United Kingdom (There are a variety of closed material procedure (statutory) proceedings, as well as (common law) cases involving public interest immunity. The former is liable to be significantly extended when the Justice and Security Bill, currently before the UK Parliament, is enacted. The leading cases on disclosure are AF (No 3) in the House of Lords and Tariq in the Supreme Court; see also Conway v. Rimmer and ex parte Wiley for disclosure under public interest immunity).

<sup>248</sup> See response to Question (7)(f)(iii) for the United Kingdom (citing Tariq)

<sup>249</sup> See response to Question (7)(f)(i) for the United Kingdom (citing A v UK in the European Court of Human Rights and AF (No 3) in the House of Lords).

<sup>250</sup> See point 6 of the “additional comments” for Poland.

<sup>251</sup> Question (7)(g)(i) asked: “May the government refuse to disclose information to the opposing party in [a *habeas corpus* claim] on the basis of national security? Please choose one: Yes/No.” *No* was selected for 10 out of 19 responding countries: the Czech Republic, France, Germany, Hungary, Italy, Moldova, the Netherlands, Romania, Serbia, and Slovenia. *Yes* was selected for 9 out of 19 responding countries:

such disclosure in a case claiming grave human rights violations (such as torture) brought against a public authority.<sup>252</sup> Additionally, in the majority of the surveyed countries, the government may refuse disclosure in a tort claim brought against a public authority.<sup>253</sup> In several of the surveyed countries, however, the government may not withhold this information in the face of a court decision to the contrary.<sup>254</sup> In Denmark, for example, the decision to withhold information cannot be taken if it implies serious risks for the fairness of the proceeding.<sup>255</sup> In Spain, the Supreme Court, balancing the rights at stake with the national security interests, can decide that the government must disclose the information to the opposing party.<sup>256</sup> In Italy, if the prosecutor believes that the evidence covered by the state secrets privilege is not essential to reaching the final decision, s/he will go on with the trial; however, if the judicial authority disagrees, the judicial authority will raise a conflict of powers claim against the executive before the Constitutional Court.<sup>257</sup> Notably, in Italy, while the state secrets privilege can be successfully invoked before Courts to withhold information or a document, this does not happen regarding other classified information.<sup>258</sup>

*e. Dismissal on the Basis of the State Secrets Privilege*

In the vast majority (85%) of the surveyed countries, the judge is not permitted to dismiss a case, without reviewing the case on its merits, because reviewing the case would involve state secrets.<sup>259</sup> Hungary, Italy, and the United Kingdom are the exception.

---

Albania, Belgium, Denmark, Norway, Poland, Russia, Spain, Sweden, and Turkey. No answer was provided for the United Kingdom because there are so few habeas corpus cases that no clear answer could be discerned.

<sup>252</sup> Question (7)(g)(ii) asked: “May the government refuse to disclose information to the opposing party in [a claim of grave human rights violations (e.g., torture) brought against a public authority] on the basis of national security? Please choose one: Yes/No.” *Yes* was selected for 10 of the surveyed countries: Belgium, Denmark, Italy, Norway, Poland, Russia, Spain, Sweden, Turkey, the United Kingdom. *No* was selected for 8 of the surveyed countries: Czech Republic, France, Germany, Moldova, the Netherlands, Romania, Serbia, and Slovenia. In Hungary, the answer depends on what type of proceeding the claim is made in.

<sup>253</sup> Question (7)(g)(iii) asked: “May the government refuse to disclose information to the opposing party in [a tort claim brought against a public authority] on the basis of national security? Please choose one: Yes/No.” *Yes* was selected for 14 of the surveyed countries: Belgium, Denmark, Germany, Hungary, Italy, the Netherlands, Norway, Poland, Russia, Serbia, Spain, Sweden, Turkey, the United Kingdom. *No* was selected for 5 countries: the Czech Republic, France, Moldova, Romania, Slovenia.

<sup>254</sup> Question (7)(g) also asked: “If you checked ‘Yes’ for any of the above, please indicate what safeguards, if any, are in place to protect the fairness of the proceedings.” *See* responses to Question (7)(g) for Albania, Belgium, the Netherlands, and Poland.

<sup>255</sup> *See* response to Question (7)(g) for Denmark.

<sup>256</sup> *See* “feedback on draft report” for Spain.

<sup>257</sup> *See* response to Question (7)(g) for Italy.

<sup>258</sup> *See* “additional comments” for Italy.

<sup>259</sup> Question (7)(h) asked: “Can a judge dismiss a case, without reviewing the case on its merits, because reviewing the case would involve state secrets? Please choose one: Yes/No.” *No* was selected for 17 of the 20 surveyed countries: Albania, Belgium, the Czech Republic, Denmark, France, Germany, Moldova, the

## VII. Autonomous Oversight Bodies

In the majority of the surveyed countries, an autonomous oversight body exists with authority to review classification decisions by security sector, defense, and intelligence agencies.<sup>260</sup> However, in several of the countries, the oversight body is not entirely independent.<sup>261</sup> A wide variety of oversight bodies exist:<sup>262</sup> with some countries having Parliamentary oversight<sup>263</sup> and others having oversight by the Ombudsman,<sup>264</sup> the Information Commissioner,<sup>265</sup> or another national authority or inter-departmental committee.<sup>266</sup> The powers of these bodies also range considerably from country to country. In France, the oversight body does not take up inquiries of its own initiative, but can only review a classification decision if declassification is sought by a judge in connection with a judicial proceeding.<sup>267</sup> In both Germany and Slovenia, the Commissioner can either act on its own motion or examine citizens' complaints of denied access to information, but in Germany, the Commissioner can only publish non-binding opinions or issue "reclamations" to be published in its biannual report,<sup>268</sup> whereas, in Slovenia, the Commissioner can mandate declassification.<sup>269</sup> In Spain, the National Intelligence Centre is required to annually inform the Parliament Committee about its

---

Netherlands, Norway, Poland, Romania, Russia, Serbia, Slovenia, Spain, Sweden, and Turkey. *Yes* was selected for the remaining 3 countries: Hungary, Italy, and the United Kingdom.

<sup>260</sup> Question (8)(a) asked: "Is there any autonomous oversight body with authority to review classification decisions by security sector, defence, and intelligence agencies? Please choose one: Yes/No." *Yes* was selected for 12 out of 19 responding countries: Czech Republic, France, Germany, Hungary, Italy, Moldova, the Netherlands, Norway, Poland, Serbia, Slovenia, and Spain. *No* was selected by Albania, Belgium, Denmark, Romania, Russia, Sweden, and Turkey. No answer was provided for the United Kingdom. Notably, in Sweden, where classification is purely administrative: there is an autonomous oversight body with competence to oversee certain aspects of the work of the Security Police: this board reviews security screening decisions, but not decisions to classify information. In Romania, ORNISS may assist in reviewing classification decisions, but it is not autonomous, nor an oversight body. In Italy, the affirmative answer regards only the state secrets privilege.

<sup>261</sup> See responses to Question (8)(a)(i) for the Czech Republic ("It is dependent of the government") and Italy ("the oversight body is not entirely independent") and response to Question (8)(a)(ii) for Hungary ("It's President is appointed by the Prime Minister.").

<sup>262</sup> Question (8)(a)(i) asked: "Identify the body. What are its mandates and powers?" See responses for the Czech Republic (National Security Authority), France (CCSDN - Consultation Commission for National Defence Secrecy), Germany (Federal Commissioner for Data Protection and Freedom of Information), Hungary (National Authority for Data Protection and Freedom of Information), Italy (Parliamentary Committee for the Intelligence and Security Services (COPASIR)), Moldova (inter-department commission for state secrets), the Netherlands (Dutch Review Committee on the Intelligence and Security Services), Norway (Norwegian Parliamentary Intelligence Oversight Committee), Poland (national classification authority), Serbia (the Ombudsperson, Commissionaire, State audit institution, and Anti-corruption agency), Slovenia (Information Commissioner), and Spain (the Parliament and the Ombudsmand).

<sup>263</sup> See responses to Question (8)(a)(i) for Italy, Norway, and Spain.

<sup>264</sup> See responses to Question (8)(a)(i) for Serbia and Spain.

<sup>265</sup> See responses to Question (8)(a)(i) for Germany, Serbia, and Slovenia.

<sup>266</sup> See responses to Question (8)(a)(i) for Moldova and Poland.

<sup>267</sup> See response to Question (8)(a)(ii) for France.

<sup>268</sup> See response to Question (8)(a)(i) and (ii) for Germany (the Commissioner does not have the power to declassify information; sending a "reclamation" is the Commissioner's "sharpest sword").

<sup>269</sup> See response to Question (8)(a)(i) for Slovenia.

activities, but these reports tend to be very general and vague: as a result, the Committee usually develops more of an ex post oversight than an ex ante control.<sup>270</sup>

For all of the oversight bodies, access to classified information is essential to enabling their review: however, the extent of access varies, and only some of the oversight bodies have unlimited access.<sup>271</sup> In the Netherlands, the Dutch Review Committee on the Intelligence and Security Services has access to all relevant information of the services and may make inquiries of all of the staff of the services as well. Furthermore, the Committee has the right to hear witnesses under oath or to call experts and may access all places which it deems necessary to access in the context of its task, with the exception of dwellings.<sup>272</sup> In Spain, a significant exception to access exists, insofar as the Committee is not given access to any classified information coming from a foreign secret service.<sup>273</sup> Also, in Spain, the Government can decide through a written agreement that secret documents shall not be shared with the Ombudsman: if the Ombudsman thinks this denial seriously interferes with his investigation, he will notify the Congress-Senate Committee, so that Parliament can act.<sup>274</sup> In Italy, if two-thirds of the relevant Parliamentary Committee decide to carry out an investigation, the Government cannot invoke secrecy and the Committee must be granted the right to access all information and documentation; however, this is a recent development in Italy: previously, the Committee had to vote unanimously in order for such access to be ensured.<sup>275</sup> Also notably, in Serbia, access to classified information is given only to the head of the relevant institution,<sup>276</sup> and in Spain, only some MPs, the Ombudsman himself, and his deputy have access (and they cannot be accompanied by any advisor or technical expert);<sup>277</sup> whereas, in Slovenia, employees of the Information Commissioner's institution may acquire permission to access classified information as well.<sup>278</sup>

## **VIII. Criminal Prosecutions of Public Personnel**

### *a. Criminal Penalties for Unauthorized Disclosure*

---

<sup>270</sup> See response to Question (8)(a)(ii) for Spain.

<sup>271</sup> Question (8)(a)(ii) asked: "What, if any, limitations are there on this body's ability to review classified information?" Compare responses for the Czech Republic (none) and Norway (There are no limitations) with Poland (The national security authority are limited to checking the premises of the organizational units, controlling documents related to the protection of classified information, and demanding clarifications from the heads and employees of branch authorities) and Germany (I did not come across any information confirming that the Commissioner and staff have examined classified information themselves).

<sup>272</sup> See response to Question (8)(a)(i) and (ii) for the Netherlands

<sup>273</sup> See response to Question (8)(a)(ii) for Spain.

<sup>274</sup> See response to Question (8)(a)(ii) for Spain.

<sup>275</sup> See response to Question (8)(a)(i) for Italy.

<sup>276</sup> See response to Question (8)(a)(ii) for Serbia.

<sup>277</sup> See response to Question (8)(a)(ii) for Spain.

<sup>278</sup> See response to Question (8)(a)(i) for Slovenia (The Information Commissioner has access to information without permission).

All twenty (100%) of the surveyed countries provide that public personnel who have been granted authorized access to classified national security information may be criminally charged for disclosing that information to the public.<sup>279</sup> Moreover, fifteen of the surveyed countries report that charges have been brought against public personnel for the disclosure of classified information within the past twenty years.<sup>280</sup> Nonetheless, in the majority of the surveyed countries, there have been very few such cases,<sup>281</sup> and convictions have been even rarer.<sup>282</sup> Notably, in Sweden, the law expressly states that petty cases will not be punished.<sup>283</sup>

The elements of this offense vary between countries,<sup>284</sup> with some countries prosecuting only intentional disclosure and others prosecuting negligent disclosure as well.<sup>285</sup> Some countries require a showing of endangerment of an important public

---

<sup>279</sup> Question (9)(a) asked: “May public personnel who have authorized access to classified national security information may be subject to criminal penalties if they disclose that information to the public? Please choose one: Yes/No.” The experts for all twenty countries selected *Yes*.

<sup>280</sup> Question (9)(b) asked: “Have any public personnel been charged with a crime for disclosing classified national security information in the past two decades? Please choose one: Yes/No.” *Yes* was selected for 15 out of 19 responding countries: the Czech Republic, Denmark, France, Germany, Hungary, Italy, Moldova, the Netherlands, Romania, Russia, Serbia, [Slovenia], Spain, Sweden, and the United Kingdom. In 4 countries, there have been no such charges: Albania, Belgium, Norway, and Turkey. Also, in Poland, there was no available data in this regard. For Turkey, the National Criminal Convictions Database only contains data for 2006-2011, but no prosecutions or convictions were reported therein; moreover, an extensive media search did not yield any such reports either.

<sup>281</sup> Question (9)(b)(i) asked: “If you checked Yes [to Question (9)(b)], approximately how many prosecutions have there been?” See responses to Question (9)(b)(i) for the Czech Republic (one); Denmark (one); Italy (one); the Netherlands (only a few); Sweden (a few, perhaps one every two years). Notably, the highest count reported was about a dozen: see responses to Question (9)(b)(i) for Romania (No prosecutions have been reported by the prosecution, but about a dozen cases were reported in the media, which include other related offenses, such as espionage, undermining the national economy, and treason, as opposed to disclosure of state secrets); Russia (eleven); the United Kingdom (Public personnel were charged in 5-10 instances, but only 3-5 of these resulted in prosecution; the rest were dropped). Notably, in Germany, according to statistics published by the Federal Criminal Police Office on an annual basis, from 1998 to 2011, each year there were more than 100 cases (ranging from 130 in 1998 to 307 in 2009) of breaches of “official secrets;” however, these crime statistics only count crimes investigated by the police, and do not indicate how many persons were eventually prosecuted and sentenced. See response to Question (9)(b)(i) for Germany; see also follow-up from Nils Leopold for Germany (warning against relying on these numbers).

<sup>282</sup> Question (9)(b)(ii) asked “If you checked Yes [to Question (9)(b)], approximately how many convictions have there been, and what punishments were imposed, if any?” See responses to Question (9)(b)(ii) for the Czech Republic (none); Denmark (one); Italy (no record of conviction); the Netherlands (only a few); Romania (none); Spain (none for disclosing classified information, but two on related charges); Sweden (none known). See also responses from Russia (10) and the United Kingdom (3-5).

<sup>283</sup> See response to Question (9)(a)(ii) for Sweden.

<sup>284</sup> Question (9)(a)(ii) asked: “If you checked Yes [to Question (9)(a)], what must the government prove in order to obtain a conviction?”

<sup>285</sup> Compare responses to Question (9)(a)(ii) for Belgium (intentional), Denmark (intentional), the Netherlands (intentional), Romania (intentional) with response for Italy (intentional and negligent), Slovenia (intentional and negligent), and Sweden (intentional and negligent).

interest.<sup>286</sup> In the Netherlands, it must also be shown that the person knew, or reasonably expected, that the secrecy of the information was vital to the interests of the state or its allies.<sup>287</sup> In Poland, knowing receipt of the information by an unauthorized person is also an element of the offense.<sup>288</sup> In a few of the countries, the offense is universal, and applies to any unauthorized disclosure, whereas, in others, the offense is limited to disclosure by a person who had a duty to protect the secrecy of the information.<sup>289</sup>

Notably, in at least some of the countries, the charges brought in the past two decades were not for the disclosure of classified information, as such, but rather for other related crimes, such as espionage,<sup>290</sup> or the improper handling of classified information.<sup>291</sup> In addition, in some countries, short of criminal prosecution, public personnel have been investigated or otherwise sanctioned.<sup>292</sup> Thus, in both Norway and the Czech Republic, administrative (*i.e.*, non-criminal) punishments, such as fines, have occasionally been imposed.<sup>293</sup> Likewise, in Denmark, in one case, although no charges were brought, a member of the military was suspended from his position, and the Ministry of Defense sought to interfere with his publication of a book containing the information at issue.<sup>294</sup>

While all of the surveyed countries recognize the unauthorized disclosure of classified information by public personnel as a crime, how severely this offense may be punished also varies considerable from country to country. The maximum penalty that can be imposed on public personnel who disclose classified information ranges from two

---

<sup>286</sup> See, *e.g.*, responses to Question (9)(a)(ii) for Germany, Italy, the Netherlands, Romania, and Spain.

<sup>287</sup> See response to Question (9)(a)(ii) for the Netherlands.

<sup>288</sup> See response to Question (9)(a)(ii) for Poland (In order for an action to be punishable it must cause an effect – *e.g.* disclosing information to at least one, not authorized person, by giving access to a document or any other classified as secret object is punishable when the person actually becomes familiar with its meaning.)

<sup>289</sup> Compare response to Question (9)(a)(ii) for Poland (it is a universal crime; it is not limited to persons who have an access certificate) with response for Slovenia (the offence is committed by an official or any other person who had a duty to protect classified information) and France (disclosure is made by someone officially holding such classified information). See also “additional comments” for the Netherlands (the Criminal Code makes no distinction between a disloyal employee and a journalist).

<sup>290</sup> See response to Question (9)(b)(i) for Romania.

<sup>291</sup> See response to Question (9)(b)(i) for Spain (None for disclosing classified information, but a couple of cases for unlawfully taking away documents from the National Intelligence Centre). Notably, in Germany, there were 37 instances of treason and causing risk to the national security investigated in 2000 alone, in addition to the above-mentioned investigations for breach of official secrets.

<sup>292</sup> Question (9)(b)(ii) also asked “If you checked No [to Question (9)(b)], 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?” Of the countries that checked *No* to Question (9)(b), the experts for Norway responded *Yes*, Albania and Belgium responded *No*, and Turkey did not respond. The experts for the Czech Republic and Denmark also responded *Yes*. The experts for the other countries did not respond, but had answered *Yes* to Question (9)(b).

<sup>293</sup> See responses to Question (9)(b)(ii) for Norway and the Czech Republic.

<sup>294</sup> See response to Question (9)(b)(ii) for Denmark.

years of imprisonment (see, *e.g.*, Denmark) to life imprisonment (see, *e.g.*, Turkey).<sup>295</sup> Several factors, such as whether the information was disclosed during wartime, by a member of the armed forces, or with the purpose of favoring a foreign country, may also bear on the severity of the punishment available.<sup>296</sup>

*b. Disclosures Made Internally or to an Independent Oversight Body*

In the majority of the surveyed countries, public personnel may be prosecuted if they disclose classified national security information in making a complaint internally to someone within their own ministry, department, or unit.<sup>297</sup> As noted by both the experts for Spain and Serbia, such prosecution is only possible, however, if the person that receives the information was not entitled to receive the information.<sup>298</sup>

In several countries, public personnel are actively encouraged to make internal complaints.<sup>299</sup> However, few countries seem to have established safeguards to provide

---

<sup>295</sup> Question (9)(a)(i) asked: “What is the maximum penalty for this crime?” See response for Albania (10 years if disclosed publicly); Belgium (5 years and a fine of 30,000 Euros); Czech Republic (12 years); Denmark (2 years); France (7 years and a fine of 100,000 Euros); Germany (15 years for treason; 5 years for violation or publication of official secrets); Hungary (15 years for disclosing Top Secret information to a foreign person); Italy (5 years for disclosure of state secrets, 10 years if during wartime, life if constitutes espionage; for disclosure of other classified information, 3 years, 10 years if during wartime, 15 years for espionage, life if espionage during war; for negligent disclosure, 2 1/2 years, 15 years if during wartime); Moldova (if not espionage or treason, 5 years; if resulted in serious consequences, 10 years plus inability to hold certain offices for up to 5 years); Netherlands (15 years; if during wartime, life); Norway (10 years); Poland (8 years if acting on behalf of a foreign entity); Romania (15 years); Russia (20 years); Serbia (15 years); Slovenia (3 years, 5 year if committed out of greed, 1 year if the result of negligence); Spain (4 years, 10 years for members of armed forces, 12 years if to favor a foreign country, 25 years if to favor a foreign country and by a member of armed forces); Sweden (4 years for aggregated disclosure of very secret information); Turkey (life); United Kingdom (2 years).

<sup>296</sup> See, *e.g.*, responses to Question (9)(a)(i) for Italy, Moldova, the Netherlands, Poland, and Sweden.

<sup>297</sup> Question (9)(d) asked: “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? Please choose one: Yes/No.” *Yes* was selected for 12 out of 18 responding countries: Belgium, the Czech Republic, France, Hungary, Moldova, Norway, Poland, Romania, Russia, Slovenia, Spain, and Sweden. *No* was selected for 5 countries: Denmark, Germany, Italy, the Netherlands, and the United Kingdom. Notably, however, in Italy, a disciplinary procedure is possible. No answer was provided for Albania or Turkey.

<sup>298</sup> See response to Question (9)(d) for Serbia and “additional comments” for Spain.

<sup>299</sup> Question (9)(f) asked: “Are public personnel encouraged to make internal disclosures when they encounter information about government wrongdoing? Please choose one: Yes/No.” *Yes* was selected for Belgium, Germany, Moldova, and the United Kingdom. Although the experts for the other countries did not select *Yes*, in several of these countries, there appear to be practices which would constitute encouragement. In Italy, for example, public officials are duty-bound to report crimes they become aware of. In the Czech Republic, in some offices, internal regulations order reporting on wrongdoing, but there is not a duty to disclose, as such. In Hungary, whistleblower protection laws call for whistleblowers to be financially rewarded; notably, however, no authority has yet been designated to implement the whistleblower laws.

protection against retaliation.<sup>300</sup> To the contrary, in the United Kingdom, the Public Interest Disclosure Act provides for compensatory remedies, in addition to internal disciplinary means, in the event of retaliation.<sup>301</sup>

Nearly one-third (30%) of the surveyed countries have an independent body designated to receive complaints involving classified information.<sup>302</sup> In general, disclosures made to such a body are protected:<sup>303</sup> however, in some of the countries, the independent body may not be approached until an internal complaint has been made first.<sup>304</sup> In several countries, public personnel have a duty to report criminal wrongdoing.<sup>305</sup> In Romania, the criminal code provides a penalty up to 5 years in jail for omitting to report a crime related to the activity of one's own institution; if the omission belongs to someone in a management or control position, the penalty may go up to 7 years.<sup>306</sup>

---

<sup>300</sup> Question (9)(f)(iii) asked: "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? Experts for only 6 countries provided responses: five of them indicated that there were no specific penalties set forth in legislation. See response from Albania (legislation is vague and there is no recorded practice); Belgium (no real sanctions unless the actions are themselves crimes), Czech Republic (none); Denmark (no specific regulations); Romania (no explicit penalties, but there may be opportunities for judicial recourse for the victim). Compare response for the United Kingdom.

<sup>301</sup> See response to Question (9)(f)(iii) for the United Kingdom.

<sup>302</sup> Question (9)(e) asked: "Is there an *independent* body, expressly designated to receive complaints involving classified information from public personnel? Please choose one: Yes/No." *Yes* was selected for 6 of the 20 surveyed countries (30%): Belgium, Hungary, the Netherlands, Serbia, Slovenia, and the United Kingdom. *But see* clarification for the United Kingdom (The answer depends on what is meant by "independent". Disclosure may lawfully be made to the staff counselor; to the Attorney General, Director of Public Prosecutions or Commissioner of the Metropolitan Police; or to the Prime Minister, Foreign Secretary or Home Secretary.) See also response for Germany (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, but the Commissioner can issue only non-binding opinions and complaints issued to the Commissioner are not an instrument of legal redress. Thus, the only independent institutions where the classification of documents could be reviewed are administrative courts.)

<sup>303</sup> Question (9)(e)(i) asked: "If you checked Yes [for Question (9)(e)], are public personnel prosecutable if they disclose classified national security information to the designated independent body?". See responses for Belgium (no), Hungary (it is unclear), the Netherlands (no), Serbia (it depends), and the United Kingdom (no).

<sup>304</sup> Question (9)(e)(ii) asked "If you checked Yes [for Question (9)(e)], Must such personnel complain internally before approaching the independent body?" See response to Question (9)(e)(ii) for Serbia (if the Ombudsman is addressed, there is a need to first exhaust possible means prior to asking for the Ombudsman's intervention) and Hungary (Protections do not differ, as in practice no effective protection is offered to any whistleblower, in any sector. Reporting channels differ: 'If a member of any intelligence agency becomes aware unlawful activities of the agencies he/she is allowed to report it to the minister. The minister shall examine the report and inform the Committee).

<sup>305</sup> See response to Question (9)(f)(i) ("How are internal disclosures encouraged?") and Question (9)(f)(ii) ("Do public personnel have a duty to disclose information of governmental wrongdoing to an internal or designated independent body?")

<sup>306</sup> See response to Question (9)(f)(ii) for Romania.

### *c. Information in the Public Domain*

In several countries, prosecution for the unauthorized disclosure of classified information may occur, even if that information is already available in the public domain.<sup>307</sup> According to the Spanish expert consulted in this study, information does not automatically lose its classified status by becoming public, and the government may prove, even after its publication, that further dissemination can still pose a threat or harm to national security.<sup>308</sup> In Denmark, in at least one case, the court has punished a public servant for leaking classified information, even though the information could “rather easily” be obtained from public sources on the internet.<sup>309</sup> Likewise, in Russia, in at least one case, a public servant was convicted, despite a showing by the defense that the information could have been obtained from the public domain.<sup>310</sup> Nonetheless, as noted by the expert for Sweden, although the government may, in principle, prosecute for revealing national security information which has previously entered the public domain, the courts in such cases would be likely to rule that no further damage to the national security has occurred, and so acquit.<sup>311</sup>

### *d. Defenses against Criminal Penalties*

#### 1. The Public Interest in Disclosure

Although the majority of the surveyed countries report that national law does not take the public’s interest in the disclosure of the information into consideration when deciding whether to penalize the disclosure,<sup>312</sup> a few do have a public interest test. In Denmark, for example, the public interest test requires that the accused was disclosing information in order to achieve an obvious public interest and that this interest shall

---

<sup>307</sup> Question (10)(f) asked: “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 choose one: Yes/No. If you checked Yes, please explain what is required for the government to prevent or sanction dissemination of this information.” *See, e.g.*, response for Italy (The President of the Council of Ministers may confirm the assertion of the state secrets privilege in a criminal trial, even if the information has already been disclosed to the public.)

<sup>308</sup> *See* response to Question (10)(f) for Spain.

<sup>309</sup> *See* response to Question (10)(f) for Denmark (citing the case of Frank Grevil).

<sup>310</sup> *See* response to Question (10)(f) for Russia (citing the case of Igor Sutyagin).

<sup>311</sup> *See* response to Question (10)(f) for Sweden; *see also* response for the United Kingdom (citing the Spycatcher case, regarding the inability to quell publication, where there has been prior publication).

<sup>312</sup> Question (9)(a)(iii) asked: “Does the law take the public’s interest in the disclosure of the information into consideration when deciding whether to penalize the disclosure? Please choose one: Yes/No.” *Yes* was selected for Denmark, the Netherlands, and Sweden. *No* was selected for Albania, Belgium, the Czech Republic, France, Germany, Hungary, Italy, Moldova, Norway, Poland, Romania, Russia, Serbia, Slovenia, Spain, Turkey, and the United Kingdom. *But see* response to Question (9)(f) for Moldova (according to the law on access to information, no one can be punished for making public information with limited accessibility, in the case when the disclosure of information does not or may not harm a legitimate interest related to state security or the public interest to know this information is bigger than the prejudice caused by the disclosure of information).

exceed the interest in keeping the information secret.<sup>313</sup> In addition, in other countries, related challenges may be raised in defense of unauthorized disclosures. As noted by the expert for the Netherlands, although the criminal code itself does not mention a public interest defense, a suspect could submit that his conviction would violate Article 10 of the European Convention of Human Rights. As such, the factors mentioned in the case law of the European Court, see, in particular, *Guja v. Moldova*, may be considered.<sup>314</sup> In Hungary, although the criminal code does not have a public interest test, it is a requirement for any criminal offence that the concrete act adjudicated by the court has to be dangerous to society: where there is a stronger public interest in disclosure than in withholding information, this prerequisite can be an effective argument of the defense.<sup>315</sup> In addition, in Sweden, although there is not a public interest defense, the burden is on the prosecution to show that the information falls properly within the exception and that “damage” to national security has occurred.<sup>316</sup>

## 2. The Lack of Actual or Probable Harm

Most of the surveyed countries require a showing of either actual or probable harm resulting from the disclosure in order for a penalty to be imposed.<sup>317</sup> Of those that do not require such a showing, one-third allow the lack of harm to be raised as a defense or mitigating circumstance.<sup>318</sup> In Hungary, a person who commits an act in the erroneous belief that it is not dangerous for society and who has reasonable grounds for this hypothesis shall not be punished.<sup>319</sup>

---

<sup>313</sup> See response to Question (9)(a)(iii)(2) for Denmark. Question (9)(a)(iii)(1) asked: “If you checked Yes [to Question (9)(a)(iii)], who bears the burden of proof in regard to whether the disclosure was in the public interest?” and Question (9)(a)(iii)(2) asked: “What factors must be present to meet this burden?”

<sup>314</sup> ECHR (GC) 12 February 2008, *Guja v. Moldova*, par. 73-78

<sup>315</sup> See response to Question (9)(a)(iii) for Hungary.

<sup>316</sup> See response to Question (9)(a)(iii) for Sweden.

<sup>317</sup> Question (9)(a)(iv) asked: “Is a showing of either actual or probable harm to national security, resulting from the disclosure, required for a penalty to be imposed? Please choose one; Yes, actual / Yes, probable / No, neither.” One out of 19 responding countries selected *Yes, actual*. That country was Moldova. Nine out of 19 responding countries selected *Yes, probable*. Those countries were Albania, Czech Republic, Germany, Italy, the Netherlands, Norway, Romania, Spain, and Sweden. According, 10 out of the 19 responding countries (53%) require a showing of harm. The remaining 9 countries (47%) do not require any showing of harm: Belgium, Denmark, France, Hungary, Poland, Russia, Slovenia, Turkey, and the United Kingdom.

<sup>318</sup> Question (9)(a)(iv) also asked: “If you checked “No,” is it a defense or mitigating circumstance that the disclosure did not harm national security?” *Yes* was selected for 3 of the 9 countries: Hungary, Denmark, and France. The other 6 countries (Belgium, Poland, Russia, Slovenia, Turkey, and the United Kingdom) responded *No*.

<sup>319</sup> See response to Question (9)(a)(iv) for Hungary.

### 3. Using Internal Reporting Procedures

Nearly one-third (30%) of the surveyed countries provide a defense for having used, or tried to use, internal reporting procedures before making the information public.<sup>320</sup> Notably, in Albania, what constitutes adequate exhaustion of the internal procedures varies with and is defined by each department or ministry.<sup>321</sup> In France, although using the internal reporting procedures does not provide a defense, a showing that the internal reporting procedures are ineffectual is.<sup>322</sup> In at least some of these countries, it may also be a defense or mitigating circumstance that the personnel had a good faith belief that using the internal reporting procedures would be ineffectual, or would result in retaliation.<sup>323</sup> In Serbia, it is not a requirement that one use the internal reporting procedures, but rather only that the whistleblower acted in good faith: a showing of good faith might be achieved by using or attempting to use the internal procedures, but may also be achieved in other ways, including conceivably by having the good faith belief that such procedures would result in retaliation.<sup>324</sup>

#### *e. Criminal Penalties for Disclosure by Persons without Authorized Access*

The vast majority of the surveyed countries also provide criminal penalties for disclosure of classified information by persons without authorized access to that information<sup>325</sup> In several countries, the criminal offense is the same, regardless of whether the disclosure was made by someone with authorized access to the information

---

<sup>320</sup> Question (9)(a)(v) asked: “Is it a defense 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?” *Yes* was selected for 6 of the 20 surveyed countries (i.e., 30%): Albania, Germany, the Netherlands, Romania, Serbia, and the United Kingdom. Notably, in the U.K., it would not be a defense, but may be a mitigating circumstance; however, this point has not been definitively decided yet, as the leading case did not involve using the staff counselor. *No* was selected for the other 14 countries: Belgium, Czech Republic, Denmark, Hungary, France, Italy, Moldova, Norway, Poland, Russia, Slovenia, Spain, Sweden, and Turkey.

<sup>321</sup> See response to Question (9)(a)(v) for Albania.

<sup>322</sup> See responses to Question (9)(a)(v) and (vi) for France.

<sup>323</sup> See responses to Question (9)(a)(vi) for Germany, the Netherlands, and Romania. Notably, in France, even though the use of the internal procedure itself is not a defense or mitigating circumstance, it may be a defense 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. The expert for Serbia also explains that the question is whether the whistleblower was acting in good faith: in support thereof an argument could be made that one believed in good faith that using internal procedures would cause retaliation. No answer was provided by Moldova.

<sup>324</sup> See response to Question (9)(a)(vi) for Serbia.

<sup>325</sup> Question (10)(a) asked: “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 that information to the public? Please choose one: Yes/No.” *No* was selected for Germany and Moldova. Although *Yes* was selected for Belgium, the Belgian expert says, “In principle, [there are] no sanctions for persons that do not have authorized access to that information.” *Yes* was selected for the other 17 countries. But see follow-up for Germany, which suggests that Section 353b of the penal code has been applied broadly to any unauthorized disclosure.

or not.<sup>326</sup> Where disclosure by such persons is not criminalized, such persons may instead be charged for related crimes, such as soliciting criminal disclosure by someone with authorized access.<sup>327</sup> Nonetheless, in the majority of the surveyed countries, a showing of either actual or probable harm, resulting from the disclosure, is required in order for a penalty to be imposed.<sup>328</sup> Notably, when it comes to penalizing persons without authorized access to the information, both Moldova and the United Kingdom require a showing of actual harm. Some also recognize the lack of harm as a defense or mitigating circumstance.<sup>329</sup> Belgium, Poland, Russia, Slovenia, and Turkey do not recognize this defense, although claims may be made, for example, that the information was not classified in accordance with the law.<sup>330</sup>

*f. Criminal Penalties for Unauthorized Possession*

In the majority of the surveyed countries, criminal penalties may be imposed for the possession of classified information by a person who did not have authorized access to that information (such as a journalist).<sup>331</sup> The maximum penalty for this crime ranges from three to twenty years imprisonment, although the higher end penalties may refer to espionage or other related crimes, rather than mere possession.<sup>332</sup> In Slovenia, the

---

<sup>326</sup> See (9)(a)(ii) for Poland. (The judgment of the Supreme Court of 26 March 2009, I KZP 35/08, states that an offense under Article 265(1) may be committed by any person who became familiar with the classified information or by whom the information was confined. Thus, it is a universal crime; it is not limited to persons who have an access certificate for classified information. However, this is not a binding interpretation and is broadly criticized.)

<sup>327</sup> See, e.g., additional comment for Germany (it is still a crime to instigate a violation of official secrets); see also response to Question (10)(a)(i) for Belgium (e.g., helping to steal information).

<sup>328</sup> Question (10)(a)(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 choose one: Yes, actual / Yes, probable / No, neither. *Yes, actual* was selected for 2 out of 18 (or 11% of the) responding countries: Moldova and the United Kingdom. *Yes, probable* was selected for 9 out of 18 (or 50% of the) responding countries: Albania, the Czech Republic, Germany, Italy, the Netherlands, Norway, Romania, Spain and Sweden. *No, neither* was selected by 7 out of 18 (or 38% of the) responding countries: Belgium, Denmark, France, Poland, Russia, Slovenia, and Turkey. No answer provided for Hungary or Serbia.

<sup>329</sup> Question (10)(a)(iv) also asked: "If you checked No, is it a defence or mitigating circumstance that the disclosure did not harm national security?" Of the 7 responding countries, *No* was selected for 5: Belgium, Poland, Russia, Slovenia, and Turkey. *Yes* was selected for Denmark and France.

<sup>330</sup> See, e.g., response to Question (10)(a)(v) for Slovenia.

<sup>331</sup> Question (10)(c) asked: "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)? Please choose one: Yes/No." *Yes* was selected for 13 out of 19 responding countries: Albania, France, Hungary, Italy, the Netherlands, Romania, Russia, Serbia, Slovenia, Spain, Sweden and Turkey. Although there are criminal penalties for possession in Serbia, the expert for Serbia says practice has shown, so far, that one cannot be prosecuted for mere possession, only distribution. The experts for Italy and Russia also go on to discuss disclosure, not possession, in their answers. *No* was selected for the Czech Republic, Denmark, Germany, Norway, Poland, and the United Kingdom. The expert for Belgium did not answer, but noted in follow-up that, in general, there are no sanctions for persons without authorized access.

<sup>332</sup> Question (10)(c)(i) asked: "If you checked Yes [for Question (10)(c)], what is the maximum penalty for this crime?" See response for the Netherlands (6 years); Romania (3 years), Russia (20 years), Serbia (15 years), Slovenia (3 years, but if committed out of greed, 5 years, and if committed through negligence, 1

maximum penalty is three years imprisonment, but if the act was committed out of greed is five years, and if committed out of negligence is one year.<sup>333</sup> In Turkey, separate penalties are available for the act of securing the documents without authorization, in addition to the act of possession.<sup>334</sup> To the contrary, in Spain, obtaining the classified information, knowing that it was classified, and failing to return it to the empowered authority are all elements of the offense of unauthorized possession.<sup>335</sup> In several of the countries, in addition to proving the intentional possession of the information without authority, the prosecutor must also demonstrate that the unauthorized possession could harm national security.<sup>336</sup>

In half of the surveyed countries, criminal penalties are also available for the unauthorized possession of classified information by a person who had authorized access to that information.<sup>337</sup> In Sweden, the information must be of real significance to fall under this crime; accordingly, there is not a penalty for the unauthorized possession of most defense and police information.<sup>338</sup> Notably, whistleblower protections, where they exist, are not commonly available for the unauthorized possession of information, but tend instead to focus on unauthorized disclosure.<sup>339</sup> In Germany, the unauthorized

---

year), Spain (3 years); Turkey (1-5 years for possession of documents concerning state security; 1-3 years for securing prohibited information; 3-8 years for securing information relating to state security; 15-20 years for espionage).

<sup>333</sup> See response to Question (10)(c)(i) for Slovenia.

<sup>334</sup> See response to Question (10)(c)(i) for Turkey.

<sup>335</sup> See response to Question (10)(c)(ii) for Spain.

<sup>336</sup> Question (10)(c)(ii) asked: "What must the government prove in order to obtain a conviction?" See response to Question (10)(c)(ii) for Italy (The public prosecutor shall prove, as well, that the illegal possession could actually harm national security); the Netherlands (the secrecy of the information must be vital); Romania (the potential damage to a state interest and the causal relation from mere possession of that information to actually triggering the potential damage);

<sup>337</sup> Question (9)(g) asked: "Are there criminal penalties for the unauthorized possession of classified information by a person who had authorized access to that information?" *Yes* was selected for 10 out of 19 responding countries: Belgium, the Czech Republic, France, Italy, Moldova, the Netherlands, Serbia, Spain, Sweden, and Turkey. *No* was selected for 9 out of 19 responding countries: Denmark, Germany, Hungary, Norway, Poland, Romania, Russia, Slovenia, and the United Kingdom. No answer was provided by Albania.

<sup>338</sup> See response to Question (9)(g) for Sweden.

<sup>339</sup> Question (9)(g) also asked: "If yes, do whistleblower protections apply to unauthorized possession of information?" Of those that penalize possession, only Sweden and the Netherlands provide whistleblower protection, that is 2 out of 11 responding countries. However, the Yes answer provided by the Netherlands appears to refer not to national whistleblower protections, but rather to Article 10 of the European Convention on Human Rights. No was selected for Belgium, the Czech Republic, France, Hungary, Italy, Moldova, Serbia, Spain, and Turkey. Notably, only Hungary, Romania, Serbia, Slovenia, Sweden, and the United Kingdom have whistleblower protections at all. Of the countries that have whistleblower protections, only three, Serbia, Sweden and the United Kingdom, prosecute for unauthorized possession. Two of these three do not protect unauthorized possession. See responses for the United Kingdom (the Public Interest Disclosure Act is concerned with certain disclosures, not with possession, of information) and Serbia (The whistleblower law only covers disclosure of suspected corruptive activity). However, in several of the countries, a defense may be raised that the information could not be considered to be

possession of “national secrets” and the attempt to get in possession of national secrets are criminal acts, only if done with the intention to disclose the information.<sup>340</sup> In Hungary, it is not the possession, as such, that is criminalized, but the unauthorized obtaining.<sup>341</sup>

## **IX. Whistleblower Protections**

Nearly one-third (30%) of the surveyed countries have enacted “whistleblower” laws to protect persons who disclose classified information pertaining to government wrongdoing.<sup>342</sup> The categories of information covered by whistleblower protection laws varies, but most cover the disclosure of information showing criminal or illegal activity by the government.<sup>343</sup> In Romania, whistleblower laws protect the disclosure of any and all wrongdoings, breaches of legislation, professional ethics, or principles of good administration, efficiency or transparency;<sup>344</sup> however, in Serbia, reference is made only to corruption.<sup>345</sup>

All of the countries that have whistleblower laws also apply those protections to personnel in the security sector.<sup>346</sup> However, in some countries, whistleblower protections are not meaningful as applied to personnel in the security sector. In the United Kingdom, for example, while whistleblower protections provide coverage for the

---

classified if classified in order to cover up criminal activities. See response to Question (10)(c)(iii) (“What are the defenses?”) for Spain.

<sup>340</sup> See response to Question (9)(g) for Germany.

<sup>341</sup> See response to Question (9)(g) for Hungary.

<sup>342</sup> Question (9)(c) asked “Do laws protect ‘whistleblowers’ who disclose certain categories of classified information pertaining to government wrongdoing?” *Yes* was selected for 6 of the 20 surveyed countries (30%): Hungary, Romania, Serbia, Slovenia, Sweden, and the United Kingdom. *No* was selected for the other 14 countries: Albania, Belgium, Czech Republic, Denmark, France, Germany, Italy, Moldova, the Netherlands, Norway, Poland, Russia, Spain, and Turkey. Notably, however, as concerns Hungary, although there is a general whistleblower protection law, it cannot be enforced, as the authority responsible for its enforcement has never been set-up or designated. Also, notably, in the United Kingdom, the protection is entirely or materially undermined by the Official Secrets Act, such that while there is technically protection, it is not meaningful as applied to whistleblowers in the security sector, defense, and intelligence agencies.

<sup>343</sup> Question (9)(c)(i) asked: “What categories of information are covered by the whistleblower protection laws?”

<sup>344</sup> See response to Question (9)(c)(i) for Romania.

<sup>345</sup> See response to Question (9)(c)(i) for Serbia.

<sup>346</sup> See responses to Question (9)(c)(ii). *Yes* selected by 6 out of 6: Hungary, Romania, Serbia, Slovenia, Sweden, and the United Kingdom. The expert for the United Kingdom also selected *No*, because the application is not meaningful. Notably, in Hungary, some protection applies to officials of intelligence agencies, but the security and defence sectors are covered in their entirety. See also Question (9)(c)(iii), which asked: “How do the protections afforded to whistleblowers in the security sector, defense, or intelligence agencies differ from whistleblowers in other government sectors, if at all?” Note also, in Italy, there is no legal difference between personnel of the security sector and employees of other government agencies, regarding the duty to report crimes and the inability to be sanctioned for such reporting. See response to Question (9)(c) for Italy.

disclosure of information which is reasonably believed to show some form of criminal or other illegal activity, there is no statutory protection if the disclosure is itself a criminal offense; accordingly, while there is technically protection of all whistleblowers, this protection is not meaningful as applied to whistleblowers in the security sector, because the criminal provisions of the Official Secrets Act trump the whistleblower protections.<sup>347</sup> In Sweden, while there is protection for leaking “ordinary” secret information to the press, the disclosure of “qualified” secret information is a criminal offense, and no limits are imposed on the government’s investigation when the disclosure of very secret national security information is at issue.<sup>348</sup>

Notably, for half of the countries with whistleblower protections, the protections also vary depending on whether the disclosure was made publicly, internally, or to a designated independent body.<sup>349</sup> For example, in Sweden, only leaking to the press is protected;<sup>350</sup> whereas, in the United Kingdom, disclosure must be made to one’s employer or the Minister of the Crown.<sup>351</sup>

In addition, in several of the countries that do not have whistleblower protection laws, there are nevertheless circumstances in which the disclosure of classified information may be protected. Indeed, several countries, without whistleblower laws, even require disclosure where criminal wrongdoing is involved.<sup>352</sup> For example, the Italian Code of Criminal Law obliges any public official or civil servant, who by reason of his/her duty becomes aware of a crime, to report it to the prosecutor’s office. Failure to comply with this obligation is a crime as well, and the public official who, in compliance with the law, reports a crime cannot be sanctioned for having disclosed classified information.<sup>353</sup> In Germany, although there is not a whistleblower protection law, there are specific sections of laws that justify, for instance, the disclosure of information about

---

<sup>347</sup> See response to Question (9)(c)(i) for the United Kingdom (The Public Interest Disclosure Act 1998 offers limited protection for whistleblowers but its provisions are subject to the Official Secrets Act 1989).

<sup>348</sup> See response to Question (9)(c)(i) for Sweden (Notably, it has been made deliberately difficult to investigate leaks of qualified secret information, but there are not limits on the investigation of the disclosure of very secret national security information).

<sup>349</sup> Question (9)(c)(i) also asked: “Do the protected categories vary depending on whether the information is disclosed publicly, internally, or to a designated independent body? Please choose one: Yes/No.” Of the 6 countries with whistleblower laws, 3 selected *Yes* and 3 selected *No*. *Yes* was selected for Hungary, Sweden, and the United Kingdom. *No* was selected for Romania, Serbia, and Slovenia.

<sup>350</sup> See response to Question (9)(c)(i) for Sweden.

<sup>351</sup> See response to Question (9)(c)(i) for the United Kingdom.

<sup>352</sup> See responses to Question (9)(f)(i) for Belgium (statutory obligation to report to leading official and to Public Prosecutor if there is also crime), Czech Republic (in some offices are internal regulations that order or allow report on wrongdoing) and Germany (they are obliged to report crimes and have the right to remonstrate to a higher ranking officials) and responses to Question (9)(f)(ii) for Denmark (people in leading positions have a duty to report about unlawful orders to his/her superior) and Norway (in practice, a public authority would probably be held responsible for not reporting).

<sup>353</sup> See response to Question (9)(c) for Italy. See also “feedback on draft report” for Spain (one who, by reason of his/her duty, becomes aware of a crime and fails to report it may be subject to a fine).

cases of corruption in public administration.<sup>354</sup> Likewise, in Albania, the Council of Europe Civil Law Convention on Corruption provides that disclosures about corruption should not be met with sanctions.<sup>355</sup> Also notable, in Moldova, although there is no duty to report wrongdoing, the law says that no one can be punished for making public information, if release does not or cannot damage legitimate interests related to national security, or if the public interest in knowing the information outweighs the damage that can result from dissemination.<sup>356</sup>

## **XII. Media Protections**

### *a. Prior Restraints on Publication*

In the majority of the surveyed countries (65%), the government cannot prevent the media from publishing information, even on the basis of national security.<sup>357</sup> Of those that can, most require involvement of the courts.<sup>358</sup> However, several countries effectively operate a system of prior restraints by contacting the media directly.<sup>359</sup>

Once information has entered the public domain, approximately half of the surveyed countries provide that the government may not prevent or sanction the further dissemination of that information, even by public personnel.<sup>360</sup> However, in a few

---

<sup>354</sup> See response to Question (9)(c) for Germany (citing section 38 para 2 of the amended Public Servants Status Act, *Beamtenstatusgesetz*; and similarly the *Dienstrechtsneuordnungsgesetz 2008*)

<sup>355</sup> In Albania, the Council of Europe Civil Law Convention on Corruption, which was ratified by Albania in 2000 and entered into force in November 2003, recognizes that employees who disclose information about corruption should not be subject to sanctions, but such approach is not provided in the legal framework at all levels (constitutional, statutory, regulations, etc.). See also “additional comments” for Albania. In Albania, the current law on classified information does not recognize the possibility that information might be released for the sake of public interest, even if properly classified. Accordingly, the law lacks a number of important safeguards, such as protection for “whistleblowers.”

<sup>356</sup> See response to Question (9)(f)(i) for Moldova.

<sup>357</sup> Question (10)(e) asked: “May the government prevent the media from publishing information on the basis of national security? Please choose one: Yes/No.” *Yes* was selected for 7 of the 20 surveyed countries (35%): Denmark, Italy, the Netherlands, Russia, Serbia, Slovenia, and the United Kingdom. *No* was selected for 13 of the 20 surveyed countries (65%): Albania, Belgium, the Czech Republic, France, Germany, Hungary, Moldova, Norway, Poland, Romania, Spain, Sweden, and Turkey. But see response to Question (10)(f) for Turkey (It is possible that a blocking order to deny access to a website, such as WikiLeaks, may be issued by a Court. Currently, access to thousands of websites are blocked from Turkey.)

<sup>358</sup> Question (10)(e)(i) asked: “What information must the government provide to justify a prior restraint on publication?” and Question (10)(e)(ii) asked: “To whom must this information be provided?” See responses for Denmark (the courts); the Netherlands (the court); Serbia (district court); Slovenia (the court).

<sup>359</sup> See responses to Question (10)(e)(ii) for Italy (publisher, editor and journalist) and Russia (editor-in-chief), and response to Question (10)(e)(i) for the United Kingdom (“DA Notices” are provided to the media). As explained by the expert for the United Kingdom, “Just because it’s not legally entrenched does not mean that it’s not mightily effective! The DA Notice system is an extremely effective means whereby the media operates a series of prior restraints.”

<sup>360</sup> Question (10)(f) asked: “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

countries, even after publication, the media may be prevented from further dissemination information. In Turkey, blocking orders have been issued to deny access to thousands of websites on this basis.<sup>361</sup> In Slovenia, in the context of a criminal procedure, the government may require destruction of the offending publication (*e.g.*, newspapers, if the information was published in them), but when it comes to publishing on the Internet, the government may only ask the ISP to withdraw the content, citing the illegality of publication.<sup>362</sup> Still, in the majority of the surveyed countries, it is not possible to prevent publication by the media.

### *b. Media Privileges*

In most (60%) of the surveyed countries, the government cannot compel the media to disclose confidential sources.<sup>363</sup> Notably, although such disclosure could be compelled in Sweden, this has not happened in the last thirty years.<sup>364</sup> Also, notable, in Belgium, compelled disclosure of confidential sources is only possible if the information is crucial to prevent a crime of great danger for the integrity of persons and cannot be obtained otherwise.<sup>365</sup> In Poland, journalists may refuse to testify on account of their professional secrecy requirements, unless the court orders an exemption, a decision which the journalist can appeal. The exemption is possible only when the court determines that a journalist's testimony is indispensable for the proper functioning of the justice system and in the circumstances of the case, when the information cannot be determined otherwise. Moreover, as concerns the protection of anonymous sources or authors, the judge cannot order an exemption, except where the information sought relates to certain enumerated offenses: *inter alia*, terrorism, assassination, genocide, and

---

website)? Please choose one: Yes/No." *Yes* was selected for 9 out of 18 responding countries: Belgium, Denmark, Italy, Moldova, Russia, Slovenia, Spain, Sweden, and Turkey. *No* was selected for 9 out of 18 responding countries: Albania, the Czech Republic, France, Germany, the Netherlands, Norway, Poland, Romania, and Serbia. Notably, the experts for Hungary and the United Kingdom checked both Yes and No. The expert for the United Kingdom notes that the government may *seek* to prevent or sanction dissemination, but the court is unlikely to grant such an order. Compare with response for Poland, for example (Neither repeating nor passing secret information to others qualifies as disclosing a state secret if the information has already been disclosed, especially in the media or is commonly known or anyone can easily learn about it).

<sup>361</sup> See response to Question (10)(f) for Turkey; *see also* response for Hungary (law enforcement authorities may investigate and prosecute the disclosure and interrupt the criminal offense (the disclosure)).

<sup>362</sup> See response to Question (10)(f) for Slovenia; *see also* response for Moldova (dissemination may be quelled by so-called "prophylactic" talks, by explaining that dissemination of some information may prejudice public or state interests, asking a person not to do this or to renounce).

<sup>363</sup> Question (10)(d) asked "May the government compel a member of the media to reveal a confidential source in the interests of national security? Please choose one: Yes/No." *Yes* was selected for 8 of the 20 surveyed countries: Belgium, Denmark, Germany, Moldova, Serbia, Slovenia, Sweden, and the United Kingdom. *No* was selected for the remaining 12 countries: Albania, the Czech Republic, France, Hungary, Italy, the Netherlands, Norway, Poland, Romania, Russia, Spain and Turkey. Notably, the expert for Russia notes that only the court may compel a member of the media to reveal a confidential source.

<sup>364</sup> See response to Question (10)(d) for Sweden.

<sup>365</sup> See response to Question (10)(d) for Belgium.

threats to public safety.<sup>366</sup> Nonetheless, in Poland, a journalist's refusal to disclose information protected by professional secrecy does not prevent him or her from liability for an offence committed by publishing classified information. Journalists who disclose classified information may be at risk of criminal liability for the offense of unauthorized disclosure.<sup>367</sup>

*c. Prosecution of the Media*

Half of the surveyed countries (50%) have criminally charged members of the media for the disclosure of classified information in the last two decades.<sup>368</sup> However, such prosecutions have occurred no more than once or twice in each of these countries.<sup>369</sup> Moreover, none of these prosecutions have resulted in conviction.<sup>370</sup> Indeed, the only punishment reported to have been meted out was in Serbia, where a book containing the information at issue was confiscated.<sup>371</sup> Nonetheless, most of those countries that have not criminally charged any members of the media for publishing government secrets within the past two decades have still investigated or otherwise threatened members of the media with government sanction.<sup>372</sup> In some of the surveyed countries, such as the Netherlands, the Criminal Code makes no distinction between a disloyal employee that sells documents for a profit and a journalist who publishes a leaked document, revealing corruption in the military.<sup>373</sup> In Germany, the crime of "aiding & abetting" unauthorized disclosure as applied to journalists was recently removed from the criminal code; however, it is still a crime to instigate a violation of official secrets for journalistic purposes.<sup>374</sup>

---

<sup>366</sup> See "additional comments" for Poland.

<sup>367</sup> See "additional comments" for Poland (However, there are presently efforts to amend Polish law to protect journalists from criminal liability for disclosing such information, *inter alia*, in order to protect a socially justified interest.)

<sup>368</sup> Question (10)(b) asked: "Have any members of the media (journalists, editors, publishers, etc.) been charged with a crime for publishing government secrets in the past two decades? Please choose one: Yes/No." 10 out of 10 selected *Yes*: Albania, Denmark, France, Germany, Hungary, Italy, Poland, Russia, Serbia, and Slovenia.

<sup>369</sup> Question (10)(b)(i) "Approximately how many times have charges been brought?"

<sup>370</sup> Question (10)(b)(ii) "Approximately how many convictions have there been, and what punishments were imposed, if any?"

<sup>371</sup> See response to Question (10)(b)(ii) for Serbia.

<sup>372</sup> Question (10)(b) "If you checked No, have any members of the media been investigated or otherwise threatened with government sanction as a result of publishing government secrets in the past two decades? Please choose one: Yes/No." 6 out of 10 responded *Yes*. *Yes* was selected for the Czech Republic, Moldova, the Netherlands, Romania, and the United Kingdom. The expert for Belgium also noted yes, that members of the media have been investigated. *No* was selected for Norway, Spain and Sweden. No answer was provided for Turkey.

<sup>373</sup> See "additional comments" for the Netherlands.

<sup>374</sup> See response to Question (10)(a) for Germany. Note, also, in Germany that a search of an editor's office aimed at identifying the source of a leaked classified document was declared illegal by the Federal Constitutional Court.

## X. Record Maintenance

### a. *The Duty to Archive and the Duty to Destroy*

Nearly all (95%) of the surveyed countries recognize a duty to archive.<sup>375</sup> Of those, 100% also apply that duty to the security sector.<sup>376</sup> However, when classified information may be destroyed varies.<sup>377</sup> The majority of the surveyed countries allow information to be destroyed before being declassified.<sup>378</sup> To the contrary, in Serbia, the destruction of classified information is defined as “damage.”<sup>379</sup> Only the Czech Republic, Moldova, Poland, Romania, and Serbia report that information may not be destroyed before being declassified.<sup>380</sup> In other countries, such as Denmark, security and intelligence services are compelled to destroy classified information when the security reasons for maintaining the information cease to exist.<sup>381</sup> In several countries, however, information may only be destroyed when it is not subject to archival requirements.<sup>382</sup>

In the majority of the surveyed countries, the law does not provide specific categories of information (such as information pertaining to human rights violations or

---

<sup>375</sup> Question (11)(a) asked “Is there a duty to archive classified documents. Please choose one: Yes/No.” Nineteen of the twenty countries have a duty to archive. Only Turkey answered *No*. The expert for Germany did not provide an answer, but notes that federal authorities have to offer all documents not needed anymore to the federal archive if of lasting value for research and understanding of German history. *See* response to Question (11)(b) for Germany.

<sup>376</sup> Question (11)(a) also asked: “If you checked “Yes,” does the duty to archive classified documents apply to the security sector, defence, and intelligence agencies? Please choose one: Yes/No.” *Yes* was selected by all 18 of the responding countries. No answer was provided for Germany. *See*, however, follow-up explanation provided by the additional expert consulted for Germany (Any public authority is obliged to keep documentations according to the specific regulations of each sector).

<sup>377</sup> Question (11)(b) asked “Under what circumstances is classified information permitted to be destroyed?”

<sup>378</sup> Question (11)(b)(i) asked “May classified information ever be destroyed before becoming declassified?” *Yes* was selected for 13 of the surveyed countries: Albania, Belgium, Denmark, France, Germany, the Netherlands, Norway, Russia, Slovenia, Spain, and Sweden. Also in response to (11)(b), the expert for Italy states that “Classified information can be destroyed before being declassified.” *No* was selected for 5 of the surveyed countries: the Czech Republic, Moldova, Poland, Romania, and Serbia. No answer was provided for Turkey or the United Kingdom.

<sup>379</sup> *See* response to Question (11)(b) for Serbia.

<sup>380</sup> *See* responses to Question (11)(b) for the Czech Republic, Moldova, Poland, Romania, and Serbia.

<sup>381</sup> *See* responses to Question (11)(b) for Denmark (in general, the files and documents in the intelligence services have to be destroyed whenever they are no longer relevant for those services) and Italy (classified information can be destroyed before being declassified, and, in general, it is destroyed when considered useless for the purposes that led to its classification). Compare response to Question (11)(b) for Russia (A duty to archive document is provided in the law. . . But there are not specific legislative provisions defining any responsibility for destroying information).

<sup>382</sup> *See* response to Question (11)(b) for Germany (“If the Federal Archive does not archive the documents, the classified information has to be destroyed”) and Poland (a document this is not intended for further use, unless it constitutes archive materials, may be destroyed); *see also* response to Question (11)(b)(ii) for Belgium and response to Question (11)(b)(iii) for the Czech Republic.

government corruption) that are not permitted to be destroyed.<sup>383</sup> However, in Albania, the destruction of information related to physical or legal persons and private or public entities is not permitted.<sup>384</sup> Likewise, in Spain, it is not permissible to destroy documents that have evidential value related to right or obligations of public persons or entities.<sup>385</sup> Although specific categories of information are not mentioned in Swedish law, it is nonetheless required, according to the archives act, that sufficient material must be retained for the purposes of the public's right of access to official documents, the needs of administration and the courts, and for purposes of research.<sup>386</sup>

### *b. Oversight of Document Destruction*

The degree of oversight involved in the decision to destroy classified information varies from country to country.<sup>387</sup> Many of the countries have no oversight of the decision to destroy classified information, or provide only internal oversight measures.<sup>388</sup> Notably, in Italy, the regulation concerning the destruction of information by the security services is itself classified and, therefore, information on these practices is not readily available; however, according to a senior officer of the Prime Minister's office, the decision to destroy classified information is made by a special commission, internal to the security services, according to guidelines provided by the government.<sup>389</sup> In several of the surveyed countries, oversight is provided by the archival department.<sup>390</sup> In Belgium, for example, authorization must be received from the General Archivist for the destruction of documents, and such authorization will only be given if the information

---

<sup>383</sup> Question (11)(b)(iii) asked: "Are there certain categories of information that are not permitted to be destroyed (e.g., information pertaining to human rights violations or corruption)? Please choose one: Yes/No." *No* was selected for Belgium, the Czech Republic, France, Germany, Moldova, the Netherlands, Norway, Romania, Russia, Slovenia, and Sweden. As noted for Romania, however, limitations based on human rights may be applicable by precedence of international treaties, such as the 1997 NATO Agreement on security of information, or the 2005 EU-Romania Agreement on security procedures concerning the exchange of classified information.

<sup>384</sup> See response to Question (11)(b)(iii) for Albania.

<sup>385</sup> See response to Question (11)(b)(iii) for Spain (The problem, however, is that there are not mechanisms of oversight to ensure that this is so).

<sup>386</sup> See response to Question (11)(b) for Sweden; see also response to Question (11)(b) for Norway (classified information is not permitted to be destroyed if the document is either subject to case handling or of value as documentation).

<sup>387</sup> Question (11)(b)(ii) asked "What oversight is involved in the decision to destroy classified information?"

<sup>388</sup> See responses to Question (11)(b)(ii) for Denmark (no special oversight); Germany (no specific oversight, although it must be documented which documents are destroyed, by whom and when, and witnessed internally); Norway (none); Romania (none); Russia (only internal oversight); and Turkey (none).

<sup>389</sup> See response to Question (11)(b) for Italy.

<sup>390</sup> See responses to Question (11)(b) for Belgium (authorization has to be asked of the General Archivist), the Czech Republic (proceeded under the Archive Act), Germany (have to offer all documents not needed anymore to the Federal Archive), the Netherlands (supervised by the General Archives Inspector and his staff), and the United Kingdom (under the direction of the Keeper of Public Records).

has no scientific or historical value.<sup>391</sup> In Germany, the decision of whether a document is of “lasting value” is a co-decision made by the Federal Archivist and the relevant federal authority.<sup>392</sup> In the Netherlands, a list of such documents is created by the relevant authority, approved jointly by the minister of culture and subject-matter minister, published in the national gazette, and subject to challenge by interested parties; although in extraordinary circumstances, the Prime Minister can allow deviation.<sup>393</sup>

In several countries, the oversight provided is not for the decision to destroy, but rather for the destruction process, *i.e.*, to ensure that the documents are completely destroyed.<sup>394</sup> In some countries, while there is no oversight, as such, there is a requirement that a record of the destruction be made.<sup>395</sup> In Germany, for instance, it has to be documented which documents have been destroyed, when, and by whom the decision was taken, and this information must be accompanied by a witness signature.<sup>396</sup>

### *c. Maintenance of Classified Document Lists*

In the majority of the surveyed countries, each public authority that classifies information must maintain a list of classified documents that it holds.<sup>397</sup> These lists commonly contain document reference numbers, dates, and classification levels.<sup>398</sup> Some also include description of the document,<sup>399</sup> the identity of recipients of the document,<sup>400</sup>

---

<sup>391</sup> See response to Question (11)(b)(ii) for Belgium.

<sup>392</sup> See response to Question (11)(b) for Germany.

<sup>393</sup> See response to Question (11)(b) for the Netherlands

<sup>394</sup> See response to Question (11)(b)(ii) for Poland (a document must be destroyed in a way preventing entire or partial reconstruction of its content); Albania (each ministry and state institution has a Commission of Destructions, and the National Security Authority oversees the procedures of destruction); Spain (there are control organs that supervise the destruction of the information depending on the degree of the classification of the information).

<sup>395</sup> See responses to Question (11)(b)(ii) for Poland (destruction must be placed on record in the files) and Spain (the control organs under which the destruction is done must fill in a file with data about the destruction and the fact of the destruction will be recorded in the registry).

<sup>396</sup> See response to Question (11)(b)(ii) for Germany.

<sup>397</sup> Question (11)(c) asked: “Is each public authority that classifies information required to maintain a list of classified documents that it holds? Please choose one: Yes/No.” *Yes* was selected for 13 of the surveyed countries: Albania, the Czech Republic, France, Germany, Hungary, Italy, Moldova, Norway, Poland, Romania, Serbia, Slovenia, Spain and Sweden. Notably, although the expert for Romania selected *Yes*, in Romania, such a list may only be deduced by confronting the documents required for proactive disclosure. In Germany, the requirement is governed by internal administrative regulations particular to each sector. *No* was selected for 5 of the surveyed countries: Belgium, Denmark, the Netherlands, Russia, and Turkey. No answer was provided for the United Kingdom.

<sup>398</sup> Question (11)(c)(i) asked: “What information must be included in this list?” See, *e.g.*, responses to Question (11)(c)(i) for Italy, Norway, and Spain. See also follow-up from Nils Leopold for Germany (this lists contain dates, level of classification, size, and responsible officer carrying out the classification).

<sup>399</sup> See, *e.g.*, response to Question (11)(c)(i) for Sweden (in principle, the titles of all documents must be registered).

<sup>400</sup> See responses to Question (11)(c)(i) for France (identity of the recipient), Poland (evidence of the persons having access to classified documents), and the Czech Republic (recipient’s name).

and other identifying data.<sup>401</sup> Such lists are not generally available to the public.<sup>402</sup> In Sweden, 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 agencies, the register itself can be kept secret from the public.<sup>403</sup> In Italy, the only information from this list made available to the public is the classification level.<sup>404</sup> In Hungary, although in theory information in the list that is not itself classified should be made public, in practice, no information on the list is made publicly available.<sup>405</sup>

---

<sup>401</sup> See response for the Czech Republic (number of pages, number of attachments, year document is to be discarded, and other information) and Poland (characteristics of the classified document, registry of correspondence, and other information).

<sup>402</sup> Question (11)(c)(ii) asked: “What information from this list, if any, must be made available to the public?” See responses for Albania (none); France (none); Norway (none), Romania (none); Spain (none); the Czech Republic (it is not expressly provided, but exceptions to disclosure for classified information would apply), Moldova (these lists cannot be published); Poland (not regulated); Serbia (missing secondary legislation, so hard to tell), Italy (only the classification level), and Hungary (in practice nothing).

<sup>403</sup> See response to Question (11)(c)(ii) for Sweden.

<sup>404</sup> See response to Question (11)(c)(ii) for Italy.

<sup>405</sup> See response to Question (11)(c)(ii) for Hungary.