Chapter 5

Behind the Scenes of the EU Practices on Secrecy
**INTRODUCTION**

On basis of what criteria are you going to say that I over-classify? [Classification of documents] is no exact science and that means before a court it would be an interpretation and you would lose. You will lose your case as a disciplinary authority or even as a criminal authority.¹

This candid statement by a high EU official points to a key issue regarding the classification of documents: it is based on discretion. The initial decision to classify a document commences a complex administrative procedure as a result of which information is publically inaccessible, sometimes for more than 30 years. Access to classified information is also restricted internally within the EU administration and among institutions, leading to a group of ‘inside-insiders’, i.e. those officials who have access to European Union Classified Information (hereinafter: EUCI).

This chapter examines the practices of classifying information in the European Union. It seeks to expose the institutional workings behind the scenes in the EU administration and to assess whether and to what extent they match the EU actors’ obligation to conduct their work ‘as openly as possible’.² Towards that end, the chapter enquires firstly into how the discretion to classify is used in the EU and whether internal administrative review mechanisms exist to address possible unwarranted secrecy claims, either *ex durante* or *ex post*. Secondly, it provides an account of the central principles of EUCI that determine internal access to classified information and questions the role of the national rules and authorities in this regard. Thirdly, the chapter examines the practical implications for oversight as well as the differences and similarities in the application of the EUCI rules.

---

1 Respondent No. 15.
2 Art 15 TFEU.
5.1 The Discretion to Create Secrets

Some people simply want to show that they are important. They use the classification system to stamp documents in order to give importance to their work.³

The discretion to classify documents empowers the official to selectively hide or disclose information favourable to her self-interest. Besides enhancing one’s career position, this discretion may be used at an institutional level to conceal incriminating information or information that is deemed unfavourable to be publically disclosed. Max Weber alluded to this aspect of secrecy pointing out that it enables bureaucracies to increase their influence.⁴ Research further shows that the discretion to classify information could be used to cover errors and inefficiency.⁵

Discretion, as understood and applied in this research, implies that an official cannot strictly apply standards set in advance and uses personal judgment.⁶ This definition of discretion is identified as a ‘classical discretion’ in the literature.⁷ More specifically regarding EUCI, an official decides what security grading will be applied to a document and for how long. The drafter of classified documents has a certain view and expertise on the subject matter and she is also guided by experience.⁸ These elements are combined with a table of examples and a variety of guidelines or manuals.⁹ Yet, as the EU officials point out, classifying documents ‘is not black and white’ and the ‘ability to assume personal responsibility plays a huge role’ when it comes to

---

³ Respondent No. 10.
⁸ Mention should be made to the concept of ‘born classified’. This concept assumes that newly discovered information might be so significant with respect to security that it requires immediate and absolute control. A unique example of this concept is to be found in the US Atomic Energy Act of 1945, where there is an assumption that the newly discovered atomic-energy information is important for security reasons and that it requires instant and utter control. See Richard G. Hewlett, ‘Born Classified in the AEC - A Historian’s View’ (1981) 37 Bulletin of the Atomic Scientists 20; and Harold P. Green, ‘Born Classified in the AEC - A Legal Perspective’ (1981) 37 Bulletin of the Atomic Scientists 28.
⁹ The more specific manuals for EUCI are classified and inaccessible. Some older versions of documents, with blacked out passages, have been released.
making a decision. In this respect, classifying documents is assumed to be ‘an art based on experience’.

Although some level of discretion is inevitable because the system of classifying documents requires officials to assess information that merit protection, this does not imply that the discretion is open-ended. Primary law provides a clear legal obligation for all institutions, agencies, and bodies to conduct their work openly. Indeed, there is also a legal obligation arising from Regulation 1049/01 to balance the EU’s necessity for some level of secrecy with the constitutional commitment and public interest in openness. Hence, in the EU’s institutional setting, the discretion for classifying should be guided (or restricted) by the legal obligations in favour of openness. The presumption in favour of openness in the institutional workings regarding EUCI should be reflected in all stages of the classification process starting with the decision to classify a document. Whether a document should be classified at all, who has the authority to make this decision and what considerations justify keeping information undisclosed are all aspects of EUCI that should be examined and balanced, not merely with respect to security concerns but also with respect to the concerns of how and to what extent openness is limited. Besides taking into account openness during the process of classifying documents, the presumption in favour of openness is also related to the oversight of decisions regarding EUCI. Oversight is salient for the classification discretion, which is related to the potential for the EU institutions to conceal error or embarrassment through EUCI. The starting premise of this chapter is not that EU officials use secrecy as a means of advancing their personal interests or as an instrument for concealing maladministration. However, as developed by Chapter II in more depth, secrecy creates the potential for the abuse of power and hence justifies some level of suspicion and oversight even if we are fully convinced of officials’ good faith. Importantly, the discretion to classify documents directly impacts the level of openness and publicly available information, which is another significant reason why oversight of EUCI is justified.

This chapter seeks to identify the officials who have the power to classify information and under what considerations they do so. In addition, the chapter

10 Respondent No. 8.
11 Respondent No. 6.
12 Art 1 TEU.
14 This perspective is also based on the theoretical foundations of this thesis; the arguments here provide the concrete legal aspects. See Chapter II.
assesses whether these decisions are guided by assumptions in favour of openness. The emphasis is intentionally not on the amount of classified information, which by comparison is often the centre of discussion in the US. Many salient reasons motivate the focus of the chapter on the substantive side of EUCI decisions instead of merely looking at the EUCI numbers. Firstly, the amount of classified information, as a quantitative indicator, would fail to show the working principles and culture regarding EUCI, which in turn is crucial to comprehend how and why oversight is challenged by secrecy. Secondly, the amount of EUCI classified information is not systematic, fully accurate and public. The internal review mechanisms that focus on the amount of classified information are often missing or do not offer a systematic tracking of numbers, which would make the overall analysis of numbers more reliable. For example, the Council’s report on the number of documents classified as ‘Confidential’ produced in 2012 was found to be incorrect due to a ‘technical error’ and this was only clarified in a footnote in a different report a year later. In the case of some actors, such as Europol, the amount of classified information is itself classified information. In addition, Member States and third parties may veto the public registration of documents they have shared with the EU institutions, leading to incomplete numbers for classified information at EU level. Thirdly, and more importantly, even if the EUCI numbers were systematic, fully accurate and public, they would not reveal or indicate the broader issues at stake caused by the rules of EUCI. A high or low amount of classified information as such is secondary to the fact that the system of classified information could conceal the most relevant information from processes of accountability and public deliberation. For example, the numbers of EUCI provided by the Council are not significantly high.

16 Respondent No. 1, 3.
As the numbers above indicate, the Council for example has not reported any TOP SECRET document in the past ten years and other levels of classification remain relatively modest, although the amount of information classified as Restricted is rising significantly. However, Chapter VI will show the many problems oversight institutions face when accessing classified information on salient policy issues. The general public too remains largely uninformed, as for example regarding the EU’s negotiating mandates such as the accession to the European Convention on Human Rights or the Transatlantic Trade and Investment Partnership with the US. Therefore, instead of quantitative indicators, this section focuses on the application of the EUCI rules.

5.1.1 EU Officials with Power to Classify Documents

Every official can potentially classify documents. This is particularly the case with the executive and administrative actors in the EU. However, for institutions such as the European Parliament, the discretion to classify documents is much more limited. In accordance with Article 4 of the European Parliament’s Bureau Decision on classified

---


information, the President of the European Parliament, the chairs of the parliamentary committee, the Secretary General and ‘any person duly authorised’ by the Secretary General have discretion to ‘originate confidential information’. Authorisation for creating originally classified information must be granted in writing.

There are also officials who, while working with original classified information, generate or create new documents and materials based upon this information. The latter, in the technical expressions of the classification system, are known as ‘derivative’ classifiers. These officials do not need to possess original classification authority. They reproduce, extract or summarize classified information, and apply classification markings derived from source material.

This distinction implies that the margin of discretion is to a large extent limited for the derivative classifier, whose role is to use the classified information in strict accordance with the originator’s will. An official frankly points out that ‘you will not agree with [the decision of the originator] but you still have to put the [same classification] marking.’ This in turn, Council officials explain, may result in over-classification because ‘if the [national] Capital over-classifies, you are stuck.’ Internal EU administrative documents define over-classification as attributing a higher security level than that warranted for a given piece of information. Over-classification also means that a document is classified when it should have been made public instead.

Marking documents as classified may vary at the EU level considering that each EU actor has its own specific guidelines and concerns for security when it comes to EUCI. Differences in classification levels also arise at the national level since each Member State may have its own approaches to classified information and officials point out that some ‘some Member States do over-classify.’

Derivative classification is particularly prevalent at the EU institutions and bodies that have a more intergovernmental character because they rely mostly on Member States to receive classified information. In fact, some actors’ main purpose of work is precisely the collection of information from Member States in order to produce more comprehensive reports, which in turn are shared with national

---

20 Respondent No. 15.
21 Respondent No. 8.
24 Respondent No. 3.
authorities. Information gathering and sharing with the Member States is a significant task of many EU actors in security policy. For example, Europol as a law enforcement cooperation agency or the EU Intelligence Analysis Centre (INTCEN) functioning within the European External Actions Service, are fully reliant on the Member States and their classified information.\(^\text{25}\) Officials explain that they rarely originally classify documents and most of their documents have a direct link with national information, which in turn means that national classification marking authority is decisive for the EU level of classification.\(^\text{26}\) Discretion at EU level, defined above as the official’s use of personal judgment, is minimal in such cases, since the newly created document cannot be personally assessed for a different classification marking than the one deriving from the national authorities. The question of derivative classification is also relevant at the Council, as the personal experience of an official illustrates:

So far in my own practice, which includes 5 years, I have only classified 1 or 2 documents on my own initiative. The rest are all from the position of the derivative classifier.\(^\text{27}\)

Other differences in the authority to classify a document, especially when it concerns higher classification levels, arise in the hierarchical position of the official. A junior official for example would be under an obligation to consult her superiors in the official ranks because ‘a junior official would not [decide to classify] things ‘EU Secret’ without the agreement of a manager’.\(^\text{28}\) In practice, the decision to classify is mostly the prerogative of the Head of Unit.\(^\text{29}\)

The decision to classify is not always an individual one. A classification marking could be a result of a decision by the author of the document in consultation with the Director or the Director General. The classification level can also change, one ‘would send the document as Restricted and it comes back as [public] or Secret’.\(^\text{30}\) Hence, the classification marking could originate from a group at a particular unit or an individual decision. The group decision raises questions about locating responsibility and variations in the motives of the classifier. However, at the same time it is a manner of

---

25 Respondents No. 1, 2, 3, 4, 18, 19, 20, 21.
26 Respondents No. 1, 2, 5, 7, 11, 12, 22. See below subsection 5.2.2.
27 Respondent No. 5.
28 Respondent No. 6.
29 Respondent No. 9.
30 Respondent No. 12.
exchanging different opinions about the sensitivity of the information and possibly avoiding over-classification.

The current discussion might suggest that classification marking is a precise process and that it takes time and priority to apply the appropriate EUCI marking. But do EU officials actually invest serious thought and time into classifying documents? What considerations do they take into account?

5.1.2 Justifying Secrecy: Reasons for Classifying Documents

The process of classifying a document implies deciding about the security grading and duration for keeping a document undisclosed. The security or classification grading indicates the relative importance of classified information for the protection of particular interests and determines the specific security requirements for its management in the administration. Determining the duration of classification, which may be defined in terms of a future date or a future event, is also very important as it directly affects the public accessibility of the document.

Setting a specific duration for the applicability of secrecy at the time of classifying a document is not an obligation for the EU institutions. In principle, the default duration of security marking is five years and some rules, as in the case of Europol, foresee a maximum of 30 years and longer if necessary, whereas institutions like the European Parliament foresee a review for possible declassification and archiving after 25 years.31

The working culture of a specific EU institution or body is relevant in whether discussions and meetings are documented at all and if so to what extent these documents are perceived to be security sensitive. For example, Europol information is undisclosed unless it is specifically designated as public. Due to law enforcement cooperation, the working premise of the agency is ‘information is secret, unless’ as opposed to ‘information is public, unless’. The EU’s High Representative and its diplomatic helping hand, the European External Action Service, are another example on how the nature of a body affects the practice of secrecy. The practice so far has shown an inclination for more informal meetings and informal communications, which do

not lead to formal documents and hence classification _per se_ is also redundant.\(^{32}\) The European Council also shares such tendency of informality in its meetings when crucial policies are discussed.\(^{33}\)

The broader working culture is also reflected in the considerations for classifying documents. As Chapter IV explained, in the EU there are three security categories foreseen in the only legislative act applicable to EUCI. Article 9 of Regulation 1049/01 provides that sensitive information may be _Confidential, Secret_ and _Top Secret_. However, the internal rules of the EU executive institutions and bodies foresee _Restricted_ as an additional category. This chapter aims to uncover the application of these categories and the assessments the officials make in practice. For example, officials at the Council have a high sense of security of information, as a senior EU official explains:

"If you're dealing with operational information related to a military crisis management situation that the EU is running somewhere in Africa or whatever, some of that information could be very sensitive. _You could be affecting the lives of the people on the ground._ You have to be aware of that. If that information falls in the wrong hands that could have a lot of consequences."\(^{34}\)

The Commission officials acknowledge that the sensitivity of the issues might keep the information undisclosed but would not lead to a classification decision and protection within the meaning of EUCI, as the following statement illustrates:

"You can imagine that when the Commission is preparing its decision on Microsoft, if we going to fine them at all, how much are we going to fine them, this is Top Secret information. I would say Top Secret in the normal common sense. But do we classify it? Perhaps we don't because we are working in a different environment."\(^{35}\)

However, this does not mean that the Commission makes the information publicly available. Although the system of classification under EUCI and the security procedures that are foreseen therein might not be used, other markings and internal

\(^{32}\) For example, see former High Representative's opinion on formality, Catherine Ashton, 'Quiet diplomacy will get our voice heard' _The Times_ (17 December 2009).


\(^{34}\) Respondent No. 6.

\(^{35}\) Respondent No. 15.
rules on non-disclosure could apply. In the current framework, besides the classification markings, the Commission has 22 categories of protected information with specific distribution and handling instructions, which are not made public. These categorizations address the different Directorates in the Commission and the Units. In fact, officials admit that there is ‘internally a confusion regarding what happens and what is classification’. Confusion is not only part of the categories of marking and classification, but also relates to the legal terminology that is supposed to be guiding the decisions to classify documents.

If the legal terminology of the classification categories is not precise or only broadly stipulates the interests to be protected, it offers more leeway for classifying documents. Experts in issues of classified information point out that ‘high levels of generality may provide some needed flexibility, but it heightens the inherent subjectivity of the classification process and introduces an element of unchecked arbitrariness’. In this regard, notions such as ‘disadvantages’ or ‘inappropriate’ are too open-ended. For example, ‘inappropriate’ in practice may mean: ‘a statement of a politician or head of state that would undermine the EU position on diplomacy: embarrassing by providing a frank opinion about a person or a situation’. But it can also mean ‘application for tenders: these types of information are not necessarily sensitive from a security point of view, but it would be inappropriate for the party involved if the information is known publically’. Under the wording of ‘disadvantageous’, the security marking could refer to issues pertaining to the ‘internal cooking’ of decision-making or to a ‘mandate to negotiate’. Sometimes it is not a question of sensitivity or damage, ‘but it can create problems’ even if it is ‘background facts’. These types of interpretations of legal categories show that information in the EU may be over-classified if the wording of even the lowest marking is broadly applied.

EU officials mostly consider ‘damage’ or ‘identifiable damage’ when classifying information. One way to specifically address the damage question is by considering ‘what if a journalist publishes this?’ or ‘what happens if the document is made

36 Respondent No. 16.
37 Respondent No. 10.
40 Respondent No. 10.
41 Respondents No. 21, 22.
42 Respondent No. 12.
43 Respondent No. 12.
44 Respondents No. 2, 5, 6, 11, 20, 22, 23, 24.
For former practitioners these question were irrelevant because it ‘used to be very simple: Restricted was a normal classification for all [documents], everything’. Besides the interests of the Member States or the EU, officials could have their own personal interests in mind when labelling documents secret or not.

EU officials point out the disproportionality between usability and protection of information. For example, a document marked as Secret, will be stored only physically and not electronically; it may only be accessed and used within a designated highly secured area; the document cannot be copied and taken outside the secure area. In contrast, a document classified as Restricted is accessible in electronic form and is generally made more easy to use. In practice, this leads the officials to favour lower marking levels, while making sure that the security of the information is ensured. Omitting information from a document that would render the classification higher is one manner to create documents classified as Restricted.

A key issue with the classification markings, as noted above, is that the legal terminology is often described as ‘very vague’. On the one hand, it is broad in order to encompass a variety of issues, on the other hand, this makes the categories open-ended and possibly inclusive of issues that should not be classified at all. Hence, the key aspect of the classification markings and EUCI process is whether there are clear legal stipulations that require EU officials to balance the interests of openness with their classification decision. In the following subsection, we examine the aspect of openness in the application of EUCI rules.

5.1.3 Is Openness Missing in the EUCI Practices?

What is confidential? Imagine a document stamped “Confidential”, a large document, about 30 pages. All pages are stamped confidential. But the question is: within these 30 pages, what is actually confidential? Names? Locations? Actions? Very little information is confidential actually. 

45 Respondents No. 21, 22.
46 Respondent No. 12, emphasis added.
47 Respondents No. 4, 10.
49 Respondents No. 4, 22.
51 Respondent No. 4.
Nevertheless, the entire document is classified and hence these 30 pages, as the EU official explains, will be inaccessible to the public, possibly to the oversight actors and even to the officials who do not fulfil the internal access to EUCI requirements. Providing security for the relevant information is important but concurrently it has tremendous consequences for the public accessibility of the document. Classification has an impact, as do the processes of oversight and administrative management. It can hence be viewed as a cost both from an openness perspective and in terms of usability of the information for the effectiveness of decision-making.

During the process of classifying documents as well as the broader management of the EUCI, many administrative mechanisms may be established to ensure that openness is taken into account. This subsection aims to point out more specifically how the presumption in favour could be taken into account within the EUCI process and questions whether that is already the case in the current practices. Firstly, considerations of openness in EUCI could be part of the briefing process that every EU official receives at the start of his/her employment contract. The briefing as it is currently structured in the EU is only focused on security measures and there is no mention of openness or public access to information. This briefing is utilized to make officials aware of the security risks and protection measures but it does not expand to discuss the implications of classified information, especially from an openness perspective. Some practitioners are very direct that:

There is no link to openness. We do not really look at that side. Our job is the security of the document. [Official’s] job is to classify… No need to know about access and transparency. [Officials] have to start thinking like ‘what if the document is going to be in the newspaper’. This is the logic we want them to have, to be prudent.52

A second possibility of implementing the presumption of openness within the classification process would be to include a written justification for the decision to classify a specific document. This could be an incentive to rethink the specific harm and it would facilitate the process of declassification or disclosure.53 For example, if a request for public access to information that concerns a classified document is received, the justification regarding the harm disclosure would cause is already stated in the document. This written

52 Respondent No. 22.
justification would enable an EU official to immediately assess whether the reasons for classification of the document are still applicable, i.e. whether the disclosure of the document would specifically and actually harm EU interests, or whether the document should be disclosed. However, this aspect is also lacking in EU practice. In fact, as we noted above, EU officials confess that sometimes security grading is used not to give protection to the documents but more to provide a personal enhancement of interest in what they call ‘stamps-of-importance’. The issue with this aspect of classifying documents is that there is neither an *ex post* mechanism of review of the classification decision nor a system that would try to allocate “wrong” classification decisions or track responsibility. Quite the contrary, practitioners insist that such a system of review of classification decisions is not feasible precisely because the ‘classification decision is always subjective’.

Thirdly, the registration of classified documents and public records are other specific means to apply the aspect of openness within the classification procedure. Keeping track of classified information is relevant for the usability of the information but even more so for possible declassification purposes. As we noted in Chapter IV, the Solana Decision established that there would be no reference to classified information in the public register of documents of the Council. Consequently, the level of visibility of EUCI was further hindered by making them invisible, not merely in substance (the text of the document) but also in form (the procedural number of the document). EUCI is registered by each institution or body. The EU practices in this regard are not unified. For example, Europol’s Register is classified as Restricted, with access only to confidentiality desk officers. Heads of Unit have access to their ‘own part of the Register’ but no official has an overall view other than confidentiality desk officials. In this respect, the Register is centralized. At the Commission, there is a centralized register, at the level of Secretary General, but there are also local registries. Not every Directorate General has a local register since some do not have much classified information in the first place, such as in areas of education and culture. Hence, the practice is not unified even within the administrative structure of one institution, but it is established based on necessity and the number of classified documents. For the EEAS, the register is classified as Restricted as well. However, this registry does not ‘keep figures

54 Respondent No. 6.
55 Goitein (n 23).
57 Respondent No. 1.
systematically’ and it lacks an overview of the amount of classified information or possibly declassified information. The Council is similar to the Commission in the sense that there is a central and a sub-registry. For both institutions, the organisation of the register takes place on basis of the institutions’ size and functions. Among practitioners there is consensus that ‘the register is in a significant position of possible power; it controls access in and out’. However, the registry is not set up for the purpose of maintaining an overall track of classified information, to facilitate the declassification, to report on numbers of documents or to in any way facilitate a review of the security basis or the transparency of the figures. For example, for classified documents there is no strict legal obligation for the Council to identify the originator, which would facilitate tracking who was responsible for the classification and noting whether the document was originally classified by officials within the Council. The latter would be relevant in cases when access is requested from third parties, such as the Court of Justice of the EU. Moreover, the officials in these settings do not have access to the overall register or to an overview of numbers. This also eliminates the possibility of Reports or Reviews, whereby no body in the EU is required to facilitate consistent annual reviews and measures to prevent over-classification. Some actors consider that it is not necessary to follow-up on declassification and numbers of documents. A Review of the technical and security issues of the systems takes place, but there is no review driven by the idea of internal oversight of the EUCI system. Besides security focused internal reviews, an inter-administrative review between EU actors also exists to check the applicable security measures and whether the actors share similar technical facilities for safeguarding EUCI. These reviews are not focused on oversight, however, which would facilitate openness or question the balance an actor makes between openness and the classification of documents.

Overall, the internal organisational setting for classified information in the EU is focused on the security of information, but it lacks mechanisms to address challenges that could arise. One notable example is classification for personal gains or systematic misconceptions by officials. Administrative instruments, such as the registry, which could be used for preventing over-classification, are established mostly (if not only) on the basis of security concerns, although these instruments have the potential to be utilised beyond such goals.

58 Respondents No. 21, 22.
59 Respondent No. 4.
61 Respondent No. 3.
5.2 Restrictions on Internal Access to EUCI

Restriction of access to classified information is the key consequence of the EUCI system. This limitation has drawn the attention of citizens and oversight institutions in the EU and will be fully discussed in the following chapters. However, access to classified information is also limited internally within the executive actors and has pertinent consequences.

Internal limits of access to classified information impact the decision-making process, both in terms of efficiency and creating a cluster of inside-insiders, i.e. only a limited number of officials know the classified information. In addition, it leads to information asymmetries and compartmentalization.\(^\text{62}\) It is the insiders, those who know the secret information, that are in a position to determine which other officials may gain access to classified information and when such access may be granted.\(^\text{63}\) The issue of compartmentalization becomes even more pressing to examine if we follow the reasoning that agencies and institutions are involved in an incessant competition.\(^\text{64}\) Indeed, as we noted, the EU is more generally characterized by the contest of powers between institutions, and we saw such instances specifically regarding the EUCI with respect to its establishment and regulation discussed in Chapter IV. The following section provides the broader institutional setting before focusing on the central EUCI principles that limit access internally. The Member States’ involvement is also significant. This involvement can be seen in the application of national rules for issues that relate to EUCI as well as to the institutional structures. This section aims to identify when national rules apply and point out instances of the EU’s dependence on the Member States.

5.2.1 Institutional Structure and Organisation

The organisation of access to classified information depends on specific technical rules aimed at the security and protection of EUCI. The specific institutional structure and organisation is also relevant in this regard. The internal organisation of


\(^{63}\) Such asymmetries are not strictly limited to executive actors, see Vijay Krishna and John Morgan, ‘Asymmetric Information and Legislative Rules: Some Amendments’ (2001) 95 American Political Science Review 435.

\(^{64}\) David C. Kozak and James M. Keagle, Bureaucratic Politics and National Security: Theory and Practice (Lynne Rienner Publishers 1988) 7, discussing the new approach to the study of administration which is called bureaucratic politics paradigm, combining the view of administration and politics.
institutions varies depending on whether issues pertaining to EUCI are decided on a more central administrative level. For example, the Commission is more decentralized, unlike Europol, where most decisions regarding classification are taken in consultation with the Confidentiality Desk Office. At the Commission, many of the issues regarding classified documents are decided at the level of the Director General. The other bodies responsible for EUCI function within the security organisation of the Commission, which is structured on two levels: at the institutional level of the Commission there is a Commission Security Directorate, whereas at the level of the Commission departments, responsibility lies with one or more Local Security Officers. The Commission Security Policy Advisory Group and the Commission Security Board are the two other relevant bodies that are specifically related to the EUCI system. The Directorate on Human Resources and Security is the only structural body that can mark documents when they are reviewed under the security policy. Issues of physical security, mostly contracted to third (private) parties, are organised at the central level of the Commission. However, for other matters, such as registers of classified information, the organisation falls under a particular Directorate General. The Commission officials note that ‘preparing [and changing] a decision at College of Commissioners level is not easy’, therefore many of the issues are handled at the Directorate General level.

The EEAS shares features with the Commission regarding the level of complexity and the broad structures involved. The institutional structure of EEAS is divided into the Headquarters, Delegations and position of the Military Unit. As a diplomatic body related to more than 140 EU missions (civil or otherwise) in the world, the level of information flows at the EEAS is paramount. The institutional aspect of the

65 This Directorate consists of different Authorities, which are in charge of various security aspects of the information. Examples include the Security Accreditation Authority also acting as Crypto Authority.

66 Consists of the Member of the Commission responsible for security matters, representatives of the NSA of each Member State. Representatives of other European institutions may also be invited. Representatives of relevant EC and EU decentralized agencies may also be invited to attend when issues concerning them are discussed.

67 Respondent No. 15.

68 Respondent No. 15.


classification system structure encompasses many directorates that have a specific focus on security of information or their exchange. In short, the internal institutional structure of the EEAS that is important for the classification system involves: Managing Directorate, Security Directorate, Security Committee and EU INTCEN.

The Council’s institutional set-up for classified information is split between issues decided at the ministerial level and the different organs, some of which are especially created to manage the classification system. At the ministerial level, the Council only acts when it is necessary to approve security agreements with third parties, to authorize the release of EUCI to third States and international organisations, and to consent to an annual inspection programme proposed by the Secretary General concerning inspections of Member States’ and EU’s agencies services and premises. The Secretary General (SG) has the role of the Security Authority in the Council. The SG exercises a few key responsibilities in this capacity. Firstly, it is up to the SG to implement the security policy and keep it under review. Secondly, the SG coordinates with the Member States’ national security authorities on all security matters relating to the protection of classified information relevant for the Council’s activities. Throughout these tasks, the Security Office that was formally established in 2001 assists the SG with the coordination, supervision and implementation of security measures. One should not visualize the SG conducting all these different activities as such, since in practice most are performed at the level of the Security Office by the responsible officials. The legal structure merely implies that responsibility lies with the SG.

5.2.2 National Rules and the EUCI system

Member States’ rules and authorities have a significant role in the functioning of the EUCI. The extent of their involvement and relevance depends on the specific institutional setup and nature of each EU actor. In the area of security, besides the Commission, most EU actors mainly have an intergovernmental character, which implies that these actors rely on national authorities in several respects.

Firstly, national representatives participate in EU bodies that make relevant decisions for the application and development of EUCI rules at EU level. More specifically, the Security Committees consist of EU and national officials who make key decisions and provide guidelines on how documents are classified in the EU and set procedures and determine partners for the exchange of classified information. For
example, within the structure of Europol, there is the Security Committee, which is comprised of representatives from Member States and of Europol, which is in charge of setting broader policies when it comes to classified information. Besides Europol, it was noted in Chapter IV that the Council Security Committee is also a very prominent body that is involved in setting guidelines and providing opinion beyond the Council that is also applicable to EU oversight actors. The EEAS also has a Security Committee comprised of similar members to those in the Council, which in turn leads EU officials to remark at times on the duplication of efforts.⁷¹

Secondly, national authorities and rules matter for specific decisions within the EUCI system. For example, as it was already noted above, the initial decision of whether to classify a document at all often takes place at the national level since most of the information originates from the Member States and carries with it national markings. More specifically, bodies and agencies, such as INTCEN and Europol, receive the classified information from Member States and work on analyses and reports that are sent back to the Member States. National rules, in this regard, follow the document in terms of classification and declassification markings. In addition, for some EU actors, a more direct involvement of the national authorities is possible, although not through specific decisions regarding EUCI but through the institutional organisation and the tasks foreseen at the EU and national level. For example, within Europol distinctions may be drawn between actors involved at the Member State level and those that function within Europol’s structures. At the level of the Member States, it is their national regulations that apply when deciding which bodies are entrusted with handling classified information. This can vary from the State Commission on Information Security, the Ministry of Justice and Home Affairs or possibly to the Ministry of Defence.⁷²

Lastly, national rules and national authorities enable the technical and security functioning of the EUCI system, particularly as it concerns granting officials accessibility to classified information. For example, national authorities conduct the screening of officials who will be working at EU institutions and bodies to assess whether a security clearance should be granted. As it will be explained in more detail below, national rules apply to the screening process resulting in differences between the Member States as to how these procedures are carried out. A similar example, also examined more in-depth below, is the process of determining the application of

⁷¹ Respondent No. 22.
⁷² See Council Decision 2013/488/EU (n 48), Appendix C.
the principle of ‘need-to-know’, which means establishing whether an EU official will be granted access to specific classified document. Significantly, national rules apply if there is a breach of security of EUCI and if criminal charges were to be initiated against an EU official suspected of violation of EUCI security, the prosecution would take place at the national level. Overall, national rules apply to classified information that originates from Member States and as we will see in the next chapter this aspect of the classification system has direct consequences for the access of EU oversight actors to classified information. In the following subsections, the two main principles that determine internal access to classified information are examined. Their technical function is beyond the interest of this discussion; the focus rather is on how these principles provide structure to EU officials involved in the EUCI system and lead to a division of groups between inside-insiders and inside-outsiders.

5.2.3 Security Clearance

The procedure for the issuance of a security clearance is similar in all institutions and bodies of the EU. It is actually one of the few elements in the system of the EUCI that is more commonly shared. It is similar in two very important respects: at the national level, the vetting procedure takes place in accordance with applicable national regulations, which is thereafter followed by a decision regarding approval at EU level.

The question that arises then is what is the EU’s level of discretion in the process. What would be the outcome of a situation when the Member State does not approve the vetting of a prospective EU official? EU officials could not report a case in which the Member State would not approve of the person and that person would get the job.73 This does not mean that the institution in question has no discretion whatsoever to at least address the Member State in question and raise concerns that the vetting result might not be correct. However, the EU body would have no legal authority to overturn the national decision. Everyone is vetted by the Member States and EU officials admit that they are ‘bound to accept’ the national vetting decision.74

This situation of the national vetting process having final implications at EU level could lead to a strange situation for the elected Members of the European Parliament. A MEP who has a direct mandate from European citizens would be limited in her

73 Respondents No. 3, 6, 22.
74 Respondents No. 1, 6.
functions due to the vetting process for classified information. This, according to MEPs, ‘makes no sense’.75

Different issues regarding security clearance and vetting arise in the missions of the EU. For example, regarding EULEX, three different types of security clearance procedures exist: Seconded staff must have a security clearance before they arrive; Contracted staff will receive a security clearance from the Member State of which the person is a national; and then there are officials who are part of the ‘contributing third states’ and are vetted by their own states in accordance with their regulations.76 From a practical viewpoint, the two-step process of vetting at national level and approval at EU level is sensible considering that the state would have most information on the person concerned. But this does not eliminate the fact that there are different regulations and practices between Member States. For example, some Member States have more robust examinations while others have more privacy protection oriented measures. The institution in question de facto acts on the basis of the national decision. Hence, differentiation exists within each institution or body regarding how the official’s background is checked.

The security clearance is not necessarily linked to the hierarchical level of the official. A security technician can get clearance up to TOP Secret as can a Director General. In practice, most officials are not cleared for Top Secret access; their access remains valid for the level of Secret or (mostly) Confidential. The question then is how and to what extent does the security clearance structure the individuals towards classification? A security clearance is important in order to be able to be part of the administration of classification in the first place. But thereafter, it is not the prevalent factor regarding whether or not an official receives access. Hence, the security clearance determines those officials who have access at a broader level of the EUCI system, in a more abstract manner, regardless of whether in principle they would gain access to classified information. Whether indeed such official would gain access to classified information in a concrete case is determined by another key principle of the functioning of the EUCI, the need-to-know principle, which will be elaborated in the next subsection.

Some key issues derive from the discussion on security clearance. Firstly, the two-step approach is the common feature of the security clearance procedure in the EU. This means that it is always the national states that conduct the vetting process (sometimes in cooperation with other states where the official has been a resident), and only

75 Respondent No. 26.
76 For EULEX for example it is inter alia the US, Canada, Turkey; Respondents No. 23, 24.
thereafter does the EU level administration make a decision regarding the approval. However, approval should be seen in a soft sense, considering that the level of discretion (in this case, not to follow the results of the vetting procedure of the Member States) is minimal. Secondly, differences are in practice linked to the first step of the process: different national regulations apply despite the fact that all these officials upon admission become part of the EU administration that is independent of the Member States. The more complex situations are those of the EU missions where the diversity of backgrounds of officials leads to a bigger mix of vetting procedures. The concern here is that there are no mechanisms at the EU level to ensure some sense of consistency in the multiple procedures applicable both to Member States and third parties. The variety of rules results in EU officials undergoing a different scrutiny treatment, with direct consequences for the security of information. After all, practitioners are the first to admit that the human element is the weakest link in the chain of security of classified information.\footnote{Respondents No. 3, 4, 6, 15.} Beyond the security of information, another relevant consequence for the EU is that officials could face responsibility at their national level. The national authorities, however, do not have prerogatives for any oversight mechanism at the EU level. This duality creates a situation for the official that her clearance and responsibility remains at the national level for matters that are of EU level concern and her actions take place within the EU working environment.

The security clearance enables the official to possibly gain access to classified information, but as such is not definitive if, in a particular case, the official would indeed gain access. An official must have a ‘need-to-know’ in order to gain access.

\subsection*{5.2.4 The Need-To-Know Principle}

The principle of need-to-know, as the name suggests, implies that an official must have some necessity in order to be acquainted with the classified information. This principle did not always exist in the EU. For example, it was introduced to the Council in 1998.\footnote{Council Decision 98/319/EC of 27 April 1998 relating to the procedures whereby officials and employees of the General Secretariat of the Council may be allowed access to classified information held by the Council [1998] OJ L140/12, art 1(1).} The question is how broad or narrow is the application of the principle of ‘need-to-know’ and who decides or determines its scope? To answer this question, we need to recall the distinction between the originator classifier and the derivative one, and keep
in mind that the discretion of decision-making lies with the first. Hence, the originator of the classified information has the primary discretion to decide with whom the document will be shared. This could be done in several manners. For example, in Europol, a clear system exists to enable a Member State to share only with Europol, or with another Member State or many others, through a system of “handling codes”. In other cases, for instance at the Council, a third party may share the information with a certain Directorate and the latter is responsible for determining access within the unit. Another generally applicable manner to decide on the need-to-know is through the function of the official in question. For example, there would be no question that a Commission Director-General must be able to access the information.

The principle of the need-to-know is not applicable for all classified information. Namely, for the lower level of classification, Restricted documents, this principle does not apply; yet it should be pointed out that the largest amount of classified information is precisely in the Restricted category.79 What does this mean in practice? For example, everyone working in Europol, which adds up to almost 800 individuals could gain access to Restricted documents. With more than 160 officials in Brussels and an office in Luxembourg directly linked to issues of classified information,80 the Commission too has many individuals who can access documents.

The principle of the need-to-know gives an image of a system where access to classified information is determined and applied very strictly and mostly reserved for officials ‘at the top’ of the administrative hierarchical ladder. Practice does tell us that there are exceptions:

When you have a colleague with you and you are working together on a topic you show a page or a paragraph so in that case you do not give the whole file but yet they see something even though you have not checked all the need-to-know and other conditions. You could say then that access is tailor made. It needs to fit the purpose and fit the occasion.81

Hence, the usability of the information is at times more relevant in practice than strictly abiding to the security requirements for classified information. When the classified information is indeed shared on good faith and on the basis of progressing

79 See Council annual reports on access to documents.
80 Respondent No. 15.
81 Respondent No. 22.
with a particular policy, perhaps such de facto exceptions to security principles are understandable or even desirable. However, at the same time, the example shows that documents may be shared in practice, even in circumstances when they should not be. Informally sharing documents could be beneficial to a policy as well as to advance some particular interest of the official. Importantly, these situations often go unnoticed and are considered as part of the ‘everyday practice’ of classification.\(^2\)

Throughout the EU the principle of the need-to-know is designed in a similar fashion. Although each administrative actor establishes it separately, the logic of its functionality is similar. Differences might arise in practice to questions of to what extent more concrete mechanisms are established to separate the information or on the level of the rigidity with which the principle is applied.

If we could note discretion in any way, it is mostly related to the originator and the possible distinctions regarding who can view the information. In this sense, an outsider actor of the EU, such as a third state or organisation has the potential to create different circles of who gets to see what. The authority of the ‘outsider’ extends both within the institution and (crucially) between the institution and other actors. It is a similar case with the Member States when they are in the position of the originator. Yet, what we noted is that in practice this rigidity is followed by utility motives: practitioners would share information with their colleague if they consider that it is relevant for their work. In this respect, the need-to-know becomes a peer-judgment, made by fellow colleagues.

If access is not as limited, especially for the largest amount of classified information in the EU, the Restricted category, the question arises whether there is any system or mechanism to keep track of the individuals involved? Is there a way to know how many people received access to a particular document? Some sense of traceability may be noticed for higher classified information, especially for those documents that are received from third parties and for whom access is either strictly determined by the originator or the originator determines it more broadly, but then the Head of the unit decides who specifically gains access. For other categories of documents, there is no organised manner or intention to keep systematic track records. A clear overview of officials who have classified information even at lower levels of markings would benefit the EUCI system from an openness perspective, since this would make it easier to trace and consult the officials who have marked on the document whether or not a public access request for information could be positively answered. Namely, as the Court of Justice of the

\(^2\) Respondent No. 4.
European Union held in the case of Jurašinović v Council, the classification marking is merely an indicator of the sensitivity of the information and as such does not automatically exclude public access requests. In this sense, when the officials that have worked with the document must be consulted, the review and possible disclosure of the information is faster if there was already an overview of the officials involved.

Actors of the EU involved in classification display differences in the manner in which the general structure of classification is designed. Due to functionality and size, some administrations are more centralized while others work by separating issues into those that are dealt with at the institutional level and issues that concern a particular unit. In this sense, the issue of classified information is structured in accordance with broader administrative principles regarding the organisation of functions and tasks. The same could also be noticed for principles that are core to the functionality of officials regarding classified information: security clearance and the need-to-know. The regulatory framework and its rationale are shared throughout institutions and bodies of the EU. Questions regarding differences arise in their application; some bodies are more inclined to focus on the usability of information, hence share or discuss it with their colleagues even if they do not fulfil the legal conditions; other institutions, especially if more dependent on information received from third parties, would apply the principle of the originator strictly. The difference that arises hence is how bodies respond to the disproportionality between usability and security of the information.

5.3 Administrative Culture of Secrecy?

I don’t believe in full transparency. This may be a generational thing.

The principle of openness in the EU may indeed be viewed as a ‘generational thing’. The EU has evolved from an international organisation in which legitimacy was rooted at the national level, to an autonomous legal order with a comprehensive set of competences and established on principles of representative democracy at the EU level. However, the roots of a working culture of secrecy have not immediately brushed off, despite the EU’s constitutional commitments to openness. In the following final section, we examine the implications of the EUCI practices from an openness perspective and aim to identify the similarities and differences in the application of the rules.

83 Case C-576/12 P Jurašinović v Council, EU:C:2013:777.
84 Respondent No. 15.
5.3.1 Lack of Internal Oversight Perspective

The administrative regulatory approach in the EU has ignored aspects in the system of classified information that are relevant from an oversight or openness perspective. The classification system in the EU is predominantly focused on security and does not make use of the potential of the mechanisms in place for oversight concerns. Two particular examples may be mentioned derived from our elaborate discussion on the structural and organisational aspects of the classification system in the EU. Firstly, the initial decision to classify a document is not supported or guided in any manner, which would make the official with classifying authority more aware and prudent of the consequences of her decision. The obligatory briefing that every official undertakes before having the authority to classify does not include elements of how classification impacts the level of openness in the EU, most directly public access to the information. Also, we discussed in length that the decision to classify has the crucial component of discretion, which is not addressed by any classification mechanism, either \textit{a priori} or \textit{ex post}. The decision to classify raises further concerns when we turn to the legal terminology applicable for the four different levels of classification. As we noted, the interests that are supposed to be protected are stated in a broad manner and in practice they can encompass anything from negotiation mandates, to background facts, or simply the interests of the official with classifying authority. Secondly, and directly connected to these issues, administrative mechanisms such as the Register are not utilized to address these concerns or provide a broader picture of classification from openness concerns in any manner. There is no particular mechanism to oversee each decision to classify and there is no manner to keep track of individuals involved, unless the document is classified at the highest level or comes from a third party. Besides missing an overall picture of who is precisely involved (not merely at an abstract level, but when a specific document is concerned), the actors we examined do not have mechanisms such as an overview of documents that would be declassified. Reports or reviews with regard to internal oversight are also lacking.

It cannot be ignored that the security aspects of the classification system are highly relevant; after all that is why the system was built in the first place. However, the system is designed to fit a security rationale of protection of sensitive information without addressing the relation of the system to issues that it has direct consequences for, such as openness. All these issues would require small steps of reform in order to make the EU system not merely one focused on security but also balance it with internal oversight.
Hence, the empirical findings suggest that discretion, which it was one of the main aims of this chapter to identify, is not as such an issue at the EU level. We actually noted instances when the EU has no discretion whatsoever, due to the role of the Member States. One such example is the vetting procedure, where the EU has no mechanisms or procedures of its own and relies on the Member States. However, in instances where possible discretion could arise, such as the decision to classify, the issue is not that the decision involves a level of discretion, but rather that no mechanism is set to guide or support the decision from a perspective of oversight.

5.3.2 Differences and Similarities in the EUCI Practices

The EU legal regime on classified information is fragmented and administrative. As Chapter IV elaborated in greater details, the EU legal regime does not have an explicit legal basis in the Treaties and the classification of documents is treated as part of the rules of procedure. These features lead us to question whether and to what extent in practice we could notice differences in the rules and their application. The mere fragmentation, meaning that the rules were established separately and individually, does not as such imply that there would be no common model or standards on the overall architecture of EUCI.

Some differences in the EUCI system exist. We put aside issues that arise due to the nature of the institution or the body, such as differences between law enforcement and diplomacy. When the classification system is the main focus, the following differences may be noted. Firstly, the administrative organisation of bodies varies and depends on the actor. The larger institutions work on a two-tier level, central and local. Secondly, in cases where the legal or technical principles regarding EUCI are the same, differences could be noted in their application: some actors are more focused on the usability of the information. This is related to the distinction we drew on the disproportionality between the protection and the usability of the information. However, these differences in the rules and their application are not vast nor of such a nature to signify problems with the management and exchange of classified information.

Many similarities derive from our discussion, particularly when EUCI is more closely examined in the respect of who actually has classification authority and the process of classification. The following applies to all actors. Firstly, regarding the actors behind the scenes, at a micro level, the structure of individuals is guided by the same principles of security clearance and need-to-know. These principles function
in a similar procedural sense. For the structure of the ‘inside-insiders’, the security clearance is less relevant; it is the need-to-know principle that actually limits internal access to classified information. However, practice is focused on ‘tailor made access’, ignoring the strict access rules if the official considers her colleague should see the information as well. We noted further that each official has classification authority and it is more a question of seniority and rank in the administration that is relevant to distinguish the level of classification someone can mark. Secondly, the relevance of the Member States is a common denominator for all EU actors, albeit to different extents. The relation of EU actors to the Member States regarding the classification system is of particular relevance and bares consequences in EU procedures. The position of the Member States is important in two respects: the dependency of EU actors on national information and national rules applicable to procedures that are of EU character. In this manner, national rules and national working methods together with the EU rules and practices create a compound EUCI regulation.

**Conclusions**

This chapter examined the practices of EUCI, focusing particularly on the discretion of officials to classify documents and the arrangements for internal access to classified information. Its aim is to provide ‘real life’ perspectives from individual ‘Eurocrats’ but, simultaneously, to draw attention to patterns in practice and to provide an overall institutional perspective on the EU practices of official secrets and its special characteristics.

Discretion is inherent in the decision to classify documents. This is the starting point to understanding the workings behind the EUCI system. From the perspective of openness, it is relevant that this inherent discretion is addressed by review mechanisms. In EU practice, specific security guidelines and manuals as well as security briefings are a common feature for making sure that officials classify with prudence. However, this prudence is directed fully at security and considerations for openness are lacking. Indeed, not only are they lacking but there is a sense from EU officials, as some of their statements directly illustrate, that considerations of openness and public access to information are not relevant when it comes to classifying documents. In addition, the legal definitions of the security markings are broad and vague leaving space for interpretations of what could constitute a damage or security risk and hence
potentially lead to classifying more documents, even if EU officials apply EUCI in good faith. EU officials are aware that categories are broad and the impossibility of administrative review proving that a specific classification decision is wrong, unless it is a ‘clear case’ of negligence or abuse. This in turn implies the lack of perspective for disciplinary measures as a possible disincentive for over-classification. It is noteworthy that in practice the EU security markings are applied to cover information that officials would not want to read in the press, that could be embarrassing for a political figure, or even if some background facts are considered ‘inappropriate’ as they would reveal the internal ‘cooking’ of EU decision-making.

The three key issues: discretion, interpretations of the legal terminology for the security markings and the lack of mechanisms to review the decisions are overall features of classifying documents in the EU. This led to questions on whether there is a register of documents or other internal oversight of the classified documents. Yet, as it was noted, internal registers are not meant to facilitate reviews. Furthermore, these registers are not public nor is the amount of classified information in the EU overall. Some institutions such as the Council report on the amount of classified information, but these numbers are not always fully accurate, and more importantly, documents from originating parties may be blocked from the register and hence they would be publicly untraceable.

In the practices of EUCI, similar to its establishment and regulation, considerations pertaining to openness are lacking. It should be emphasised however, that unlike the establishment and regulation of secrecy, EU officials’ discretion and autonomy regarding classifying documents are significantly minor. Derivative classification predominates in the EU. Accordingly, the discretion is to a very large extent limited for the derivative classifier, whose role is merely to use the classified information in strict accordance to the originator’s will. In the EU’s work on security, the originators of the information are mostly the Member States, as can be seen in the examples of Europol or the EU Intelligence Analysis Centre, or third states and organisations. The derivative classification operates strictly from a security perspective and enforces a more rigid secrecy culture as it makes the highest classification marking applicable to the entire document when, for example, a variety of documents with different security markings are used. Furthermore, it creates a space of non-responsibility for the EU official as she merely needs to reproduce the classification stamp without challenging it. In fact, from a security perspective, maintaining the originator’s marking is

85 Respondents No. 3.
seen as positive as it provides the necessary assurances of a rigid security culture and trustworthiness by control. The national administrative culture of how secrets are managed affects EU level decisions and processes due to the extensive applicability of derivative classification of EUCI. As it was noted, derivative classification indicates following the original classification marking in a strict manner, which in turn implies that discretion is minimal in the classification process at EU level.

Internal access to classified information is the second main aspect examined in this chapter. Limitations for internal access are maintained through two key security arrangements: the security clearance and the principle of ‘need-to-know’. Regarding the former, the EU is dependent on the national rules and national authorities. Whether an EU official or a Member of the European Parliament is granted a security clearance and to which level of classification marking, are contingent upon the varied national procedures, some of which are more intrusive to privacy. The need-to-know principle may significantly limit internal access if we were to examine it strictly from a legal perspective. Yet, in practice, EU officials would informally share information if they personally considered the information to be valuable to their colleagues. In practice, more pragmatism and usability of classified information is favoured as opposed to strictly its security, taking into account the juxtaposition between these two aspects due to security markings and different handling procedures.

The EU practices of official secrets reflect a level of pragmatism regarding the usability of classified information and, more importantly, a neglect of internal oversight considerations fostering openness. It is debateable whether and to what extent it represents the broader EU administrative culture or whether its specificities make it a ‘special’ case; yet without a broader comparative analysis any statement could merely be of a speculative nature. Without adopting this wider comparative organisational lens to examine the EUCI practice, the current discussion does enable us to examine its links and implications with rules and practices of oversight, as the following Part III of this research does.