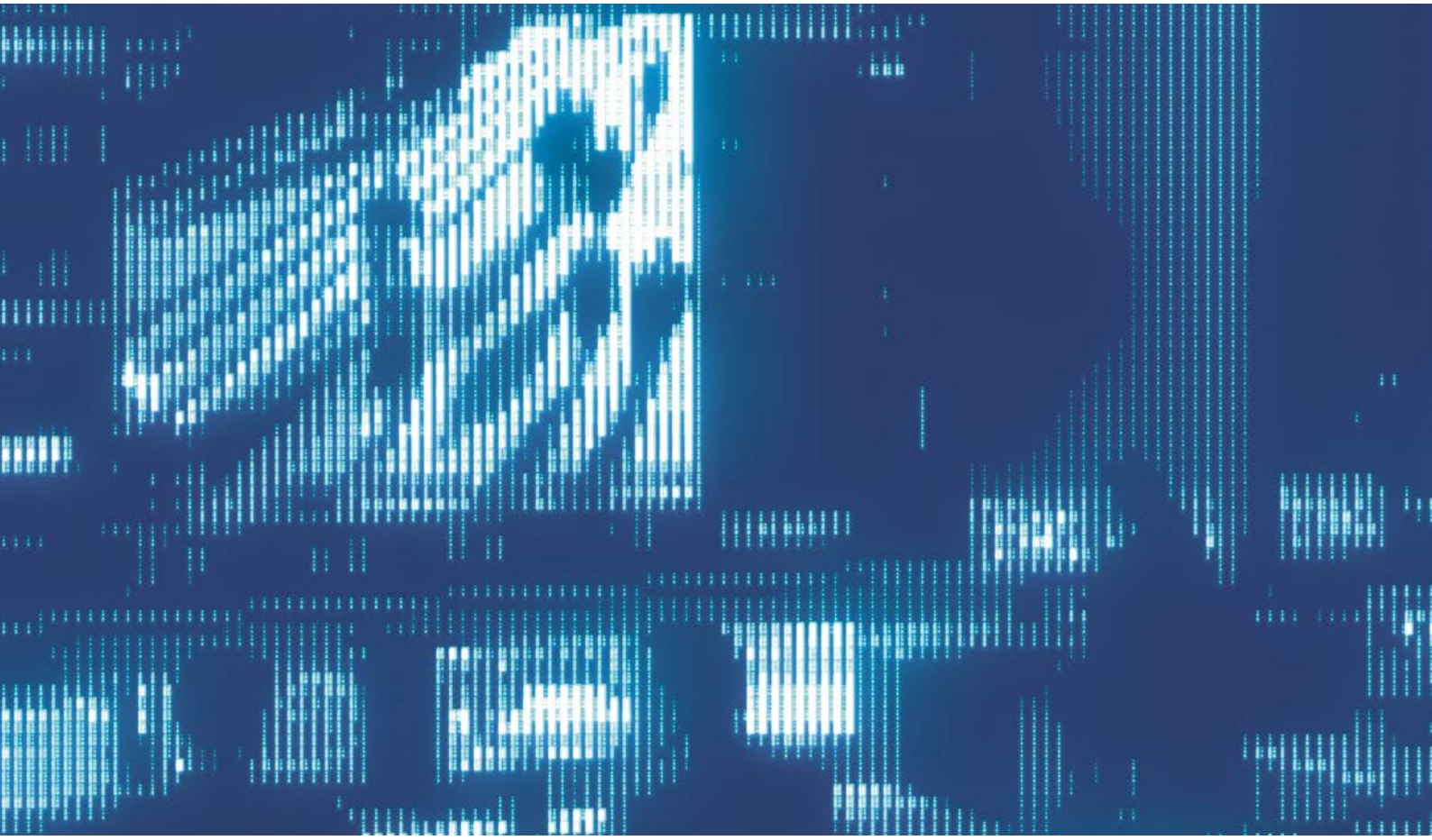
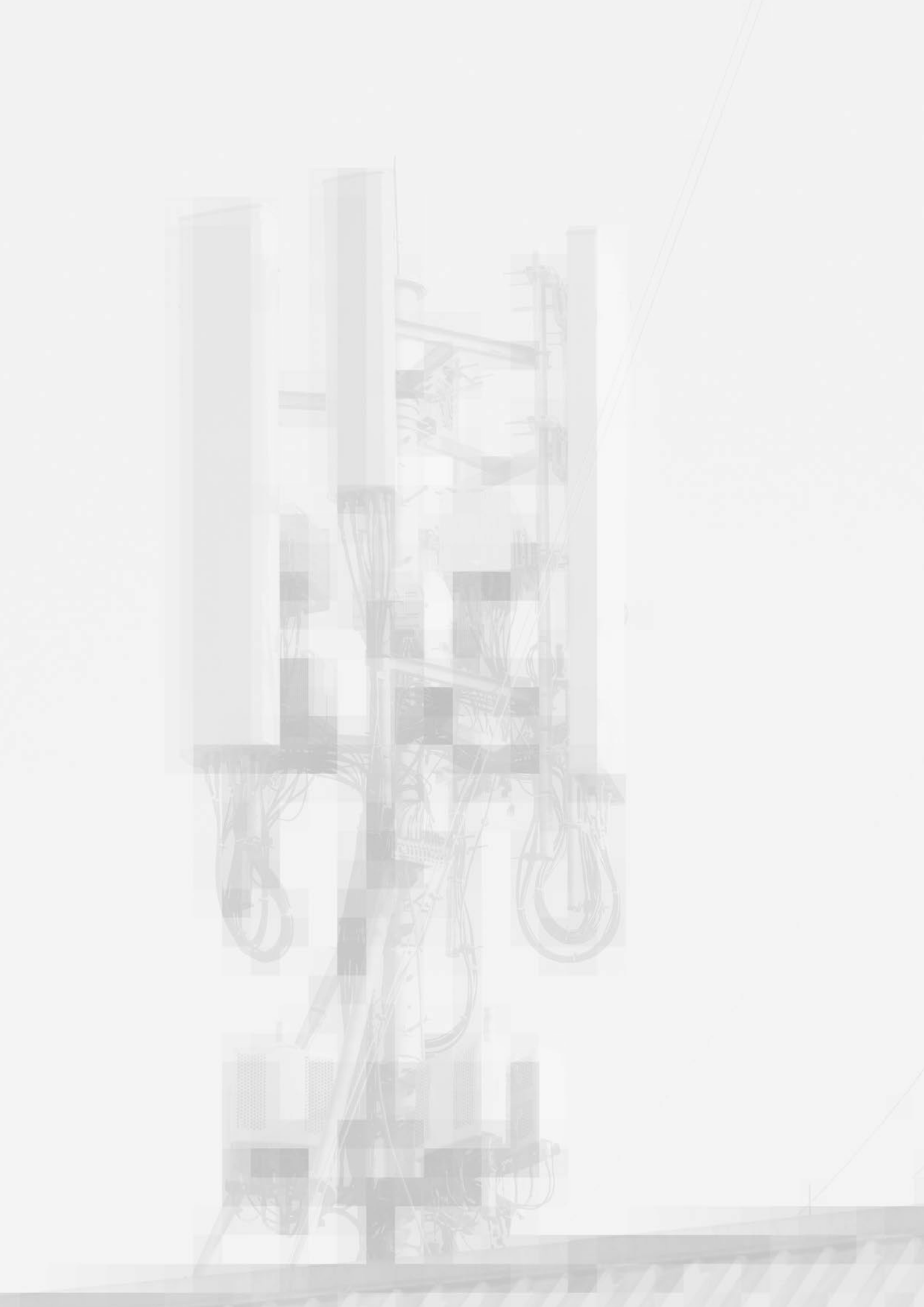
EOS COMMITTEE

NORWEGIAN PARLIAMENTARY OVERSIGHT COMMITTEE
ON INTELLIGENCE AND SECURITY SERVICES



ANNUAL REPORT 2022

DOCUMENT 7:1 (2022–2023)



To the Storting

In accordance with Act No 7 of 3 February 1995 relating to the Oversight of Intelligence, Surveillance and Security Services (the Oversight Act) Section 17 third paragraph, the Committee hereby submits its report about its activities in 2022 to the Storting.

The annual report is unclassified, cf. the Oversight Act Section 17 third paragraph. Pursuant to the Security Act, the issuer of information decides whether it is classified. Before the report is submitted to the Storting, the Committee sends the relevant sections of the report to each of the respective services so that they can clarify whether the report complies with this requirement. The services have also been given the opportunity to check that there are no factual errors or misunderstandings in the text.

Oslo, 29 March 2023

Astri Aas-Hansen

Kristin Krohn Devold

Magnhild Meltveit Kleppa

Erling Johannes Husabø

Camilla Bakken Øvald

Jan Arild Ellingsen

Olav Lysne

Henrik Magnusson

Photo: Anki Grøthe

The EOS Committee in 2022. From left: Camilla Bakken Øvald, Jan Arild Ellingsen, Olav Lysne, Astri Aas-Hansen (chair), Magnhild Meltveit Kleppa, Kristin Krohn Devold (deputy chair) and Erling Johannes Husabø.

Contents

Remark: If there is any difference between the Norwegian and the English version, it is the Norwegian version that is valid.

1.

The Committee's remit and composition

The EOS Committee is a permanent, Storting-appointed oversight body whose task it is to oversee all Norwegian entities that engage in intelligence, surveillance and security activities (EOS services). Only EOS services carried out by, under the control of or initiated by the public administration are subject to oversight by the EOS Committee.[1]

The purpose of the oversight is:

1) to ascertain whether the rights of any person are violated and to prevent such violations, and to ensure that the means of intervention employed do not exceed those required under the circumstances, and that the services respect human rights,
2) to ensure that the activities do not unduly harm the interests of society, and
3) to ensure that the activities are kept within the framework of statute law, administrative or military directives and non-statutory law

The Committee can express its opinion on matters that lie within the area of oversight. The Committee shall not seek more extensive access to classified information than warranted by the oversight purposes, and shall insofar as possible show consideration for the protection of sources and safeguarding of information received from abroad. Ex-post oversight is practised in relation to individual cases and operations, but the Committee is entitled to be informed about and express an opinion on the services' current activities.
The Committee may not instruct the EOS services it oversees, or be used by them for consultations. The oversight shall cause as little inconvenience as possible to the services' operational activities. The Committee shall show consideration for national security and relations with foreign powers in its oversight activities. The Committee does not express its opinion on the services' effectiveness, how they prioritise their resources etc.

The Committee has seven members. They are elected by the Storting in plenary session on the recommendation of the Storting's Presidium for terms of up to four years. The members can be reappointed once. No deputy members are appointed.

The Committee is independent of both the Storting and the Government. The Government cannot issue instructions to the Committee. The Storting may, however, in plenary decisions order the Committee to undertake specified investigations within the oversight remit of the Committee.

Committee members cannot also be members of the Storting, nor can they previously have worked in the EOS services. The committee members and secretariat employees must have top level security clearance and authorisation, both nationally and pursuant to treaties to which Norway is a signatory. This means security clearance and authorisation for TOP SECRET and COSMIC TOP SECRET, respectively.

Below is a list of the committee members and their respective terms of office for 2022:

Astri Aas-Hansen, Asker, chair
1 July 2019 – 30 June 2024

Kristin Krohn Devold, Oslo, deputy chair
1 July 2021 – 30 June 2025

Magnhild Meltveit Kleppa, Hjelmeland
1 July 2019 – 30 June 2024

Erling Johannes Husabø, Bergen
1 July 2019 – 30 June 2024

Camilla Bakken Øvald, Oslo
1 July 2019 – 30 June 2024

Jan Arild Ellingsen, Saltdal
1 July 2021 – 30 June 2025

Olav Lysne, Bærum
1 July 2021 – 30 June 2025

Of the seven board members, five have political backgrounds from different parties. The other two have professional backgrounds from the fields of law and technology.

1 References to the Oversight Act are found in the Act relating to National Security (the Security Act) Section 11-1, the Act relating to the Norwegian Intelligence Service (the Intelligence Service Act) Section 2-6, and the Act relating to the Processing of Data by the Police and the Prosecuting Authority (the Police Databases Act) Section 68.

2.

Key figures

The Committee's expenses amounted to NOK 35,095,000 in 2022. The total budget, including transferred funds, amounted to NOK 36,835,000. The Committee has applied for permission to transfer the unused funds to its budget for 2023.

The workload of the chair of the Committee corresponds to about 30 per cent of a fulltime position, while the office of committee member is equivalent to about 20 per cent of a full-time position.

The Committee is supported by a secretariat. At yearend 2022, the Committee Secretariat consisted of 21 full-time employees: the head of the secretariat, a legal unit with a staff of nine, a technology unit with a staff of six and an administrative unit with a staff of five. One position was vacant.

3.

Overview of the Committee's activities in 2022

3.1 General information about the oversight year

The Russian military attack on Ukraine on 24 February 2022 changed the political security situation in Europe. This affected the intelligence and security services in 2022. The Committee is aware of its obligation to organise its oversight in such a way that it causes as little inconvenience as possible to the services' ongoing activities.

It is in difficult times that the principles of the rule of law are challenged. The Committee's function is to keep an independent eye on the services' actions and maintain the fundamental principles of law. It is an important oversight task to ensure that the services do not interfere with the rights of individuals to a greater extent than the law permits.

The law does not always develop in step with the changing threat situation and accelerating technological developments. The Committee is aware that the failure to update the legislation poses a challenge for the services. At the same time, the development of law depends on open and informed public debate. The potential effects of new technology are not easy to predict. Several dilemmas arise at the intersection between protection of the rights of individuals, national security and the safety of the population. It is up to the legislators to balance these interests in a field where it is vital that the citizens have trust in the authorities.
The Committee is concerned with the sufficient clarity of the legal provisions authorising interventions by the intelligence and security services. This is a prerequisite for the Committee's ability to determine if the services conduct their activities in accordance with the legislators' intentions.

3.2 Oversight activities

In 2022, the Committee conducted 22 inspections. Some of the inspections were directed against several of the services at the same time.

In 2022, the Committee held nine internal full-day meetings, in addition to internal working meetings on site in connection with inspections. During the internal meetings, the Committee discusses planned and completed inspections, complaints and cases raised on the Committee's own initiative, reports to the Storting and administrative matters.

The Committee raised 8 cases with the services on its own initiative in 2022, compared with 13 in 2021. The Committee concluded 16 cases raised on its own initiative in 2022, the same number as in 2021.

The Committee investigates complaints from individuals and organisations. In 2022, the Committee considered 40 complaints against the intelligence and security services, compared with 25 complaints in 2021. Several of the complaints were directed against more than one service. The Committee concluded 38 complaints in 2022, compared with 26 complaints in 2021.

3.3 The Committee's oversight methods

Inspections of the services is an integral part of the Committee's work. The Committee's inspections consist of a briefing part and an inspection part. The topics of the briefings are mostly selected by the Committee. In 2022, the committee increased its topical approach to the oversight.

The services are also asked to brief the Committee on any matters they deem to be relevant to the Committee's oversight, including non-conformities that the services have identified.

The Committee is briefed about the service's ongoing activities, national and international cooperation, and cases that have given rise to public debate. The Committee asks verbal questions during the briefings and sends written questions afterwards.

During the inspection part, the Committee conducts searches directly in the service's computer systems. The services are not notified of what the Committee searches for. This means that the inspections contain considerable unannounced elements. The goal is to conduct a qualified spot check-based oversight. The thorough preparations of the Secretariat in the services' computer systems enable the Committee to conduct targeted inspections.

The Committee initiates cases on its own initiative based on findings made during its inspections. Such cases are also initiated based on information received from whistle-blowers, or from issues that have attracted public attention. Documents from the service in question are reviewed. The services' employees can also be summoned for interviews. The service must always be given the opportunity to state its opinion on the issues raised in the case before the Committee submits its statement.

3.4 The Committee's consideration of complaints

Complaints that fall within the Committee's oversight area are investigated in the service or services that the complaint concerns. The Committee has a low threshold for considering complaints. The complaints vary in complexity.

The Committee's statements to complainants shall be

Inspections by the Committee in 2022

Oslo
The NIS, PST, NSM and FSA

Bærum
NSM

Bergen
The Naval Special Operations Command

Ringerike
The NIS

Hamar
PST

Moss
The Civil Security Clearance Authority

Ski
PST

Vadsø
The NIS

Kirkenes
PST

Vardø
The NIS

Setermoen
The Army Intelligence Battalion

unclassified. It is classified information that a person is under surveillance, as well as information that a person is *not* under surveillance.[2] It is only if the Committee's investigations show that the complainant's rights have been violated, that the Committee can confirm to the complainant that the person in question has been under surveillance by the service – as the Oversight Act states that the Committee can inform the complainant that 'criticism' has been expressed.

If the Committee is of the opinion that a complainant should be given a more detailed explanation, it can propose this to the service in question or to the responsible ministry. The service's decision regarding classification of information is binding on the Committee. The Committee is therefore prevented from informing the complainant about the basis for criticism without the consent of the service or the responsible ministry.

3.5 Consultation submissions

The EOS Committee has submitted two consultation submissions in 2022:

- Consultation submission of 8 April 2022 concerning amendments to the Oversight Act (Appendix 1)
- Consultation submission of 26 September 2022 concerning amendments to the Intelligence Service Act (Appendix 2)

3.6 External activities

The Committee hosts an annual conference every March. The annual conference is open to everyone. The topic for the 2022 conference was oversight of bulk collection of information. More than 100 people attended the conference.

The Standing Committee on Scrutiny and Constitutional Affairs met with the EOS Committee to discuss relevant issues. The EOS Committee also met with Minister of Defence Odd Roger Enoksen and described its oversight of the intelligence and security services that fall within the minister's area of responsibility. The Norwegian Bureau for the Investigation of Police Affairs met with the Committee to clarify certain questions regarding the boundary between their respective remits.

The International cooperation between oversight bodies has resumed after the pandemic. In 2022, the Committee attended the Nordic Oversight Conference in Stockholm and went on a study trip to London to learn more about the British oversight system. The Committee met with the Investigatory Powers Commissioner's Office, the Investigatory Powers Tribunal, the organisation Privacy International and the intelligence services MI5 and GCHQ.

See Appendix 3 for an overview of the Committee's other external activities.

Sir Brian Leveson, head of the British oversight body IPCO, was the keynote speaker at the EOS Committee's annual conference in Oslo in March 2022.

Photo: Arvid Grøtting

The Committee was on a study trip to London in October 2022. This picture is taken outside the Royal Courts of Justice.

Photo: The EOS Committee

2 The Oversight Act Section 15 first paragraph second sentence reads as follows: 'Information concerning whether or not a person has been subjected to surveillance activities shall be regarded as classified unless otherwise decided.'

4.

The Norwegian Intelligence Service (NIS)

The NIS is Norway's foreign intelligence service

4.1 General information about the oversight

The Committee has conducted three inspections of the NIS headquarters in 2022, in addition to inspections of the NIS stations in Vadsø and Vardø and at Ringerike, as well as its locations in the Army Intelligence Battalion and the Norwegian Naval Special Operations Commando. The Committee also inspected the Joint Intelligence and Counter-Terrorism Centre (FEKTS), where the NIS cooperates with PST, and the Joint Cyber Coordination Centre (FCKS). FCKS is a centre for cooperation between the NIS, PST, NSM and the National Bureau of Crime Investigation (Kripos).

During its inspections of the NIS, the Committee focuses on the following:

- The NIS's use of collection methods that could entail interference in relation to individuals pursuant to the Intelligence Act chapter 6.
- The service's processing of information
- The service's exchange of information with domestic and foreign partners
- Cases that have been submitted to the Ministry of Defence[3]
- Internal approval cases[4]
- National control of the NIS's stations, equipment, methods and information collection

In 2022, the Committee's oversight has focused particularly on the NIS's bulk collection.

The Committee's right of access does not extend to information defined as particularly sensitive information[5] by the NIS. The Committee is regularly informed about the scope of information that falls within this category. The information is made available to the Committee once it is no longer defined as being particularly sensitive.[6]

4.2 Oversight of facilitated bulk collection

In 2022, the Committee conducted oversight activities relating to the service's development of the system for facilitated bulk collection of transboundary electronic communication. Pursuant to the Intelligence Service Act Section 7-11, the EOS Committee is charged with continuously overseeing the NIS's compliance with the provisions on facilitated bulk collection.

4.2.1 The testing and development phase

During an inspection in December 2021, the Committee was informed that the NIS was in dialogue with an electronic communications provider about the transfer of real data after 1 January 2022. The purpose of the planned transfer was to test and develop the facilitated bulk collection system.

The Intelligence Service Act's provisions on facilitated bulk collection entered into force 1 January 2022, with the exception of Section 7-3. The Intelligence Service Act Section 7-3 stipulates that the Director of the Norwegian Intelligence Service has the power to instruct electronic communication providers to give the service access to electronic communication in the manner described in Section 7-2 of the Act. With reference to the fact that Section 7-3 had not yet entered into force, the Committee asked the service about the legal basis for transferring real data for testing and development purposes.

The NIS argued that the Intelligence Service Act Section 7-2 constituted an independent legal basis that allowed the service to instruct electronic communication providers to disclose real data for testing purposes. Alternatively, the service argued that the Personal Data Act gave the provider a right to disclose real data to the NIS.

The EOS Committee did not share this view. Since the Intelligence Service Act Section 7-3 on decision-making authority had not entered into force, the Committee believed the NIS did not have legal authority to instruct electronic communication providers to disclose real data pursuant to Section 7-2. The Committee was also of the opinion that even if the electronic communication provider might have a legal basis in other legislation for disclosing real data, that would not constitute a sufficient legal basis for the NIS in this matter.

In a later inspection, the NIS informed the Committee that no real test data would be transferred based on the legal basis applicable at the time, and that the Committee's legal opinion had been raised with the Ministry of Defence.

The Government put the Intelligence Service Act into force for testing and development purposes by a Royal Decree on 2 September 2022.

3 Pursuant to the Intelligence Service Act Section 2-5, the Ministry's approval is required in cases concerning a) the establishment of collaboration and agreements with foreign services or international organisations, b) the launching of special intelligence operations that could raise political issues, c) other cases of particular importance.

4 Internal approval cases can concern permission to share information about Norwegian persons with foreign partners or to monitor Norwegian persons' communication when the persons are abroad.

5 1. The identity of the human intelligence sources of the NIS and its foreign partners 2. The identity of foreign partners' specially protected civil servants 3. Persons with roles in and operational plans for occupation preparedness 4. The NIS's and/or foreign partners' particularly sensitive intelligence operations abroad which, were they to be compromised, a. could seriously damage the relationship with a foreign power due to the political risk involved in the operation, or b. could lead to serious injury to or loss of life of own personnel or third parties.

6 Read more in section 5.5 of the Committee's annual report for 2020.

4.2.2 Facilitation of oversight

The Committee has continued its work on developing an oversight concept for facilitated bulk collection. The Secretariat has been given additional resources to support the Committee in its continuous oversight activities. The Intelligence Service Act Section 7-11 requires the NIS to facilitate the Committee's oversight through technical solutions. The Committee has drawn up a list of requirements for oversight functionality in the service's systems. The NIS has been asked to introduce technical solutions that meet these requirements. The service has stated that the work is under way.

In 2023, the Committee will follow up the NIS's facilitation of oversight and further develop its oversight of facilitated bulk collection.

4.3 Purchase of metadata in bulk

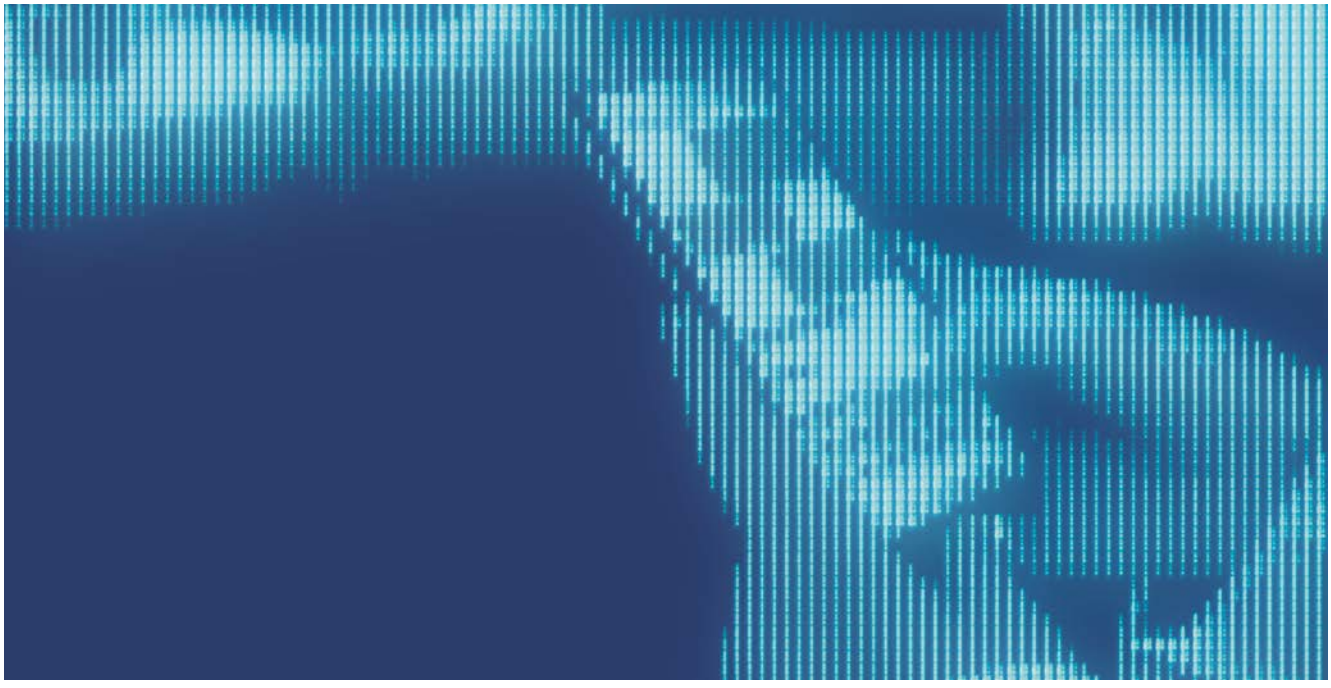
The Committee has asked the NIS about the service's legal basis for purchasing metadata from commercial enterprises. In the NIS's view, certain procurements of data from commercial providers did not constitute use of an intrusive method under the Intelligence Service Act Chapter 6.

The service was therefore of the opinion that the prohibition on collection in Norway set out in Section 4-1 of the Intelligence Service Act did not apply to the type of metadata procurement concerned. The NIS's view was that the way in which the service comes into possession of the data is the factor determining whether the procurement falls within the scope of the Intelligence Service Act Chapter 6.

The Committee considered the key question to be whether the bulk purchase of metadata that contain personal data constitutes an interference with individuals' privacy. Case law from the European Court of Human Rights (ECtHR) shows that a clear basis in law is required to use methods that constitute such interference.

In the preparatory works to the Intelligence Service Act, the Ministry of Defence wrote that 'the objective of the bill is to provide a clearer legal framework for the Intelligence Service's use of intrusive methods out of consideration for the statutory human rights requirement'.[7]

Although the Ministry considered that collection from open sources would 'fall within the general freedom of action',[8] the Ministry nevertheless proposed regulating the method separately. The reason given in the consultation paper was that 'this collection takes place without the consent of the person or persons concerned, and because the sum of the information obtained about an individual and the collation of such information over time could, depending on the circumstances, constitute interference in relation to individuals, even



7 Proposition No 80 to the Storting (Bill) (2019–2020), section 10.3.3.

8 Proposition No 80 to the Storting (Bill) (2019–2020), section 8.5.4.

in cases where the individual him/herself chose to share the information openly'.[9]

The Committee stated that the same considerations apply when purchasing bulk metadata that contain personal data that people have left online. The collation of such metadata could generate content data, and there is a risk that collation of data from several sources could make it possible to identify individuals from datasets that are initially anonymous.

In the Committee's opinion, such purchases must be deemed to constitute information collection that could entail interference in relation to individuals. Such collection may only take place to the extent that it is warranted by the Intelligence Service Act Chapter 6. The Committee disagreed with the NIS's assessment of legality.

The Committee urged the NIS to conduct a new assessment of whether the use of this method must have a basis in Chapter 6 of the Intelligence Service Act to be lawful. The NIS has stated that the service is considering raising the matter with the Ministry of Defence.

4.4 Logging of searches of raw data in bulk

Technical facilitation of the Committee's oversight is becoming increasingly important as the quantities of data increase, and the services' computer systems become more complex. Oversight mechanisms are a prerequisite if the NIS's bulk collection[10] is to be in compliance with the European Convention of Human Rights (ECHR). The Intelligence Service Act requires the NIS to log searches of raw data in bulk based on a search term linked to a person in Norway.[11] The purpose of the log is to prevent misuse and facilitate effective oversight.[12]

Based on the above, the Committee requested an overview of the most recent searches in this category.[13]

The service stated that all searches of raw data in bulk are logged, but that there is no function for indicating whether a search is based on a person located in Norway. According to the service, preparing such an overview would be a very time-consuming manual task. The NIS also stated that the Intelligence Service Act's logging requirement is met because it is possible to link individual searches to the assessments and approvals on which they were based. The service referred to the fact that the Act does not set out specific requirements for how the searches are to be logged.

The EOS Committee did not share the service's view. The vast quantity of information in the log and the challenges of navigating it mean that the Committee is unable to conduct effective oversight. The fact that the service was unable to present an overview of the most recent searches in a category for which special grounds are required, shows that the statutory requirement for logging for oversight purposes has not been met.

For a log to be useful for oversight purposes, it must be possible to use the log to identify errors. It is not good enough that the log can be used to investigate an existing suspicion that a non-conformity has occurred.

The Committee criticised the NIS for inadequate fulfilment of the requirement for logging of searches in bulk data for oversight purposes. The Committee urged the service to further develop the log function to enable the Committee to conduct effective oversight.

The NIS has maintained its view that the minimum requirements set out in the Act have been met. The service also stated that it is not satisfied with a solution that provides the bare minimum of functionality, and that work is currently under way to develop functionality that will enable more effective oversight of searches of raw data in bulk.

4.5 The NIS's handling of a source

The Committee has investigated the NIS's handling of a source who has carried out several assignments targeting a non-state actor. The Committee is concerned with ensuring that the NIS handles its sources based on a due dilligence assessment of their suitability. What constitutes due diligence care must be assessed on a case-by-case basis, and the service's need for information, the risk and circumstances relating to the source will be relevant factors.

In this case, the Committee shared the NIS's opinion about

9 Consultation paper – Draft bill for a new Act relating to the Norwegian Intelligence Service, section 10.5.7.3.

10 The Intelligence Service Act Section 1-3 letter (i) defines bulk as 'collections of information and data sets in bulk, where a substantial amount of the information is considered irrelevant for intelligence purposes'. Raw data in bulk is information whose intelligence value has not yet been assessed, and where a substantial amount of the information is considered irrelevant for intelligence purposes. The NIS may collect raw data in bulk when necessary, cf. the Intelligence Service Act Section 5-3. The NIS may collect raw data in bulk even though information regarding persons in Norway may also be included, cf. the Intelligence Service Act Section 4-7.

11 Only if strictly necessary in order to perform a task related to collection of information about foreign threats may the service search raw data based on a search term linked to a person located in Norway, cf. the Intelligence Service Act Section 5-3 third paragraph.

12 Proposition No 80 to the Storting (Bill) (2019–2020) Chapter 17 Comments on Section 5.3.

13 This case is not related to the NIS's facilitated bulk collection system.

the need for information, but considered that, due to circumstances relating to the source, the service had nevertheless failed to exercise due diligence in its handling of the source. The actions in question took place some time ago, and the NIS's regulations concerning how to handle sources have since undergone significant development.

4.6 Oversight of the prohibition against surveillance in Norway

The Committee has considered three questions concerning the demarcation between the prohibition against surveillance of persons in Norway and the service's surveillance of Norwegian persons abroad.[14]

Firstly, the Committee asked what the NIS does to clarify whether a person has returned to Norway, so that the surveillance could be discontinued. The Committee has assumed that the service always strives to minimise the time gap between a return to Norway and the discontinuation of surveillance.

Secondly, the Committee considered the surveillance of a Norwegian phone number that the NIS believed was being used by two different persons. Both the persons in question were Norwegian citizens, but only one of them was a target of intelligence relevance who sometimes spent time abroad. The Committee criticised the NIS for not having considered the potential consequences this interference could have for the person who was not a target that is relevant for intelligence.[15]

Thirdly, the Committee considered the surveillance of a Norwegian phone number that, due to an error, was not removed from the service's surveillance system when it was no longer relevant for intelligence purposes. The Committee criticised the NIS for having violated Section 4 of the Intelligence Service Act in force at the time.

4.7 Internal regulations on collection in cyberspace

The NIS's information collection methods are regulated by law through the Intelligence Service Act that came into force with effect from 1 January 2021. The NIS has operationalised some of the provisions of the Act in internal regulations on collection activities in cyberspace. These regulations are classified. The Committee has carried out a general assessment of whether the internal regulations are in line with the Intelligence Service Act.

The Committee has urged the service to consider certain provisions in its internal regulations to ensure that they are in harmony with the Intelligence Service Act, and it has asked the service to facilitate future oversight by the Committee in this area.

The NIS has notified the Committee that one of the issues will be raised with the Ministry of Defence, while another will be considered in connection with a revision of the regulations. The NIS also stated that it wishes to facilitate for effective oversight.

4.8 Complaints against the NIS

The Committee accepted 11 complaints against the NIS in 2022, compared with 10 complaints in 2021. Several of these complaints were also against more than one of the services. The Committee concluded 10 complaints against the NIS in 2022. None of the concluded cases resulted in criticism of the NIS.

14 All three questions were considered pursuant to the Intelligence Service Act of 1998, since the activities they concerned took place before the Intelligence Service Act of 2020 came into force on 1 January 2021.

15 Cf. Supplementary provisions concerning the Norwegian Intelligence Service's collection of information concerning Norwegian persons abroad and the disclosure of personal data to cooperating foreign services Section 3.

5.

The Norwegian Police Security Service (PST)

Photo: Espen Hofoss / Norwegian Armed Forces

PST is Norway's domestic intelligence and security service

5.1 General information about the oversight

In 2022, the Committee conducted four inspections of the PST Headquarters (DSE) in Oslo. The Committee also inspected the PST entities in Finnmark, Eastern and Innlandet police districts.

Furthermore, the Committee inspected the Joint Intelligence and Counter-Terrorism Centre (FEKTS), where the NIS cooperates with PST, and the Joint Cyber Coordination Centre (FCKS). FCKS is a centre for cooperation between the NIS, PST, NSM and the National Bureau of Crime Investigation (Kripos).

During its inspections of PST, the Committee focuses on the following:

- The service's collection and processing of personal data
- The service's new and concluded prevention cases, averting investigation cases and investigation cases
- The service's use of covert coercive measures (for example telephone and audio surveillance, equipment interference and covert searches) and handling of sources
- The service's exchange of information with foreign and domestic partners

In 2022, the Committee has focused on oversight activities relating to PST's registration of persons, restriction of access to information and deletion of personal data. The Committee has therefore asked PST about restriction of access to information in the service's systems, among other things. The Committee will follow up this matter in 2023.

5.2 Unlawful drone surveillance in prevention cases

The Committee has considered PST's use of drones to gather information in prevention cases. It follows from the regulatory framework currently in force that PST can use 'fixed' cameras,[16] but not mobile ones. Court permission is also required for PST to use fixed cameras. PST did not request the court's permission to use drones, but considered in four cases that such decisions could be made by the director of PST.

PST referred to the Director General of Public Prosecutions' guidelines[17] for the use of mobile cameras (including drones) by the police for investigation purposes. The service considered that the legal policy objectives underlying the Criminal Procedure Act Section 202 a did not constitute grounds for different limitations in investigation and prevention cases.

The Committee referred to the fact that the Norwegian Constitution and the ECHR require any interference by the State with the privacy of its citizens to be based on legal authority. Surveillance using drones constitutes interference with privacy. The statutory requirement means that the legal basis must be sufficiently clear, predictable and accessible to citizens, as well as offer satisfactory due process guarantees. No such legal basis exists for using drones in prevention cases.

Based on the above, the Committee strongly criticised PST for having used a covert surveillance method without a legal basis provided in law. The Committee urged the service to stop using this method and requested a reply from PST.

PST informed the Committee that the service has taken note of the Committee's assessment and stopped using the method. PST also informed the Committee that the matter has been raised with the Ministry of Justice and Public Security, and that the Ministry has taken the initiative to regulate the police's use of drones in law.

As part of PST's follow-up of the case, the service has declassified the Committee's concluding statement. The Committee's letter of 10 October 2022 to PST is enclosed as Appendix 4.

The Committee asked for PST's opinion on whether persons who have been subjected to surveillance on unlawful grounds should be informed, cf. the requirement for effective remedy in ECHR Article 13. PST has stated that persons subjected to unlawful surveillance cannot be informed because this aspect of the case cannot be declassified. Pursuant to the Oversight Act Section 11, the public administration's decision regarding classification of information is binding on the Committee.

5.3 PST's use of a source

The Committee has criticised PST's use of a source in a prevention case.

PST asked the source for information without having carried out sufficient ethical assessments of whether this would require the source to breach their duty of confidentiality. When PST received information that the service must have understood could be confidential, they did not ask the source to discontinue their investigations.

The Committee stated that when PST asks a source for information rather than file a petition for a disclosure order with the courts, that creates the impression that they are

16 Cf. the Police Act Section 17 d, cf. the Criminal Procedure Act Section 202 a.

17 Guidelines of 17 September 2021 on the police's use of mobile and remotely controlled cameras for investigation purposes.

circumventing the law. The Committee also stated that documentation in the case was inadequate and urged PST to ensure that all cases involving sources are properly documented.

5.4 Registration of individuals

5.4.1 The Committee's oversight in brief

In its oversight of PST's registrations for preventive purposes, the Committee focuses on checking that the requirements regarding necessity, relevance and specification of purpose are met. One important focus is the strict necessity requirement that applies to the processing of special categories of personal data, for example a person's political or religious beliefs, cf. the Police Databases Act Section 7.

5.4.2 Registration of members of the Storting

The Committee has considered PST's registration of three members of the Storting. PST informed the Committee that the representatives were deemed to possess assets of interest to foreign intelligence activities, and that registration was necessary to prevent them from being targeted by unlawful intelligence. At the same time, the service stated that the registrations were no longer necessary and would therefore be deleted.

The Committee has impressed on PST the importance of individual grounds in such cases. In the Committee's opinion, PST had not substantiated that the necessity criterion was met for these registrations at the time of registration.

5.4.3 Other registrations

The Committee has criticised PST for having registered three people unnecessarily, and therefore also without a legal basis. The Committee also criticised the service for having kept the registration of one person for more than a year longer than the legal basis warranted. PST has informed the Committee that the registered information has been deleted.

5.4.4 Deletion of registration at the request of the Storting

In its annual report for 2021, the Committee informed the Storting that PST had kept a registration that in the Committee's opinion should have been deleted. The Storting asked PST to delete the information about the person in question.[18] PST has informed the Committee that the registered information has now been deleted.

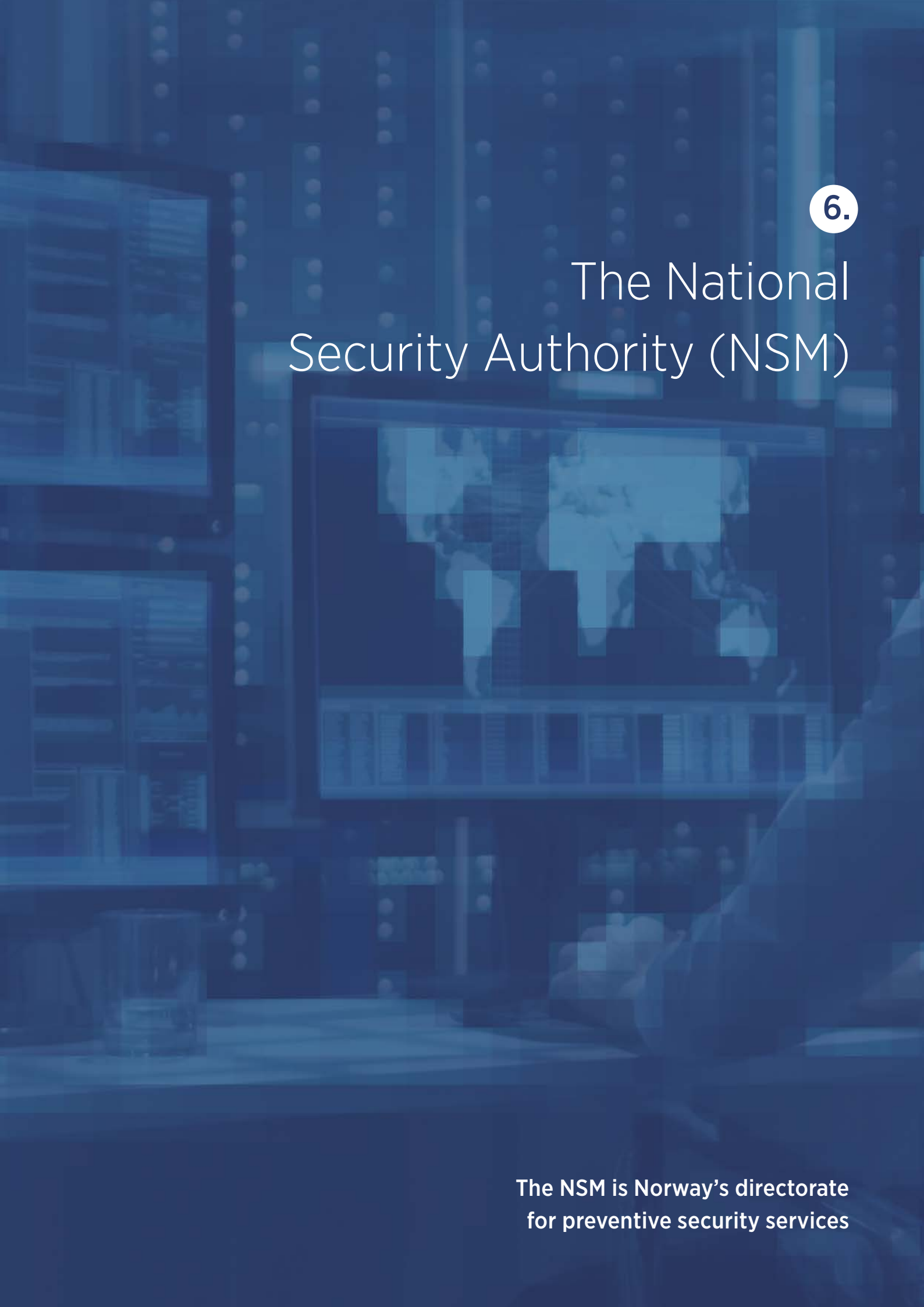
5.5 Complaint cases

The Committee has accepted 24 complaints against PST in 2022, compared with 17 complaints in 2021. Some of these complaints were also against more than one of the services. The Committee concluded 20 complaint cases against PST in 2022.

The Committee expressed criticism against PST in two complaint cases in 2022. More detailed grounds have been provided to the complainant in one of the cases. The complainant was informed that the Committee had criticised PST for having stored information about the complainant for longer than was necessary.

The Committee has criticised PST for inadequate investigations and failure to provide documents to the Committee as part of our investigation of a complaint case. PST submitted all the relevant documents before the Committee's final consideration of the case.

18 Recommendation 432 to the Storting (2021–2022), cf. the EOS Committee Annual report for 2021, section 4.2.



6.

The National Security Authority (NSM)

The NSM is Norway's directorate for preventive security services

6.1 General information about the oversight

In 2022, the Committee conducted two inspections of the National Security Authority (NSM). One of the inspections focused on NSM's processing of security clearance cases. The other inspection was of the Norwegian National Cyber Security Centre (NCSC). The function of NCSC is to protect fundamental national functions, the public administration and business and industry against serious cyber-attacks. The Committee also inspected the Joint Cyber Coordination Centre (FCKS). FCKS is a centre for cooperation between the NIS, PST, NSM and the National Bureau of Crime Investigation (Kripos).

The Committee has had a particular focus on case processing times in security clearance cases in 2022.

During its inspections of NSM, the Committee focuses on the following:

- NSM's processing of cases where security clearance has been denied, reduced or suspended by the security clearance authority, and its processing of complaints in such cases
- NSM's case processing times in security clearance cases
- NSM's cooperation with other services
- NSM's processing of personal data
- NSM's technical capabilities

6.2 Case processing times in security clearance cases

Security clearance cases shall be prepared and decided 'without undue delay'.[19] The security clearance authority must consider on a case-by-case basis how long processing time will be required considering the nature and scope of the case and the case processing resources available.

For the person for whom security clearance is requested, it is important to obtain clarification regarding whether security clearance will be granted as soon as possible. Since security clearance is often required to carry out specific types of work, living with uncertainty about whether one can accept or continue in a position is stressful. For the employer, long case processing times entail a risk of losing much needed labour.

The Committee is therefore concerned with overseeing that security clearance cases are dealt with in a manner that safeguards due process protection and within a reasonable time.

There may be acceptable reasons for long case processing times, for example the need to ensure that the case has been sufficiently elucidated. However, a large proportion of the security clearance authorities' cases are 'in the queue' without anyone actively working on them. The Committee is particularly concerned with ensuring that cases are not left for longer than necessary before being considered.

Below is a table of case processing times for 2022 as provided by NSM: [20]

CASE PROCESSING TIME NSM 2022	Average case processing time overall	Average case processing time, positive decisions[21]	Average case processing time, negative decisions
Request for access to information	70 days (8 cases)[22]		
Request for security clearance	100 days (164 cases)[23]	94 days (156 cases)	463 days (2 cases)
First-tier appeals	306 days (4 cases)[24]	No cases	335 days (3 cases)
Second-tier appeals	477 days (46 cases)[25]	582 days (3 cases)	457 days (33 cases)

19 This follows from the Public Administration Act Section 11 a, which applies in security clearance cases unless otherwise stated.

20 The statistics are based on the date on which the request was received by the security clearance authority.

21 Appeals granted in part are included under 'positive decisions'.

22 NSM also processed one complaint regarding access to information where the directorate was the appeal body. The case processing time was 12 days for that case.

23 This includes dismissed cases.

24 This includes one dismissed case.

25 This includes cases that have been dropped, rejected, revoked, returned and one case where the complaint led to a change to the complainant's disadvantage.

In its annual report for 2021, the Committee expressed concern that case processing times have increased in nearly all areas compared with 2020. In its Recommendation to the Storting[26] concerning the EOS Committee's annual report, the Standing Committee on Scrutiny and Constitutional Affairs expressed an expectation that NSM will 'take steps to reduce case processing times'.

NSM's case processing times have nonetheless increased from 2021 to 2022, both for security clearance cases and even more for complaint cases considered by NSM as the appellate body.

Pursuant to the Oversight Act Section 14 fifth paragraph, the Committee can bring matters the Ministry should be informed of to its attention. In a letter to the Ministry of Justice and Public Security dated 3 February 2023, the Committee stated that the increase in case processing times in security clearance cases gives cause for concern.

6.3 Complaint cases

The Committee has accepted 16 complaints against NSM in 2022, compared with 9 complaints in 2021. Some of these complaints were also against more than one of the services.

The complaint cases concerned both surveillance and security clearance issues. The Committee concluded 13 complaint cases in 2022. Five of the cases resulted in criticism against NSM. All of the cases that resulted in criticism concerned long case processing times in security clearance cases.

In three of the complaint cases, about a year elapsed without NSM taking any case processing steps. In the fourth case, NSM took eighteen months to consider a security clearance case as the appellate body.

In the fifth case, NSM was criticised for its long case processing time both in the part of the case that concerned access to information and in the actual security clearance case. It took NSM more than five months to process the complaint concerning access to information, and seven months elapsed from NSM received the complaint case before any case processing steps were taken in the actual security clearance case.

In two of the complaints where NSM was criticised for its case processing time as an appellate body, criticism was also levelled against the Norwegian Civil Security Clearance Authority (SKM) and the Norwegian Defence Security Department (FSA), respectively, for long case processing times in their initial decisions.

26 Recommendation No 432 to the Storting (2021–2022).

7.

The Norwegian Defence Security Department

Photo: Jonas Selim / Norwegian Armed Forces

7.1 General information about the oversight

The Committee conducted two inspections of the Norwegian Defence Security Department (FSA) in 2022.

In its oversight of FSA, the Committee has focused on the department's operational security activities. Both inspections in 2022 focused on this topic. In 2023, the Committee will inspect FSA's function as a security clearance authority.

7.2 Complaint cases

The Committee has accepted 11 complaints against FSA in 2022, compared with 6 complaint cases in 2021. 8 complaint cases against FSA were concluded in 2022. The complaint cases concerned both surveillance and security clearance issues. Three of the cases resulted in criticism against FSA. All of the cases that resulted in criticism concerned long case processing times in security clearance cases.

In one case, FSA was criticised for letting a complaint case sit unprocessed for more than six months. NSM was also criticised for its case processing time when it considered this complaint as the appellate body.

In the second case, it took FSA nearly a year to complete the processing of a case. The case processing time in the third case was one year and three months.

7.3 Case processing times in security clearance cases

Below is a table of case processing times for 2022 as provided by FSA:[27]

CASE PROCESSING TIME FSA 2022	Average case processing time overall	Average case processing time, positive decisions[28]	Average case processing time, negative decisions
Request for access to information	14 days (14 cases)[29]		
Request for security clearance	41 days (22 392 cases)	38 days (22 134 cases)	268 days (258 cases)[30]
First-tier appeals	130 days (48 cases)	135 days (6 cases)	128 days (42 cases)

The Committee notes that the case processing times for requests for access to information have increased somewhat compared with 2021, while case processing times in complaint cases where FSA makes the initial decision have decreased.

27 The statistics are based on the date on which the request was received by the security clearance authority.

28 Appeals granted in part are included under 'positive decisions'.

29 FSA processed one complaint regarding access to information. The case processing time was 14 days for that case.

30 In 101 of these cases the decision was no clearance, while in the remaining cases, clearance was granted subject to conditions, for a lower level or shorter time than requested, or with a combination of such limitations.

8.

The Norwegian Civil Security Clearance Authority

8.1 General information about the oversight

The Committee carried out one inspection of the Norwegian Civil Security Clearance Authority (SKM) in 2022. The inspection concerned case processing times in security clearance cases and new rules on personal history in such cases, among other things.

A planned inspection of the security clearance authority at the Office of the Prime Minister was cancelled because responsibility for security clearance was transferred to the Norwegian Civil Security Clearance Authority with effect from 15 September 2022.

8.2 Consideration of religious affiliation in security clearance cases

In its oversight of security clearance cases, the Committee pays particular attention to whether the factors that are taken into consideration are relevant and sufficiently elucidated. The Committee has investigated two security clearance cases in which the persons' religious affiliation was considered by the security clearance authority. The Committee found no reason to criticise the fact that the persons were denied security clearance, as other circumstances were decisive to the outcome of these cases.

The Committee remarked that SKM did not appear to have a sufficient basis for its weighting of the persons' religious affiliation. If religious affiliation is to be taken into consideration and importance attached to it, then the security clearance authority should conduct a security interview with the person in question to clarify his/her views on the relationship between religious and legal norms.

8.3 Complaint cases

The Committee has accepted two complaints against SKM in 2022, compared with one complaint case in 2021. Two complaint cases against SKM were concluded in 2022. One of the cases resulted in criticism. SKM was criticised for having taken a total of one year and seven months to consider a security clearance case and make the initial decision in the complaint case. In this complaint case, NSM was also criticised for its case processing time when considering this complaint as the appellate body.

8.4 Case processing times in security clearance cases

Below is a table of case processing times for 2022 as provided by SKM:[31]

CASE PROCESSING TIME SKM 2022	Average case processing time overall	Average case processing time, positive decisions[32]	Average case processing time, negative decisions
Request for access to information[33]	6 days (49 cases)		
Request for security clearance[34]	56 days (6270 cases)	46 days (6011 cases)	284 days (259 cases)
First-tier appeals	160 days (56 cases)	208 days (8 cases)	152 days (48 cases)

SMK's case processing times are largely comparable with 2021.

31 The statistics are based on the date on which the request was received by the security clearance authority.

32 Appeals granted in part are included under 'positive decisions'.

33 Average case processing time for appeal cases concerning access to information was 14 days in 2022.

34 SKM has also provided information about the average case processing time for incoming information in security clearance cases. In 2022, it averaged 136 days.

9.

Oversight of other intelligence and security services

Photo: Synne Nilsson / Norwegian Armed Forces

9.1 General information about the oversight

The Committee oversees intelligence and security services regardless of which part of the public administration the services are carried out by. The oversight area is defined by function rather than being limited to certain organisations.

The Committee has accepted one complaint against other intelligence and security services for consideration in 2022, compared with three complaint cases in 2021. Two complaint cases against other intelligence, surveillance or security services were concluded in 2022, both without criticism.

9.2 The Army Intelligence Battalion

The Committee shall carry out one inspection per year of the Army Intelligence Battalion (Ebn). The topics addressed in the Committee's inspection of the Army Intelligence Battalion at Setermoen in Troms included Ebn's cooperation with the Norwegian Intelligence Service and how Ebn conducts HUMINT exercises and training in Norway.

The inspection did not give grounds for follow-up.

9.3 The Norwegian Special Operation Forces

The Committee shall carry out one inspection per year of the Norwegian Special Operation Forces. In 2022, the Committee inspected the Norwegian Naval Special Operations Commando in Bergen. The topics addressed in the inspection included the cooperation between the Norwegian Naval Special Operations Commando and the Norwegian Intelligence Service and procedures for the storage and deletion of personal data.

The inspection did not give grounds for follow-up.

10.

Appendices

APPENDIX 1 – Consultation submission on proposed amendments to the Oversight Act

EOS-UTVALGET
STORTINGETS KONTROLLUTVALG
FOR ETTERRETNINGS-, OVERVÅKINGS- OG SIKKERHETSTJENESTE

Stortinget
P.O. Box 1700 Sentrum
NO-0026 OSLO

Copy:
Enclosures: 1

8 April 2022

Our ref.: 2021/276-8

Your ref.: 2021/4156

Proposed amendments to the Oversight Act etc. – consultation submission from the EOS Committee

The EOS Committee refers to the letter from the Storting dated 15 March 2022 requesting written consultation submissions concerning amendments to the Oversight Act.

The proposed new Section 18 b of the Oversight Act contains a separate provision on the processing of personal data by the EOS Committee. The Storting refers to the fact that the Oversight Act contains some provisions relating to personal data processing (Section 6 second paragraph, Sections 8 and 16), but nonetheless considers it appropriate to add a general provision. Reference is also made to the fact that there can be no room for doubt about the basis in law for the processing of personal data. A separate legal provision authorising further processing of information received from the intelligence and security services is not deemed necessary.

The provisions of the Oversight Act assume that the Committee may process such personal data as necessary for the performance of its oversight duties. In light of the development of the law, the Committee nevertheless agrees that a provision on the Committee's processing of personal data should be adopted.

The Committee also shares the Storting's view that the Committee's duty of secrecy as set out in the Oversight Act Section 11 first paragraph fulfils the need for exemption from the General Data Protection Regulation Articles 13, 14 and 15, cf. the Personal Data Act Section 16 letter d.

The consultation bodies are asked to consider 'whether further statutory exemptions are needed from Articles 5, 12, 16–22 or 34 based on the special considerations that apply to the Committee's work'.

In the Committee's view, exemptions should be made from the above-mentioned articles, given the Committee's wide-ranging right of access to classified information and general duty of secrecy. The Committee will regularly process personal data concerning persons who can never be informed that the Committee has done so, both in connection with inspections, complaint cases and in connection with matters raised on the Committee's own initiative.

The EOS Committee awaits a more detailed evaluation of the need for exemption from individual articles and, if relevant, a proposal for statutory regulation. The Committee's secretariat is at the Storting's disposal should it wish to engage in a more detailed dialogue on the form of the regulatory framework.

POSTAL ADDRESS: P.O. Box 84 Sentrum, NO-0101 OSLO
OFFICE ADDRESS: Nils Hansens vei 25
TEL.: (+47) 23310930
EMAIL: post@eos-utvalget.no
WEBSITE: www.eos-utvalget.no

Our ref.: 2021/276

The EOS Committee does not consider it expedient to include a provision in the Oversight Act stating that requests from registered persons for a copy of personal data being processed by the public administration are to be addressed to the public administration, cf. the General Data Protection Regulation Article 15(3). Reference is made to the grounds set out by the Storting in the consultation paper.

The EOS Committee has no comments on the other proposed amendments to the Oversight Act.

Yours faithfully,

Astri Aas-Hansen
Chair of the EOS Committee

APPENDIX 2 – Consultation submission on proposed amendments to the Intelligence Service Act

The Ministry of Defence
P.O. Box 8126 Dep.
NO-0032 OSLO

26 September 2022

Our ref.: 2022/414-9 Your ref.: 2016/2773-185/FD II 6/SIH

Consultation submission from the EOS Committee – Proposed amendments to the Intelligence Service Act

1. Introduction

The EOS Committee refers to the Ministry of Defence's consultation letter of 27 June 2022 on amendments to the Intelligence Service Act. The deadline for consultation submissions is set to 27 September 2022.

The proposed amendments will have a bearing on the EOS Committee's oversight activities and thus give grounds for some comments on our part.

The Committee notes that the background for this proposal includes judgments from the European Court of Justice and the Court of Justice of the European Union regarding requirements set out in the European Convention on Human Rights (ECHR) and in EU law concerning national bulk collection regimes. The proposed legislative amendments aim to guarantee and clarify Norway's compliance with ECHR and EEA law. This is also important in relation to the EOS Committee's oversight, whose purpose includes ensuring 'that the services respect human rights' (the Oversight Act Section 2).

The proposed amendment to Section 7-3 of the Intelligence Service Act entails dividing the power to make facilitation requirements of electronic communication providers that is currently vested in the Director of the Norwegian Intelligence Service. Decisions to require mirroring of communication streams to allow for searches and collection pursuant to Sections 7-8 and 7-9 shall be made by a district court (proposed new Section 7-3 second paragraph). However, the Director of the Norwegian Intelligence Service will have the power to make decisions regarding mirroring of communication streams exclusively for testing and analysis purposes pursuant to Section 7-5 and Section 7-7 fourth paragraph with a view to ascertaining whether there are grounds to file a petition for such permission from the court (proposed new Section 7-3 first paragraph).

As the Committee understands the purpose of the proposed new Section 7-3 first paragraph, the Norwegian Intelligence Service is to be allowed to assess and state factual grounds for which communication carriers that are assumed to transport communication of the greatest possible intelligence relevance, and then petition the court for permission pursuant to the

POSTAL ADDRESS: P.O. Box 84 Sentrum, NO-0101 OSLO
OFFICE ADDRESS: Nils Hansens vei 25
TEL.: (+47) 23310930
EMAIL: post@eos-utvalget.no
WEBSITE: www.eos-utvalget.no

second paragraph. Information mirrored pursuant to the proposed new Section 7-3 first paragraph cannot be used for intelligence production purposes.[1]

In the Committee's opinion, there are two main reasons why the reference to Section 7-5 and Section 7-7 fourth paragraph results in ambiguity. Firstly, the proposed new Section 7-3 first paragraph concerns another, and new, purpose compared with Section 7-5 and Section 7-7 fourth paragraph. It is therefore unclear whether test collection and test analyses under Section 7-5 can be used for the purpose stated in the proposed new Section 7-3.

Secondly, personal data legislation shall limit the scope of the collection, the processing of data and the period for which data can be stored to what is necessary for the purposes for which they are collected. Such requirements are set out in Section 7-5 for data for test purposes, and in Section 7-7 ff. for metadata and content data for intelligence production, as well as in Chapter 9. The Committee would like to see a corresponding clarification of which requirements of this kind will apply to data collected pursuant to the proposed new Section 7-3 first paragraph.

To clarify which rules apply to the processing of information obtained pursuant to the proposed new Section 7- 3 first paragraph, it should, in the Committee's view, be considered whether it is necessary to regulate this in a separate provision, where the purpose of the proposed new Section 7-3 is decisive for the drafting of the pertaining rules for processing. As Section 7-5 and Section 7-7 fourth paragraph pursue other purposes, they should not necessarily apply correspondingly.

2. Can testing and analysis pursuant to Section 7-5 be used for the purpose stated in the proposed new Section 7-3?

For the purpose stated in the proposed new Section 7-3 first paragraph, the Director of the Norwegian Intelligence Service can make decisions concerning mirroring with a view to test collection and test analysis pursuant to Section 7-5. Section 7-5 only warrants technical support of the facilitated bulk collection system to enable, e.g., the selection of communication carriers. In order to determine whether a communication carrier contains communication of intelligence relevance under the proposed new Section 7-3 first paragraph, and thus forms a basis for a petition to a court under the proposed new Section 7-3 second paragraph, the Committee assumes that the Norwegian Intelligence Service will necessarily have to carry out an assessment that goes beyond purely technical support. It is the Committee's view that even if data mirrored pursuant to the proposed new Section 7-3 first paragraph are not to be used for intelligence production, an intelligence assessment must be carried out in order for the Norwegian Intelligence Service to be able to form a qualified opinion about whether or not a communication carrier contains intelligence-relevant communication. In the Committee's opinion, test collection and analysis pursuant to Section 7-5 will not constitute legal authority for such an intelligence assessment.[2]

This illustrates the underlying shortcoming of the draft bill. The provisions in the current Chapter 7 are primarily regulated for two purposes: test collection and test analysis pursuant to Section 7-5, and intelligence production pursuant to Section 7-7 ff. In the Committee's opinion, the proposed new Section 7-3 first paragraph introduces a third purpose, namely to clarify whether a basis exists for submitting a petition to the courts for the mirroring of communication streams. The ambiguities and delimitation problems described above arise when the existing provisions in Chapter 7 are applied correspondingly for a new purpose that the original provisions were not intended to serve.

[1] Consultation paper page 17.
[2] See Proposition No 80 to the Storting (Bill) (2019–2020), pages 107 and 215.

3. Which processing rules apply to data mirrored for testing and analysis purposes pursuant to Section 7-7 fourth paragraph?

Given that the Ministry chooses to retain the reference to Section 7-5 and Section 7-7 fourth paragraph in the proposed new Section 7-3 first paragraph, it will, particularly as regards testing and analysis pursuant to Section 7-7 fourth paragraph, be impossible for the Committee to exercise real oversight to verify whether the mirrored data are *only* used to determine whether there is a basis for submitting a petition - and not for *intelligence production*.

The reason for this is that Section 7-7 was originally intended to authorise the collection and storage of metadata in bulk for use in intelligence production through searches pursuant to Section 7-8. The Ministry's proposal that the Director of the Norwegian Intelligence Service should be allowed to mirror and store metadata for test and analysis purposes under Section 7-7 fourth paragraph for a purpose other than intelligence production, is not accompanied by any mechanism to keep these data separate from data intended for intelligence production purposes. By comparison, Section 7-5 third paragraph stipulates a requirement that data collected for technical support purposes be stored separately in a short-term storage.

Moreover, Section 7-7 sets no limitations on processing other than a reference to Section 7-5 fifth paragraph. This is also different from to Section 7-5, which contains strict rules for processing. For example, Section 7-5 fourth paragraph stipulates that data may only be stored for 14 days if the information can be linked to individual persons, while metadata mirrored pursuant to the proposed new Section 7-3 first paragraph for testing and analysis pursuant to Section 7-7 fourth paragraph may be stored for 18 months, cf. Section 7-7 third paragraph.

Given that the purpose of the proposed new Section 7-3 first paragraph is to enable the Intelligence Service to provide factual grounds for a petition for mirroring pursuant to the proposed new Section 7-3 second paragraph,[3] the Committee asks the Ministry to consider whether test collection and analysis pursuant to Section 7-7 are necessary to achieve this purpose. In the Committee's view, the purpose of Section 7-7 fourth paragraph is primarily to analyse, troubleshoot and update the metadata store, and not to identify communication streams of that is relevant for intelligence.

If the Director of the Norwegian Intelligence Service is nevertheless given the power to mirror communication streams for testing and analysis purposes under Section 7-7 fourth paragraph, the Committee considers that a duty should also be stipulated to keep these data separate from other metadata collected and stored pursuant to Section 7-7. Rules for data processing should also be stipulated to reduce the risk of errors and misuse. It should particularly be assessed whether a storage period of 18 months is necessary, given that these data are not to be used for retrospective searches for intelligence production purposes.

4. No time limit on mirroring decisions made by the Director of the Norwegian Intelligence Service

The proposed new Section 7-3 first paragraph contains no time limit on the Director of the Norwegian Intelligence Service's decisions regarding mirroring. The wording of the proposed new Section 7-3 fourth paragraph only sets a time limit on mirroring decided by *the courts*.

The European Court of Human Rights and European Court of Justice have both stated that national legislation must set a maximum duration for permissions for bulk collection operations.[4]

[3] Consultation paper page 15.

[4] See, e.g., Centrum för Rättvisa paragraph 331 and La Quadrature du Net paragraph 138.

In the Committee's opinion, this means that an absolute limit must be enshrined in law concerning the duration of a decision by the Director of the Norwegian Intelligence Service's decisions regarding mirroring. Moreover, the mirroring must be discontinued at an earlier date if the fundamental conditions set out in Chapter 5 are no longer met.

5. Ambiguity about the concepts 'intelligence purposes' and 'intelligence production'

The consultation paper[5] states that information mirrored pursuant to the proposed new Section 7-3 first paragraph 'cannot be used for intelligence purposes pursuant to Section 1-3 first paragraph letter (c) of the Act, i.e. in the performance of one of the Norwegian Intelligence Service's tasks under Chapter 3'.

It follows from Section 7-1 first paragraph that one of the fundamental conditions for the Norwegian Intelligence Service's right to engage in facilitated bulk collection is that it is carried out for *intelligence purposes*. This purpose must be fulfilled in all steps of the facilitated bulk collection process.

The designation 'intelligence purposes' refers to the purposes described in Chapter 3 of the Act, cf. Section 1-3 letter (c). The Intelligence Service Act Section 3-5 letter (c) states that to 'conduct technical equipment testing and other training and exercise activity' is an intelligence purpose. It is also clear from Proposition No 80 to the Storting (Bill) (2019–2020) that technical support under Section 7-5 is considered an intelligence purpose, while such test data cannot be used for intelligence production, cf. page 107.

The Committee assumes that it was the Ministry's intention to specify that mirroring for testing and analysis purposes pursuant to the proposed new Section 7-3 first paragraph cannot be used for *intelligence production* under Sections 3-1 to 3-4. In the opposite case – if the mirrored data cannot be used for intelligence purposes – the mirroring will not meet the fundamental condition for intelligence purposes set out in Section 7-1.

6. Ambiguity about whether the proposed new Section 7-3 constitutes legal authority for mirroring for development and maintenance purposes

The proposed new Section 7-3 first paragraph states that testing and analysis pursuant to Section 7-5 and Section 7-7 fourth paragraph can be decided 'with a view to determining whether there are grounds to submit a petition for a court order pursuant to the second paragraph'. The consultation paper[6] states that '[t]he purpose of mirroring is to make it possible to determine whether there are grounds to submit a petition to the court for permission for mirroring as a basis for searches and collection pursuant to Sections 7-8 and 7-9'.

In the Committee's view, it is unclear whether the proposed provision will authorise the Norwegian Intelligence Service to mirror data for the purpose of using them for development, maintenance and updating of the facilitated bulk collection system.

Yours faithfully,

Astri Aas-Hansen
Chair of the EOS Committee

[5] Page 17.
[6] Page 17.

APPENDIX 3 – Meetings, visits, lectures and participation in conferences etc.

- The oversight bodies in the International Oversight Working Group met in March in Bern, Switzerland. The Secretariat represented the Committee. In 2022, two Swedish oversight bodies, the Swedish Commission on Security and Integrity Protection and the Swedish Foreign Intelligence Inspectorate, joined oversight bodies from Norway, Denmark, Switzerland, Belgium, the Netherlands and the UK in this collaboration group.
- In April, the Secretariat visited the Dutch oversight body CTIVD in the Hague to discuss common issues relating to oversight of intelligence and security services.
- One of the committee members gave a lecture at the Nordic Surveillance Control Conference in Oslo in May. The topic at the conference was oversight of interception of communication by the ordinary police.
- One of the committee members gave a lecture at the trade union Parat's security clearance seminar in May.
- The Secretariat visited the Norwegian Anti-Discrimination Tribunal in Bergen in May.
- In June, the committee chair met with Auditor General Karl Eirik Schjøtt-Pedersen.
- In June, the Secretariat attended a workshop on oversight of intelligence services in Berlin. The event was hosted by the think tank Stiftung Neue Verantwortung.
- In September, one of the committee members and two secretariat employees gave a lecture for Oslo District Court in connection with the Norwegian Intelligence Service's introduction of the facilitated bulk collection method and its oversight.
- Two employees from the Canadian oversight body National Security and Intelligence Review Agency (NSIRA) visited Oslo in September to share experience with the Committee's Secretariat. The Secretariat also had several digital meetings with NSIRA in 2022.
- A secretariat employee gave a lecture at an international conference on security clearance oversight in Antwerp in September.
- In October, the committee chair attended the European Intelligence Oversight Conference in London. The conference brought together representatives of oversight bodies from large parts of Europe. The eight countries that take part in the International Oversight Working Group held a meeting before the conference.
- In November, one of the committee members attended the International Intelligence Oversight Forum, which, in 2022 took place in Strasbourg, France. The conference brings together oversight bodies and invited guests from several continents.
- Also in November, the head of the secretariat gave a lecture on democratic oversight of intelligence and security services for students taking the Norwegian Defence University College's course on politics, society and intelligence.

APPENDIX 4 – Letter from the Committee to PST dated 10 October 2022

EOS-UTVALGET
STORTINGETS KONTROLLUTVALG
FOR ETTERRETNINGS-, OVERVÅKINGS- OG SIKKERHETSTJENESTE

Norwegian Police Security Service
Attn. acting director of PST Roger Berg
P.O. Box 4773 Nydalen
NO-0421 OSLO

10 October 2022

Our ref.: 2022/442-6 Your ref.: 22/02097

The legal basis for PST's use of drones

The EOS Committee refers to previous correspondence in the case, most recently PST's reply to the Committee dated 26 August 2022. Based on the service's reply, the Committee's concluding statement in the case is as follows:

The use of mobile and remotely operated cameras (drones) to gather information by recording images and, if relevant, sound, will constitute an interference with privacy. Such use will therefore require a basis in law, cf. the Norwegian Constitution Articles 102 and 113 and the European Convention on Human Rights (ECHR) Article 8. PST has informed the Committee that the service has used drones as a method in four prevention cases. The Committee cannot see that PST has legal authority for such use of drones. The practice is unlawful and should be discontinued with immediate effect.

The Committee wishes to emphasise that PST has an independent responsibility for ensuring that the service has a sufficient basis in law for the methods it uses. The Committee notes that PST has based its practice on the Director General of Public Prosecutions' assessment of the issue in relation to the investigative track. The Director General of Public Prosecutions has not considered the question of legal authority in the preventive track.

Nor has PST assessed the issue in more detail in relation to prevention cases. In its reply, the service states:

> '[T]he underlying legal policy considerations behind the Criminal Procedure Act Section 202 a give no grounds for applying different limitations in investigation and prevention cases. The right to privacy has the same protection against interference whether such interference takes place to prevent a criminal offence or as part of the investigation of a criminal offence...'.

The considerations referred to by PST above are relevant to the question of whether legal authority should be granted, but not sufficient to constitute such authority.

The principle of legality, cf. the Norwegian Constitution Article 113, requires the authorities' interference in relation to individuals to have a basis in law. According to the ECHR Article 8(2), the state may only interfere with the privacy of its citizens if such interference is in accordance with the law and is necessary in a democratic society in the interests of one or more of the purposes listed in the provision. A review of case law from the European Court of Human Rights (ECtHR) shows that this requirement means that the legal authority must be sufficiently clear,

POSTAL ADDRESS: P.O. Box 84 Sentrum, NO-0101 OSLO
OFFICE ADDRESS: Nils Hansens vei 25
TEL.: (+47) 23310930
EMAIL: post@eos-utvalget.no
WEBSITE: www.eos-utvalget.no

predictable and accessible to citizens. The basis in law must also be worded in such a manner that it offers satisfactory due process guarantees.[1]

The Ministry has deemed covert video surveillance using a fixed camera to constitute an interference that requires a basis in law, cf. Proposition No 68 to the Storting (Bill) (2015–2016). This in itself indicates that PST should have carried out a corresponding assessment of covert video surveillance using drones.

The use of drones in the investigative track also requires a clear legal authority. The Committee will not go into this in more detail, cf. the Oversight Act Section 1 second paragraph.

The Committee wishes to emphasise that there is in any case a difference between the two tracks. Investigation and prevention cases have different starting points and goals, as well as different legal provisions governing the use of coercive measures. This is also explicitly referred to in the legal provisions on the use of coercive measures set out in the Criminal Procedure Act Section 202 a and the Police Act Section 17 d. A review of the preparatory works[2] to the Police Act and the Criminal Procedure Act shows that the Ministry and the Storting have both been aware of the matters of principle and particularly problematic aspects of allowing coercive measures to be used in preventive work.

***

- *The EOS Committee strongly criticises PST for having initiated the use of covert methods without legal authority in four cases.*

- *The EOS Committee urges the service to stop its use of covert video surveillance using drones in prevention cases, cf. the Oversight Act Section 14 final paragraph.*

The Committee requests a reply on any measures taken as soon as possible and no later than by **1 November 2022,** cf. the Oversight Act Section 14.

The Committee also requests that the reply include PST's views concerning whether persons who have been subjected to surveillance on unlawful grounds should be informed, and, if so, whether deletion of the information collected should be delayed until the consideration of any legal claims made against the service has been concluded. In this connection, the Committee makes reference to the requirement for effective remedy in ECHR Article 13.

Yours faithfully,

Astri Aas-Hansen
Chair of the EOS Committee

[1] See, inter alia, Proposition No 64 to the Odelsting (1998–1999) section 4.2, Official Norwegian Report NOU 2004:6 section 7.2.3.2, Proposition No 60 to the Odelsting (2004–2005) section 3.3, Official Norwegian Report NOU 2009:15 section 6.3, Proposition No 68 to the Storting (Bill) (2015–2016) section 12.3.In ECtHR case law, see in particular *P.G and J.H. v. the United Kingdom* , *Kopp v. Switzerland, Klass and Others v. Germany, Silver and others v. the United Kingdom.* With respect to the requirement for legal authority, see *Vavřička and Others v. the Czech Republic* and *Klaus Müller v. Germany*. With respect to requirements regarding the quality of the law, see, inter alia, *Weber and Saravia v. Germany, Big Brother Watch and Others v. the United Kingdom.* With respect to requirements regarding due process guarantees, see *Bykov v. Russia, Vig v. Hungary* and *Söderman v. Sweden.*

[2] See, inter alia, Official Norwegian Reports NOU 1997:15 section 2.1, NOU 1998:4 section 10.3.3, NOU 2004:6 section 10.3 (in particular sections 10.3.2.3, 10.3.2.4, 10.3.3.2), Proposition No 60 to the Storting (2004–2005) comments on Section 17 d, Recommendation No 113 to the Odelsting (2004–2005) section 9.2, Recommendation No 343 to the Storting (Bill) (2015–2016) Tvangsmiddelbruk i avvergende og forebyggende øyemed ('Use of coercive measures for averting and preventive purposes' – in Norwegian only).

APPENDIX 5 – Act relating to Oversight of Intelligence, Surveillance and Security Services[35]

Section 1. The oversight area

The Storting shall elect a committee for the oversight of intelligence, surveillance and security services (the services) carried out by, under the control of or on the authority of the public administration (the EOS Committee). The oversight is carried out within the framework of Sections 5, 6 and 7.

Such oversight shall not apply to any superior prosecuting authority.

The Freedom of Information Act and the Public Administration Act, with the exception of the provisions concerning disqualification, shall not apply to the activities of the Committee.

The Storting may adopt provisions concerning the Committee's activities within the scope of this Act.

The Committee exercises its mandate independently, outside the direct control of the Storting, but within the framework of this Act. The Storting in plenary session may, however, order the Committee to undertake specified investigations within the oversight mandate of the Committee, and observing the rules and framework which otherwise govern the Committee's activities.

Section 2. Purpose

The purpose of the Committee's oversight is:

1. to ascertain whether the rights of any person are violated and to prevent such violations, and to ensure that the means of intervention employed do not exceed those required under the circumstances, and that the services respect human rights.
2. to ensure that the activities do not unduly harm the interests of society.
3. to ensure that the activities are kept within the framework of statute law, administrative or military directives and non-statutory law.

The Committee shall show consideration for national security and relations with foreign powers. The oversight activities should be exercised so that they pose the least possible disadvantage for the ongoing activities of the services.

The purpose is purely to oversee. The Committee shall adhere to the principle of subsequent oversight. The Committee may not instruct the bodies it oversees or be used by them for consultations. The Committee may, however, demand access to and make statements about ongoing cases.

Section 3. The composition of the Committee

The Committee shall have seven members including the chair and deputy chair, all elected by the Storting, on the recommendation of the Presidium of the Storting, for a period of no more than four years. Members may be re-appointed once and may hold office for a maximum of eight years. Steps should be taken to avoid replacing more than four members at a time. Persons who have previously functioned in the services may not be elected as members of the Committee.

Remuneration to the Committee's members shall be determined by the Presidium of the Storting.

Section 4. The Committee's secretariat

The Committee's secretariat shall be appointed by the Committee. The head of the Committee's secretariat shall be appointed by the Committee for a period of six years following external announcement of the position. The person appointed to the position may be re-appointed once for a further period of six years following a new announcement of the position.

More detailed rules concerning the appointment procedure and the right to delegate the Committee's authority will be stipulated in personnel regulations adopted by the Committee. The Presidium of the Storting may revise the personnel regulations.

Section 5. The responsibilities of the Committee

The Committee shall oversee and conduct regular inspections of the practice of intelligence, surveillance and security services in public and military administration pursuant to Sections 6 and 7.

The Committee receives complaints from individuals and organisations. On receipt of a complaint, the Committee shall decide whether the complaint gives grounds for action and, if so, conduct such investigations as are appropriate in relation to the complaint.

The Committee shall on its own initiative deal with all matters and cases that it finds appropriate to its purpose, and particularly matters that have been subject to public criticism. Factors shall here be understood to include regulations, directives and established practice.

When this serves the clarification of matters or factors that the Committee investigates by virtue of its mandate, the Committee's investigations may exceed the framework defined in Section 1, first subsection, cf. Section 5.

The oversight activities do not include activities which concern persons or organisations not domiciled in Norway, or foreigners whose stay in Norway is in the service of a foreign

35 The act was last changed on January 1st 2023.

state. The Committee can, however, exercise oversight in cases as mentioned in the first sentence when special reasons so indicate.

The ministry appointed by the King can, in times of crisis and war, suspend the oversight activities in whole or in part until the Storting decides otherwise. The Storting shall be notified of such suspension immediately.

Section 6. The Committee's oversight

The Committee shall oversee the services in accordance with the purpose set out in Section 2 of this Act.

The oversight shall cover the services' technical activities, including surveillance and collection of information and processing of personal data.

The Committee shall ensure that the cooperation and exchange of information between the services and with domestic and foreign collaborative partners is kept within the framework of service needs and the applicable regulations.

The Committee shall:

1. for the Police Security Service: ensure that activities are carried out within the framework of the service's established responsibilities and oversee the service's handling of prevention cases and investigations, its use of covert coercive measures and other covert information collection methods.
2. for the Norwegian Intelligence Service: ensure that activities are carried out within the framework of the service's established responsibilities.
3. for the National Security Authority: ensure that activities are carried out within the framework of the service's established responsibilities, oversee clearance matters in relation to persons and enterprises for which clearance has been denied, revoked, reduced or suspended by the clearance authorities.
4. for the Norwegian Defence Security Department: oversee that the department's exercise of personnel security clearance activities and other security clearance activities are kept within the framework of laws and regulations and the department's established responsibilities, and also ensure that no one's rights are violated.

The oversight shall involve accounts of current activities and such inspection as is found necessary.

Section 7. Inspections

Inspection activities shall take place in accordance with the purpose set out in Section 2 of this Act.

Inspections shall be conducted as necessary and, as a minimum, involve:

1. several inspections per year of the Norwegian Intelligence Service's headquarters.
2. several inspections per year of the National Security Authority.
3. several inspections per year of the Central Unit of the Police Security Service.
4. several inspections per year of the Norwegian Defence Security Department.
5. one inspection per year of The Army intelligence battalion.
6. one inspection per year of the Norwegian Special Operation Forces.
7. one inspection per year of the PST entities in at least two police districts and of at least one Norwegian Intelligence Service unit or the intelligence/security services at a military staff/unit.
8. inspections on its own initiative of the remainder of the police force and other bodies or institutions that assist the Police Security Service.
9. other inspections as indicated by the purpose of the Act.

Section 8. Right of inspection, etc.

In pursuing its duties, the Committee may demand access to the administration's archives and registers, premises, installations and facilities of all kinds. Establishments, etc. that are more than 50 per cent publicly owned shall be subject to the same right of inspection. The Committee's right of inspection and access pursuant to the first sentence shall apply correspondingly in relation to enterprises that assist in the performance of intelligence, surveillance, and security services.

All employees of the administration shall on request procure all materials, equipment, etc. that may have significance for effectuation of the inspection. Other persons shall have the same duty with regard to materials, equipment, etc. that they have received from public bodies.

The Committee shall not seek more extensive access to classified information than warranted by its oversight purposes. Insofar as possible, the Committee shall show consideration for the protection of sources and safeguarding of information received from abroad.

The decisions of the Committee concerning what it shall seek access to and concerning the scope and extent of the oversight shall be binding on the administration. The responsible personnel at the service location concerned may demand that a reasoned protest against such decisions be recorded in the minutes. The head of the respective service and the Chief of Defence may submit protests following such decisions. Protests as mentioned here shall be included in or enclosed with the Committee's annual report.

Information received shall not be communicated to other authorised personnel or to other public bodies, which are not already privy to them unless there is an official need for this, and it is necessary as a result of the oversight purposes or results from case processing provisions in Section 12. If in doubt, the provider of the information should be consulted.

Section 9. Statements, obligation to appear, etc.
All persons summoned to appear before the Committee are obliged to do so.

Persons making complaints and other private persons treated as parties to the case may at each stage of the proceedings be assisted by a lawyer or other representative to the extent that this may be done without classified information thereby becoming known to the representative. Employees and former employees of the administration shall have the same right in matters that may result in criticism being levied at them.

All persons who are or have been in the employ of the administration are obliged to give evidence to the Committee concerning all matters experienced in the course of their duties.

An obligatory statement must not be used against any person or be produced in court without his or her consent in criminal proceedings against the person giving such statements.

The Committee may apply for a judicial recording of evidence pursuant to Section 43, second subsection, of the Courts of Justice Act. Sections 22-1 and 22-3 of the Civil Procedure Act shall not apply. Court hearings shall be held in camera and the proceedings shall be kept secret. The proceedings shall be kept secret until the Committee or the competent ministry decides otherwise, cf. Sections 11 and 16.

Section 10. Ministers and ministries
The provisions laid down in Sections 8 and 9 do not apply to Ministers, ministries, or their civil servants and senior officials, except in connection with the clearance and authorisation of persons and enterprises for handling classified information.

The Committee cannot demand access to the ministries' internal documents.

Should the EOS Committee desire information or statements from a ministry or its personnel in other cases than those which concern the ministry's handling of clearance and authorisation of persons and enterprises, these shall be obtained in writing from the ministry.

Section 11. Duty of secrecy, etc.
With the exception of matters provided for in Sections 14 to 16, the Committee and its secretariat are bound to observe a duty of secrecy.

The Committee's members and secretariat are bound by regulations concerning the handling of documents, etc. that must be protected for security reasons. They shall have the highest level of security clearance and authorisation, both nationally and according to treaties to which Norway is a signatory. The Storting's administration is the security clearance authority for the Committee's members and secretariat. The Presidium of the Storting is the appellate body for decisions made by the Storting's administration. The authorisation of the Committee's members and secretariat shall have the same scope as the Committee's right of inspection pursuant to Section 8.

Should the Committee be in doubt as to the classification of information in statements or reports, or be of the opinion that certain information should be declassified or given a lower classification, the issue shall be put before the competent agency or ministry. The administration's decision is binding on the Committee.

Section 12. Procedures
Conversations with private individuals shall be in the form of an examination unless they are merely intended to brief the individual. Conversations with administration personnel shall be in the form of an examination when the Committee sees reason for doing so or the civil servant so requests. In cases which may result in criticism being levied at individual civil servants, the examination form should generally be used.

The person who is being examined shall be informed of his or her rights and obligations cf. Section 9. In connection with examinations in cases that may result in criticism being levied at the administration's personnel and former employees, said individuals may also receive the assistance of an elected union representative who has been authorised according to the Security Act with pertinent regulations. The statement shall be read aloud before being approved and signed.

Individuals who may become subject to criticism from the Committee should be notified if they are not already familiar with the case. They are entitled to familiarise themselves with the Committee's unclassified material and with any classified material they are authorised to access, insofar as this does not impede the investigations.

Anyone who submits a statement shall be presented with evidence and claims, which do not correlate with their own evidence and claims, insofar as the evidence and claims are unclassified, or the person has authorised access.

Section 13. Quorum and working procedures
The Committee has a quorum when five members are present.

The Committee shall form a quorum during inspections of the services' headquarters as mentioned in Section 7, but may be represented by a smaller number of members in connection with other inspections or inspections of local units. At least two committee members must be present at all inspections.

In connection with particularly extensive investigations, the procurement of statements, inspections of premises, etc. may be carried out by the secretariat and one or more members. The same applies in cases where such procurement by the full Committee would require excessive work or expense. In connection with examinations as mentioned in this Section, the Committee may engage assistance.

Section 14. On the oversight and statements in general

The EOS Committee is entitled to express its opinion on matters within the oversight area.

The Committee may call attention to errors that have been committed or negligence that has been shown in the public administration. If the Committee concludes that a decision must be considered invalid or clearly unreasonable or that it clearly conflicts with good administrative practice, it may express this opinion. If the Committee believes that there is reasonable doubt relating to factors of importance in the case, it may make the service concerned aware of this.

If the Committee becomes aware of shortcomings in acts, regulations or administrative practice, it may notify the ministry concerned to this effect. The Committee may also propose improvements in administrative and organisational arrangements and procedures where these can make oversight easier or safeguard against violation of someone's rights.

Before making a statement in cases, which may result in criticism or opinions, directed at the administration, the head of the service in question shall be given the opportunity to make a statement on the issues raised by the case.

Statements to the administration shall be directed to the head of the service or body in question, or to the Chief of Defence or the competent ministry if the statement relates to matters they should be informed of as the commanding and supervisory authorities.

In connection with statements which contain requests to implement measures or make decisions, the recipient shall be asked to report on any measures taken.

Section 15. Statements to complainants and the public administration

Statements to complainants should be as complete as possible without disclosing classified information. Information concerning whether or not a person has been subjected to surveillance activities shall be regarded as classified unless otherwise decided. Statements in response to complaints against the services concerning surveillance activities shall only state whether or not the complaint contained valid grounds for criticism. If the Committee holds the view that a complainant should be given a more detailed explanation, it shall propose this to the service or ministry concerned.

If a complaint contains valid grounds for criticism or other comments, a reasoned statement shall be addressed to the head of the service concerned or to the ministry concerned. Otherwise, statements concerning complaints shall always be sent to the head of the service against which the complaint is made.

Statements to the administration shall be classified according to their contents.

Section 16. Information to the public

The Committee shall decide the extent to which its unclassified statements or unclassified parts of statements shall be made public.

If it must be assumed that making a statement public will result in the identity of the complainant becoming known, the consent of this person shall first be obtained. When mentioning specific persons, consideration shall be given to protection of privacy, including that of persons not issuing complaints. Civil servants shall not be named or in any other way identified except by approval of the ministry concerned.

In addition, the chair or whoever the Committee authorises can inform the public of whether a case is being investigated and if the processing has been completed, or when it will be completed.

Public access to case documents that are prepared by or for the EOS Committee in cases that the Committee is considering submitting to the Storting as part of the constitutional oversight shall not be granted until the case has been received by the Storting. The EOS Committee will notify the relevant administrative body that the case is of such a nature. If such a case is closed without it being submitted to the Storting, it will be subject to public disclosure when the Committee has notified the relevant administrative body that the case has been closed.

Section 17. Relationship to the Storting

The provision in Section 16, first and second subsections, correspondingly applies to the Committee's notifications and annual reports to the Storting.

Should the Committee find that consideration for the Storting's supervision of the administration dictates that the Storting should familiarise itself with classified information in a case or a matter the Committee has investigated, the Committee must notify the Storting specifically or in the annual report. The same applies to any need for further investigation into matters which the Committee itself cannot pursue further.

The Committee submits annual reports to the Storting about its activities. Reports may also be submitted if matters are uncovered that should be made known to the Storting immediately. Such reports and their annexes shall be unclassified. The annual report shall be submitted by 1 April every year.

The annual report should include:

1. an overview of the composition of the Committee, its meeting activities and expenses.
2. a statement concerning inspections conducted and their results.
3. an overview of complaints by type and service branch, indicating what the complaints resulted in.
4. a statement concerning cases and matters raised on the Committee's own initiative.
5. a statement concerning any measures the Committee has requested be implemented and what these measures led to, cf. Section 14, sixth subsection.
6. a statement concerning any protests pursuant to Section 8 fourth subsection.

7. a statement concerning any cases or matters which should be put before the Storting.
8. the Committee's general experience from the oversight activities and the regulations and any need for changes.

Section 18. Procedure regulations

The secretariat keeps a case journal and minute book. Decisions and dissenting opinions shall appear from the minute book.

Statements and notes, which appear or are entered in the minutes during oversight activities are not considered to have been submitted by the Committee unless communicated in writing.

Section 18 a. Relationship to the Security Act

The Security Act applies to the EOS Committee with the exemptions and specifications that follow from the present Act, cf. the Security Act Section 1-4 first paragraph.

The following provisions of the Security Act do not apply to the EOS Committee: Sections 1-3, 2-1, 2-2 and 2-5, Chapter 3, Section 5-5, Section 7-1 second to sixth paragraphs, Section 8-3 first paragraph second sentence, Section 9-4 second to fifth paragraphs, Chapter 10 and Sections 11-1, 11-2 and 11-3.

Within its area of responsibility, the EOS Committee shall designate, classify and maintain an overview of critical national objects and infrastructure and report it to the National Security Authority, together with a specification of the classification category, cf. the Security Act Section 7-1 second paragraph.

Within its area of responsibility, the EOS Committee may decide that access clearance is required for access to all or parts of critical national objects or infrastructure and decide that persons holding a particular level of security clearance shall also be cleared for access to a specified critical national object or specified critical national infrastructure, cf. the Security Act Section 8-3.

The Storting may decide to what extent regulations adopted pursuant to the Security Act shall apply to the EOS Committee.

Section 18 b. The Committee's processing of personal data

The Committee and its secretariat may process personal data, including such personal data as mentioned in the General Data Protection Regulation Articles 9 and 10, when necessary for the performance of a task pursuant to this Act.

The rights mentioned in the General Data Protection Regulation Article 12–22 and Article 34 shall not apply to the processing of personal data as part of the EOS Committee's oversight activities.

The personal data shall be deleted as soon as they are no longer of supervisory interest, unless the exceptions in the General Data Protection Regulation Article 17(3) are applicable.

Section 19. Assistance etc.

The Committee may engage assistance.

The provisions of the Act shall apply correspondingly to persons who assist the Committee. However, such persons shall only be authorised for a level of security classification appropriate to the assignment concerned.

Persons who are employed by the services may not be engaged to provide assistance.

Section 20. Financial management, expense reimbursement for persons summoned before the Committee and experts

The Committee is responsible for the financial management of the Committee's activities and shall adopt its own financial management regulations based on the Regulations on Financial Management in Central Government.

Anyone summoned before the Committee is entitled to reimbursement of any travel expenses in accordance with the State travel allowance scale. Loss of income is reimbursed in accordance with Act No 2 of 21 July 1916 on the Remuneration of Witnesses and Experts.

Experts receive remuneration in accordance with the fee regulations. Other rates can be agreed.

Section 21. Penalties

Wilful or grossly negligent infringements of the first and second subsections of Section 8, first and third subsections of Section 9, first and second subsections of Section 11 and the second subsection of Section 19 of this Act shall render a person liable to fines or imprisonment for a term not exceeding one year, unless stricter penal provisions apply.

NORWEGIAN PARLIAMENTARY OVERSIGHT COMMITTEE
ON INTELLIGENCE AND SECURITY SERVICES

fdesign.no

Contact information
Telephone: +47 21 62 39 30
Email: post@eos-utvalget.no

www.eos-utvalget.no