EOS COMMITTEE

THE PARLIAMENT APPOINTED COMMITTEE FOR INTELLIGENCE OVERSIGHT

ANNUAL REPORT 2024

DOCUMENT 7 (2024-2025)

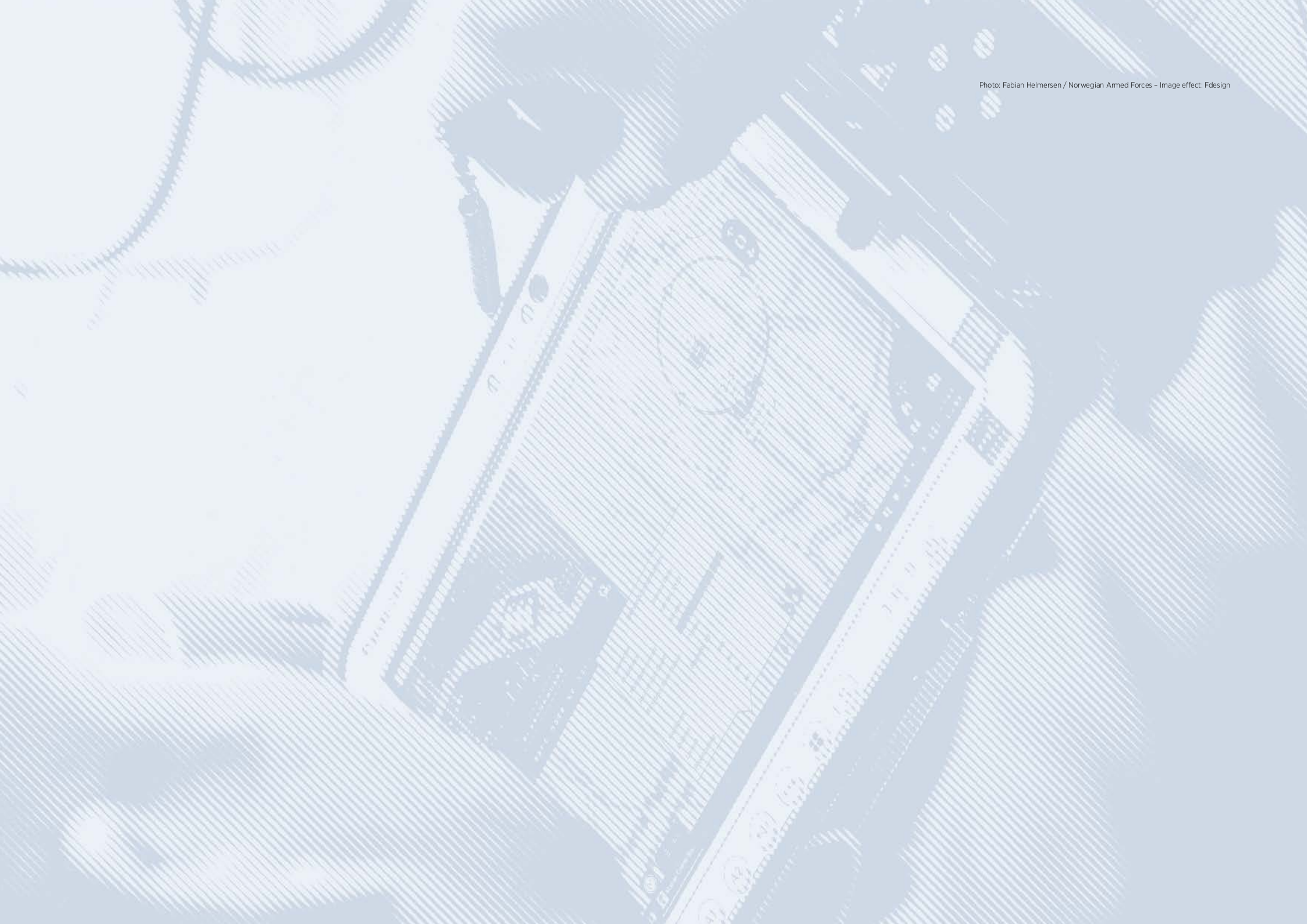


Photo: Fabian Helmersen / Norwegian Armed Forces – Image effect: Fdesign

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 2024 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 or not it is classified. The respective services have been sent text excerpts concerning the service in advance in order to meet this requirement. The services have also been given the opportunity to check for factual errors and misunderstandings in the text.

Submitted to the Storting, 26 March 2025

Grete Faremo

Kristin Krohn Devold | Erling Johannes Husabø | Jan Arild Ellingsen

Olav Lysne | Hege Solbakken | Åsa Elvik

Henrik Gudmestad Magnusson

Photo: Anki Grøthe

The EOS Committee as of 5 February 2025: From left: Åsa Elvik, Olav Lysne, Jan Arild Ellingsen, acting chair Kristin Krohn Devold, Hege Solbakken 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 on the authority of 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 may express its opinion on matters within the oversight area. It shall not seek more extensive access to classified information than warranted by the oversight purposes. The Committee's 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. Ex-post oversight is practised in relation to individual cases and operations. However, 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 but may request the services to implement measures or make decisions. The Committee's remit does not comprise reviewing the services' effectiveness, how they prioritise their resources etc.

The Committee is independent of both the Storting and the Government. The Storting may order the Committee to undertake specified investigations within the oversight remit of the Committee.

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. Members may be re-appointed once. No deputy members are appointed.

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 a NATO-treaty 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 in 2024 and their respective terms of office:

The Committee for the first half of 2024

Astri Aas-Hansen, Asker, chair
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

1 Cf. the Oversight Act Section 1.

Non-statutory law
Non-statutory law is prevailing law that is not enshrined in statute law. It is created through precedent, partially through case law, but also through customary law.

Classified information
Information that shall be protected for security reasons pursuant to the provisions of the Security Act. The information is assigned a security classification – RESTRICTED, CONFIDENTIAL, SECRET or TOP SECRET.

Ex-post oversight
The EOS Committee conducts its review of legality after the services concerned have concluded a case or made a decision.

Security clearance
Decision by a security clearance authority regarding a person's presumed suitability for a specified security classification.

Authorisation
Decision about whether to grant a person with security clearance access to information with a specified security classification.

The Committee for the second half of 2024

Astri Aas-Hansen, Asker, chair
1 July 2019 – 3 February 2025[2]

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

Erling Johannes Husabø, Bergen
1 July 2019 - 30 June 2027

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

Olav Lysne, Bærum
1 July 2021 - 30 June 2025

Hege Solbakken, Bergen
1 July 2024 – 30 June 2027

Åsa Elvik, Bø i Vesterålen
1 July 2024 – 30 June 2027

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.

2 Appointed until 30 June 2027, but left the Committee when she was appointed Minister of Justice and Public Security 4 February 2025

2.

Key figures

The Committee's expenses amounted to NOK 47,760,064 in 2024. The total budget, including transferred funds, has been NOK 49,713,000. The Committee has applied for permission to transfer the unused funds to its budget for 2025. The Committee refers to the administrative annual report published on the EOS Committee's website for further details.

The workload of the chair of the committee corresponds to about 30 per cent of a full-time 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, which at year-end 2024 consisted of 27 full-time employees. The Secretariat consists of the Director of the Secretariat, a legal unit with twelve employees, a technological unit with six employees and an administrative unit with five employees. The departments each have a head of department.

3.

Overview of the Committee's activities in 2024

Photo: Anette Ask / Norwegian Armed Forces – Image effect: Fdesign

3.1 Oversight activities

In 2024, the Committee conducted 21 inspections. Some inspections were directed against several of the services. In 2024, the Committee held eight internal committee meetings, in addition to internal working meetings on site in connection with inspections. During the internal meetings, the Committee discuss inspections, complaints and cases raised on the Committee's own initiative, reports to the Storting and administrative matters.

The Committee raised 24 cases with the services on its own initiative in 2024. It concluded 27 cases raised on its own initiative in 2024.

The Committee considered 29 complaints against the EOS services in 2024. The Committee concluded 30 complaint cases.

3.2 The Committee's oversight methods and statements

A key part of the Committee's activities is to carry out inspections of the EOS services. The Committee's inspections consist of a briefing part and an inspection part. The topics of the briefings are mostly selected by the Committee. The Committee is briefed about the services' ongoing activities, national and international cooperation, the use of methods and the processing of personal data and other topics. 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 they themselves have identified. The Committee asks verbal questions during the briefings and sends written questions afterwards.

During the inspections, the committee members conduct searches directly in the services' electronic systems. The services are not informed about which searches the Committee carries out.

The Committee has a thematic and strategic approach to the oversight. Throughout the year the Committee focused on certain subjects for the oversight of PST, the NIS, FSA and the security clearance authorities. In addition to inspections, the Secretariat conducts regular investigations of the services' data systems. This enables the Committee to conduct more targeted and risk-based inspections.

The Committee raises cases on its own initiative based on findings made during inspections and other investigations. Such cases may also be raised on the basis of information from whistle-blowers or public attention. Documents from the service in question are reviewed in order to shed light on the matter. 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 a statement that may result in criticism or other comments.

On conclusion of the case, the EOS Committee may express its opinion on matters within the oversight area. In its statement, the Committee may criticise the service, for example, if there has been an error or if the Committee believes that a decision must be considered invalid or clearly unreasonable.

If the Committee's investigations result in comments or criticism, the matter is mentioned in the Committee's annual report to the Storting.

3.3 The Committee's consideration of complaints

Complaints from individuals or organisations that fall within the Committee's oversight area are investigated in the relevant service or services. The Committee has a low threshold for considering complaints.

The Committee's statements to complainants should be as complete as possible, but may not contain classified information. Both information that a person is being subjected to surveillance and information that a person is not being subjected to surveillance is classified information.[3] If the Committee's investigation shows that the complainant's rights have been violated, the Committee may inform the complainant that the complaint contained valid grounds for criticism.[4]

If the Committee is of the opinion that a complainant should be given a more detailed explanation, the Committee may 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 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 It follows from Section 15 first paragraph of the Oversight Act that it shall only be stated 'whether or not the complaint contained valid grounds for criticism' in the Committee's statement in surveillance complaint cases.

3.4 Meetings and external activities

In March, the Committee met with members of the Ukrainian parliament, Verkhovna Rada, at the Storting. The committee chair gave a briefing about the EOS Committee's work.

The Committee submitted its annual report for 2023 to the Storting in March 2024. In connection with the submission, the committee chair met with the President of the Storting, and the Committee met with the Standing Committee on Scrutiny and Constitutional Affairs. The Committee hosted its annual conference the following day. The topic of the 2024 conference was 'Surveillance and freedom of speech'. The conference was open to the public and available via streaming.

In September, the Committee met with the German oversight body Parlamentarisches Kontrollgremium (PKGr) in Oslo. PKGr oversees the national intelligence and security services. The meeting included a briefing on the EOS Committee's oversight model and the Committee's work.

The Committee attended the Nordic meeting of the oversight bodies of Norway, Sweden, Denmark and Finland held in Copenhagen in September 2024. The topics discussed included oversight methods and oversight of artificial intelligence.

In October 2024, the Committee undertook a study trip to Canada. The Committee visited the Canadian oversight body, the National Security and Intelligence Review Agency (NSIRA). The programme also included meetings with the National Security and Intelligence Committee of Parliamentarians Secretariat (NSICOP), Global Affairs Canada (GAC) and the Canadian Security Intelligence Service (CSIS). The Committee also visited the Norwegian embassy in Ottawa.

An overview of the Committee's external activities in 2024 is provided in Appendix 1.

3.5 New English name

The EOS Committee has decided to change its English name. The purpose of this change is to emphasise that the Committee is not part of the Storting, but that its members have been a*ppointed by* the Storting. The Committee's new name in English is 'The Parliament Appointed Committee for Intelligence Oversight'.[5]

The theme of EOS Committee's annual conference of 2024 was "Surveillance and freedom of speech". In this photo the columnist Harald Stanghelle, the president of the trade union Tekna, Elisabet Haugsbø, the director of the Norwegian Human Rights Instituion, Adele Matheson Mestad and the former Director of Public Prosecutions, Tor-Aksel Busch are debating. The moderator Trude Teige stands on the right.
Photo: The EOS Committee

5 The previous English name was 'the Norwegian Parliamentary Oversight Committee on Intelligence and Security Services'. The short form of the name remains 'the EOS Committee'.

The Committee's inspections in 2024

Oslo
The NIS, PST, FSA, The PNR-unit of Kripos

Fornebu
NSM

Bergen
PST

Trondheim
PST

Setermoen
The Army Intelligence Battalion

Rena
The Norwegian Special Operations Commando

Moss
The Civil Security Clearance Authority

Reitan in Bodø
The Norwegian Armed Forces' Joint Headquarters and the NIS

4.

The Norwegian Intelligence Service

Norway's foreign intelligence service

Photo: The Norwegian Intelligence Service – Image effect: Fdesign

4.1 General information about the oversight

The Committee conducted four inspections of the Norwegian Intelligence Service (NIS) headquarters in 2024. The oversight activities focused on the NIS's international cooperation. The Committee has also inspected the Armed Forces' telecommunications test field (FTTF). The test field is built like a small-scale commercial telecommunications network where testing and training for various missions can take place. During its 2024 inspection of the Norwegian Armed Forces' Joint Headquarters (NJHQ)[6] the Committee also inspected the NIS's part of the headquarters.

The Committee also inspected the National Intelligence and Security Centre (NESS), which is an analysis centre operated in collaboration between the NIS, PST, NSM and the Norwegian police, represented by the National Bureau of Crime Investigation (Kripos).

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

- the use of collection methods that could entail interference in relation to individuals
- processing of personal data
- the exchange of information with foreign and domestic partners
- cases that have been submitted to the Ministry of Defence[7]
- internal approval cases
- facilitated bulk collection of transboundary electronic communication
- whether the NIS's stations, equipment, methods and collection of information are subject to national control.

The Committee's right of access does not extend to the NIS's particularly sensitive information. The Committee receives regular updates on 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.

4.2 Special report to the Storting on the Norwegian Intelligence Service's role in the 25 June case

On 30 January 2024, the EOS Committee submitted a special report to the Storting on the Intelligence Service's role in connection with the 25 June attack in Oslo.[8] The Committee investigated whether the Intelligence Service provoked the shooting on 25 June 2022 through its handling of sources, and whether the service fulfilled its duty to share all relevant information with the PST without undue delay before the attack.

After investigating the matter, the Committee found no grounds for criticising the NIS.

4.3 Facilitated bulk collection

The EOS Committee is charged with continuously overseeing the NIS's compliance with the provisions on facilitated bulk collection of transboundary electronic communication.

Amendments to the Intelligence Service Act's chapters on facilitated bulk collection entered into force on 1 October 2023. Following these amendments, the NIS can use the facilitated bulk collection method for intelligence production.

In 2024, the Committee checked whether the NIS's use of real data and the service's testing and development of facilitated bulk collection have been carried out within the framework of

6 See section 9.4.

7 See Act No 77 of 19 June 2020 relating to the Norwegian Intelligence Service (the Intelligence Service Act) Section 2-5.

8 Document 7:1 (2023–2024) Special report to the Storting on the Norwegian Intelligence Service's role in the June 25 case.

Internal approval
A decision made at the responsible level of the NIS in cases where such a decision is a regulatory requirement. 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.

Particularly sensitive information
By 'particularly sensitive information', cf. NIS's guidelines for the processing of particularly sensitive information, is meant:

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.

Facilitated bulk collection
Facilitated bulk collection means that the NIS can collect electronic communication transmitted across the Norwegian border through fibre-optic cables.

Intelligence production
Compiling and analysing information collected for intelligence purposes.

the Intelligence Service Act Section 7-3. Among other things, the Committee has examined whether the service has complied with the rules for instructing electronic communication providers to make electronic communication available to the service. The Committee has also checked whether collected data have been used exclusively for the purposes permitted by the regulatory framework. The oversight activities carried out did not give grounds for follow-up in relation to the NIS.

The Intelligence Service Act Section 7-11 requires the NIS to facilitate the Committee's oversight of facilitated bulk collection through technical solutions. In order to carry out its oversight duties, the Committee has requested that the service develop oversight functions in its systems. The Committee followed up the NIS's implementation of such oversight functions in 2024.

The Committee is keeping a close eye on the development of facilitated bulk collection as well as the operational use of the system. The Secretariat's technological and legal expertise, in combination with good oversight mechanisms incorporated into the system, strengthens the Committee's ability to oversee that facilitated bulk collection takes place within the framework of law. This type of oversight is expected to become more extensive in 2025.

4.4 Exchange of metadata with a partner abroad

4.4.1 Introduction

The Committee has considered the NIS's cooperation with a foreign intelligence service on the exchange of metadata in the form of raw data in bulk.

The Committee asked the NIS about the conditions for sharing raw data in bulk set out in the Intelligence Service Act Section 10-3, cf. Section 10-2, as well as the conditions for receiving raw data in bulk collected by another state. The questions included which requirements the NIS must stipulate for its partners' fulfilment of human rights obligations and its requirements concerning reviews of legality by the partner. The Committee requested that the Ministry of Defence give an opinion on some legal aspects based on the answers received from the NIS.

4.4.2 Legal requirements for sharing raw data in bulk with another state

The Intelligence Service Act does not explicitly prohibit or regulate the sharing of raw data in bulk. The Ministry of Defence's view was that the above-mentioned conditions set out in the Intelligence Service Act apply to assessments concerning sharing of raw data in bulk.

According to the Ministry, each bulk data set, or type of data set, must be assessed to determine whether sharing the data set would be proportionate, necessary and justifiable. The nature of the bulk data set will be a crucial factor. If a data set contains personal data, the data are not to be assessed individually. Instead, an overall assessment must be conducted to determine whether sharing the data set as a whole is justifiable. It is not sufficient to simply consider whether the cooperation is proportionate, necessary and justifiable.

The Committee took note of the Ministry's statement.

4.4.3 Legal requirements for receiving raw data in bulk collected by another state

The NIS stated that when receiving information, the service assumes that the relevant partner observes international law and human rights obligations in the performance of its activities. The Ministry supported the NIS's assessment.

In its subsequent statement, the Committee explained in greater detail its understanding of what the legal requirements for receiving information entail.

The Committee referred to the fact that the Intelligence Service Act Chapter 10 primarily regulates disclosure of information to other countries, and not receipt of information by the NIS. It also follows from the Intelligence Service Act Section 1-1 letter (c) that the activities of the NIS are to be conducted 'in accordance with human rights and other fundamental values of a democratic society'. This also agrees with the purpose of the EOS Committee's oversight, described in the Oversight Act Section 2 first paragraph as including to ensure that the services 'respect human rights' and that 'the activities are kept within the framework of statute law [...] and non-statutory law'.

In the Committee's opinion, the general proportionality requirement set out in the Intelligence Service Act Section 5-4 must also apply when receiving information that contains personal data. Regardless of whether the NIS has specifically

Metadata
Data that describe other data or that contain additional information relating to the data, such as the identity of the sender or recipient, or the size, position, time or duration of the communication.

Raw data
Data that are unprocessed or have been automatically processed, and have thus not been analysed or assessed to determine their intelligence value.

Bulk
The collection of large quantities of data where a significant proportion of the information is considered irrelevant for intelligence purposes.

requested the information or receives it as part of an agreed cooperation, the act of receiving it must be deemed to constitute 'collection' in the sense of this provision. The Committee referred to the fact that proportionality is a general principle of Norwegian administrative law, as well as the fact that Article 8 of the European Convention on Human Rights (ECHR) and the Norwegian Constitution Article 102 both set a proportionality requirement for all processing of personal data.

The Committee took guidance from the case law of the Norwegian Supreme Court concerning the use of information collected abroad by means of covert methods when arriving at a more detailed understanding of what these fundamental requirements entail.[9] Applied to the receipt of personal data as part of intelligence activities, it means that the information must have been collected in accordance with the regulations that apply in the country that collects the information. Also, the collection and use of the data must not conflict with fundamental Norwegian values.

The Committee found that the principle that services should not be able to circumvent the requirements set out in Norwegian law with the help of foreign partners must also apply in the field of intelligence. This is also expressed in the Intelligence Service Act Section 10-2 second paragraph and the preparatory works to the Act.[10]

As regards a potential circumvention problem, the Committee pointed out that the Intelligence Service Act Chapters 7 and 8 set out strict requirements concerning facilitated bulk collection of and searches in transboundary electronic communication by the NIS. Among other things, both collection and searches are subject to court authorisation. Let us, as a hypothetical example, assume that the NIS will in practice receive data from facilitated bulk collection if it requests or receives information that a foreign partner has obtained from cables that cross the Norwegian border. In this hypothetical example, the NIS could circumvent the security mechanisms that Norwegian law puts in place. The NIS agrees with the EOS Committee's argument concerning the problem of circumvention.

Receiving personal data, even in the form of bulk data, constitutes interference with the right to respect for private life guaranteed by ECHR Article 8 and the Norwegian Constitution Article 102. A requirement for assessment of proportionality, among other things, is inferred from the conditions for lawful interference stipulated in Article 8 no 2. Such an assessment will have to include an assessment of the guarantees of due process protection at the collection stage. This must also be taken into consideration when applying the Intelligence Service Act Section 5-4.

The European Court of Human Rights (ECtHR) has considered the receiving of personal data, including in bulk, in two Grand Chamber judgments from 2021. [11] This forms part of the legal framework and must be taken into consideration. The Committee referred to the assessments in the Big Brother Watch case paragraphs 495–499, with particular emphasis on the ECtHR's warning that 'the protection afforded by the Convention would be rendered nugatory if States could circumvent their Convention obligations by requesting either the interception of communications by, or the conveyance of intercepted communications from, non-Contracting States'. The same must apply to receiving intelligence information from states that are bound by, but do not comply with, the requirements that now follow from the ECHR.

To summarise, the Committee found that when receiving raw data in bulk, as when receiving other information, the NIS must:

- assess the lawfulness of the collection under the law of the country in question
- assess the proportionality of receiving the information
- ensure that receiving it does not constitute circumvention of the requirements set out in the Intelligence Service Act.

The Committee emphasised that it is primarily up to the NIS and the Ministry to consider the legal situation in other countries in light of the above-mentioned requirements.

4.5 Searches in bulk data for information about a minor

Searches in raw data in bulk, whether for the purpose of target identification or targeted collection, shall not be carried out if it would constitute a disproportionate interference against the individual, cf. the Intelligence Service Act Section 5-3.

9 For example Norwegian Supreme Court ruling HR-2022-1314-A paragraph 26.

10 Proposition No 80 to the Storting (Bill) (2019–2020) section 13.3.4.

11 The ECtHR's Grand Chamber judgments in the cases of *Big Brother Watch and Others versus the United Kingdom* and *Centrum för rättvisa versus Sweden.*

Target identification
Systematic work to identify new intelligence purposes.

Targeted collection
Systematic work to collect information related to identified intelligence targets.

The NIS had conducted a search in bulk data using search terms linked to a minor in Norway. The NIS had not prepared a written proportionality assessment prior to the search. The Committee referred to the fact that it must be possible for the Committee to verify for oversight purposes whether statutory assessments have been carried out. Therefore, the Committee criticised the NIS for not having met the statutory requirement to carry out a proportionality assessment, cf. the Intelligence Service Act Section 5-3 second paragraph second sentence. The Committee specified that the criticism did not mean that the search in itself was disproportionate.

This case also identified some weaknesses in the Committee's possibility to exercise oversight in relation to searches in bulk data. The Committee therefore initiated dialogue with the NIS to improve its possibility to check search logs. The case also raised some questions discussed in section 4.10.

4.6 Use of intrusive methods by the NIS in relation to a potential source in Norway

One case raised questions about how to interpret the Intelligence Service Act Sections 4-2 and 4-5, and about how these provisions relate to each other. Section 4-2 of the Intelligence Service Act regulates the use of collection methods in Norway in relation to foreign persons acting on behalf of a foreign state or state-like actor. Section 4-5 regulates the collection of information about persons in Norway in order to find, recruit and verify sources. One of the key issues in the case was the legal framework for methods used for source verification purposes in relation to foreign persons in Norway acting on behalf of a foreign state etc.

The NIS had initiated an operation in Norway to assess a foreign person's suitability as a potential source. The operation was conducted *exclusively* for the purpose of source verification, and a technical collection method that is not covered by the Intelligence Service Act Sections 6-3 and 6-4 was used in the case.

The Committee questioned the NIS about the relationship between Sections 4-2 and 4-5 of the Intelligence Service Act, as well as about the lawfulness of using such a collection method for source verification. The NIS was of the opinion that the Intelligence Service Act Sections 4-2 and 4-5 constitute two alternative provisions providing exceptions from the territorial prohibition. Therefore, the service considered that Section 4-2 can also provide a legal basis for collecting information about persons for source verification purposes, meaning that all collection methods provided for in the Intelligence Service Act Chapter 6 can be used for source verification in Norway, provided that the potential source falls within the circle of persons specified in Section 4-2 of the Act. In response to a question from the Committee, the Ministry of Defence agreed with the NIS's interpretation.

The Committee did not agree with this interpretation and referred to the purpose and wording of the provisions as well as statements in the preparatory works.

The purpose of using collection methods pursuant to Section 4-2 is to collect intelligence information related to foreign persons and their activities in Norway on behalf of a foreign state. Pursuant to Section 4-5, the purpose of information collection is to determine whether the person in question is in possession of or able to access information of relevance to the NIS or a foreign partner, and to determine their motivation, credibility and suitability as a source.

The wording of the Intelligence Service Act Section 4-5 second paragraph limits how information can be collected for source verification in Norway and which methods can be used for this purpose. Information is to be collected from open sources or through disclosure by Norwegian authorities. If weighty security reasons exist, only methods such as human intelligence and systematic observation can be used, cf. Sections 6-3 and 6-4.[12] The provision does not distinguish between Norwegian and foreign persons in Norway as potential sources. Nor does Section 4-5 stipulate an exception for the circle of persons defined in Section 4-2, as found in the Intelligence Service Act Section 5-3 third paragraph final sentence. The regulation of use of methods to clarify doubts concerning whether a foreign person is acting on behalf of a foreign state also differs between Section 4-2 second paragraph and Section 4-5 second paragraph.

It is stated in the comments to Section 4-5 in Proposition No 80 to the Storting (Bill) (2019–2020) that '[t]here will

12 A 'weighty security reason' could for example be cases where there is reason to investigate whether the source is really acting on behalf of another country's intelligence or security service or is otherwise not who the person pretends to be, cf. Proposition No 80 to the Storting (Bill) (2019–2020) chapter 17 p. 204.

Source verification
A process to collect and assess information to determine whether a potential or existing source is in possession of or able to access information of relevance for intelligence purposes, and to determine their motivation, credibility and suitability.

Territorial prohibition
The NIS is prohibited from using collection methods as described in Chapter 6 of the Intelligence Service Act to target persons in Norway. Intelligence activities targeting foreign persons acting on behalf of a foreign state or state-like actors are exempt from this prohibition.

be no legal basis for using other methods provided for in Chapter 6 unless the source is found to be acting on behalf of a foreign state or state-like actor and information can be collected pursuant to Section 4-2'.

In the opinion of the NIS, the final part of the above quotation supports their interpretation that in cases where the potential source falls within the circle of persons defined in the Intelligence Service Act Section 4-2 first paragraph, the methods used can be based on this provision.

The Committee, however, was of the opinion that, considered in the context of other statements in the preparatory works, the quotation indicates that all methods provided for in Chapter 6 can be used when the service is no longer operating based on source verification purposes, but is collecting information for intelligence purposes. Statements in the preparatory works about why source verification is important support this understanding.[13] The Committee's interpretation of the preparatory works was that it is only once the service has reason to believe that the potential source is really acting on behalf of a foreign intelligence service or is not who they pretend to be, that all collection methods provided for in Chapter 6 can be used. The NIS will then be collecting information for intelligence purposes, and no longer solely for source verification purposes.

The Committee's opinion was that the preparatory works, when read in the context of and seen in conjunction with the structure of the Intelligence Service Act and the wording of the provisions in question, must be understood to mean that Section 4-5 provides exhaustive regulation of use of methods for source verification purposes. The Committee's opinion was, therefore, that methods other than human intelligence or systematic observation could not be used as a lawful collection method for source verification purposes in Norway. The Committee criticised the NIS for having used another method in relation to the potential source.

4.7 The NIS's cooperation with a foreign service

The intelligence service shall be subject to national control, cf. the Intelligence Service Act Section 2-1 second paragraph. The NIS is also charged with ensuring national control over what information is disclosed to foreign partners, cf. the Intelligence Service Act Section 2-1 second paragraph second sentence. The Committee oversees the NIS's important agreements with foreign partners. In 2024, the Committee has examined an agreement that regulates, among other things, the NIS's facilitation of collection by a foreign partner. The Committee asked the NIS to explain how the service ensures that this collection is subject to national control. The Committee also requested an account of measures implemented to prevent the collection of data from Norwegian territory in contravention of the territorial prohibition.

The Committee took note of the account provided by the service. At the same time, the Committee stated that it will continue to oversee how the service ensures national control in its cooperation with other services in future.

Photo: The Norwegian Intelligence Service – Image effect: Fabsign

13 Proposition No 80 to the Storting (Bill) (2019–2020) chapter 8.6.4 page 59.

4.8 Proportionality assessments pursuant to the Intelligence Service Act Section 5-4

The NIS is permitted to use intrusive collection methods in relation to individuals, provided that certain conditions are met. It follows from the Intelligence Service Act Section 6-13 that a decision to use such methods must be made in writing and state, among other things, what or whom the collection concerns. The legal basis for the collection must also be stated.

In Section 4.3 of its annual report for 2023, the Committee discussed a case in which the NIS made a decision to use intrusive methods. On a general basis, the Committee raised the question of whether the service was sufficiently specific when stating what or whom the collection targeted.

In 2024, the Committee has engaged in dialogue with the NIS about matters related to the Intelligence Service Act Section 5-4 to ensure that proportionality assessments are conducted at the correct level.

The NIS deems it sufficient to state which categories of intelligence targets the decision concerns, and considers that a decision can apply to a circle of persons for whom the assessment will be much the same. The Committee expressed understanding of considerations that may necessitate joint assessments for an indeterminate circle of persons. The Committee nevertheless concluded that there was reason to doubt whether the NIS's interpretation of the requirement to specify 'what or whom' a decision applies to was in compliance with the Intelligence Service Act Section 6-13.

The NIS has since received legal clarification from the Ministry of Defence on the matter.

4.9 Bulk purchase of metadata

The annual report for 2022 referred to questions the Committee had asked the NIS about the service's legal basis for purchasing metadata from commercial enterprises. The service did not consider individual procurements of data from commercial providers to 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 this type of metadata procurement.

The Committee disagreed with the NIS and argued that the same considerations apply when purchasing metadata in bulk that contain personal data as for collection from open sources. Collection from open sources is considered use of an intrusive method, cf. the Intelligence Service Act Section 6-2. The Committee was therefore of the opinion that such purchases must be deemed to constitute information collection that could entail interference in relation to individuals, and that the territorial prohibition applies.

The Committee urged the NIS to reconsider whether the use of this method must be based on Chapter 6 of the Intelligence Service Act in order to be lawful.

The NIS reconsidered the matter and forwarded it to the Ministry of Defence. The NIS, with the Ministry's support, now takes the position that, as a rule, purchasing information from commercial enterprises constitutes collection of openly available information pursuant to the Intelligence Service Act Section 6-2. The territorial prohibition therefore applies to such purchases.

4.10 Rules governing searches in raw data in bulk collected from open sources

The basic conditions that apply to collection of and searches in raw data in bulk follow from the Intelligence Service Act Section 5-3. The condition for searches in raw data in bulk using a search term linked to a person located in Norway is that the search must be 'strictly necessary' in order to perform one of the NIS's statutory duties pursuant to Section 3-1 (foreign threats).

In its annual report for 2022, the Committee referred to its consideration on a general basis of whether provisions in the NIS's internal regulations on collection in cyberspace were in compliance with the Intelligence Service Act. A disagreement arose between the NIS and the Committee regarding whether the requirement stipulated in Section 5-3 third paragraph applies when conducting searches in raw data in bulk collected from open sources. The NIS was of the opinion that the legislators' intention and consideration for the context in the Act indicate that the limitation by purpose is not intended to apply to searches in raw data collected from open sources.

The Committee disagreed. In Section 5-3 third paragraph, the legislators imposes more stringent conditions for searches in raw data in bulk if they are based on a search term linked to a person located in Norway. The wording of the provision does not stipulate a distinction based on the method used to collect the raw data. It follows from the structure of the Act that if the service has used one of the methods provided for in Chapter 6 to collect raw data in bulk, then searches conducted in these data must satisfy the conditions set out in Section 5-3 first paragraph. Any exceptions from the requirement of the Act must have a clear legal basis. The Committee stated that the arguments put forward by the NIS were not sufficient to depart from the wording of the Act.

The NIS raised the issue with the Ministry of Defence. The Ministry agreed with the NIS's interpretation. The Ministry

of Defence stated that the stricter conditions stipulated in Section 5-3 third paragraph must be understood to be derived from the general territorial prohibition set out in Section 4-1, and thus not directly applicable to information that has already been lawfully collected and stored in accordance with the Intelligence Service Act Section 6-2, cf. Section 4-4.[14]

The Ministry of Defence's view was that the scope of Section 5-3 third paragraph, as regards the relationship between the conditions for the collection and use of information collected covertly and information collected from open sources, needed to be clarified in the Act. The Ministry referred to the upcoming evaluation of the Intelligence Service Act scheduled to be completed by September 2026.[15]

4.11 Use of urgent decision by the NIS

The Committee asked the NIS to explain an urgent decision made by a person other than the head of the NIS, a decision that had seemingly not been 'finally formalised' until four months later.

The head of the NIS has the power to make decisions to use collection methods provided for in the Intelligence Service Act Chapter 6, cf. Section 6-12. This power cannot be delegated. Decisions must be made in writing and state the mission to which the collection is linked, what or whom the collection concerns, the factual and legal basis for the collection and the duration of the decision, cf. the Intelligence Service Act Section 6-13 first paragraph. In urgent cases a decision under Section 6-12 can be made orally, but it must be put into writing as soon as possible, cf. Section 6-13 second paragraph. It is stated in Chapter 17 of Proposition No 80 to the Storting (Bill) (2019–2020) that the rule permitting urgent decisions is 'intended as a narrow exception that should be exercised with considerable caution'.

The EOS Committee took note of the fact that the person who made the urgent decision had been acting head of the NIS. The Committee remarked that its possibility to exercise subsequent oversight of urgent decisions depends on the service documenting who is authorised to make such decisions in the absence of the head of the NIS.

The Committee also noted that the case involved a considerable extension of the time period for searches in raw data from 7 to 60 days. Such an extension will be a key factor in the assessment of the proportionality of the methods used, particularly considering the effect of the interference for the persons concerned. Therefore, the NIS should have considered the extension of the search period explicitly in its proportionality assessment.

Finally, the Committee noted that, during the service's work in the case, it had identified a non-conformity in that the wrong end date was set for the search. However, no searches were conducted after the search period stated in the decision had expired.

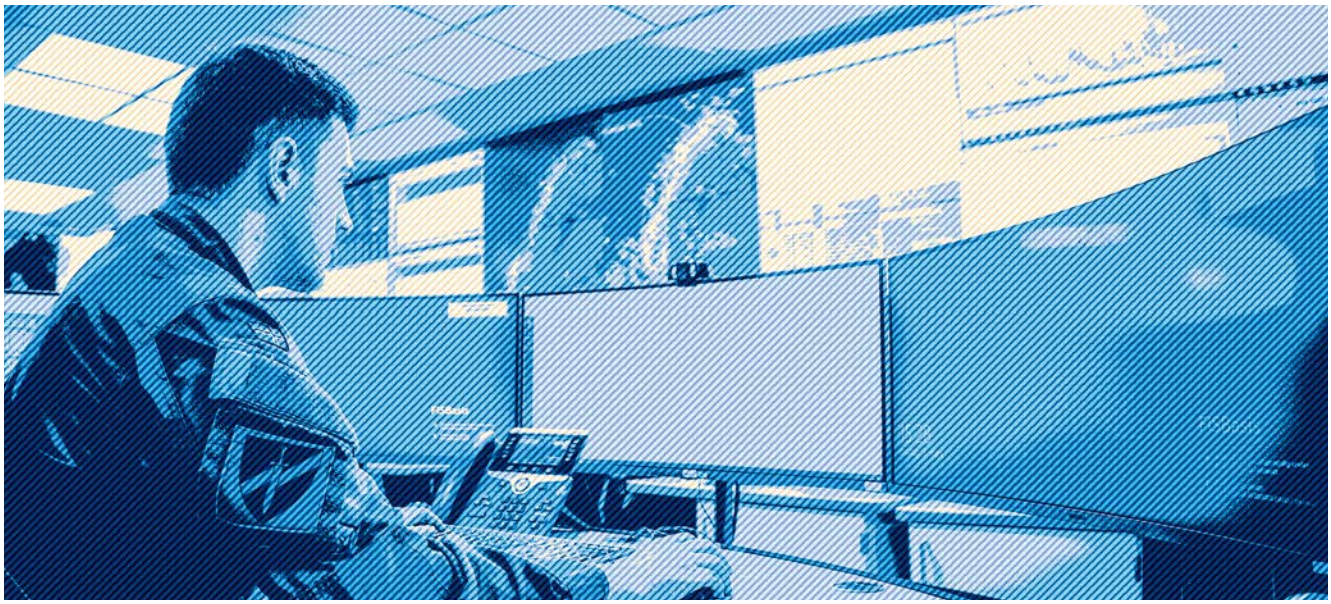


Photo: Anette Ask / Norwegian Armed Forces – Image effect: Fôesign

14 It follows from the Intelligence Service Act Section 4-4 that, notwithstanding the territorial prohibition stipulated in Section 4-1, the NIS may collect information on foreign matters from open sources pursuant to Section 6-2 even if said information has been published by or otherwise relates to persons in Norway.

15 Cf. Minister of Defence Gram's statement in the debate on the Standing Committee on Scrutiny and Constitutional Affairs' recommendation concerning the EOS Committee's annual report for 2023, Recommendation No 341 (Resolution) (2023–2024), cf. Document 7 (2023–2024).

4.12 Whistle-blowing in the NIS and processing of classified information

The Committee received a notification concerning the right and opportunity of NIS employees to report issues of concern in the service in accordance with the Working Environment Act Chapter 2 A. It was claimed that 'sensitivity considerations' and security classification block NIS employees' opportunities to have their notifications considered by parties outside the NIS.

The purpose of the EOS Committee's oversight is, among other things, to prevent the NIS from violating the rights of any persons and to ensure that the service acts within the framework of the law. The Committee has investigated whether the right and opportunity of NIS employees to submit notifications are limited compared to those of other employees of the Norwegian Armed Forces. The investigation also looked into whether the service's procedures for internal whistleblowing limit the employees' rights in contravention of the Working Environment Act Section 2 A-6 subsection 3.

In its concluding statement to the NIS, the Committee remarked that the service's employees appear to have one genuine opportunity for external consideration of their notifications of issues of concern in the service, namely with the Ministry of Defence's Internal Auditor Unit. Other Armed Forces employees appear to have more opportunities for external consideration of their notifications.

The Committee remarked that NIS employees appear to have had more limited opportunities for external consideration of their notifications compared to other Armed Forces employees until 2021. The Committee was informed that in 2021, the Ministry of Defence's Internal Auditor Unit was given 'the authority to consider notifications as well as the competence and authority to consider cases relating [to] whistleblowing in the NIS in individual cases. The Committee noted a statement by the NIS that in such cases, the service would assist the Ministry by providing the necessary information, 'regardless of classification'.

The Committee therefore concluded that no actual limitations are placed on the employees' right and opportunity to have their notifications of issues of concern in the service considered by a competent and independent external body outside the NIS. Nor did the service's procedures for internal whistleblowing limit employees' right and opportunity to submit notifications. The case was concluded without criticism of the NIS.

Finally, the Committee remarked that the NIS's whistleblowing system was not included in PwC's 2022 evaluation of the Armed Forces' whistleblowing system. This evaluation led to the creation of the Armed Forces' central whistleblowing unit. The unit was established to strengthen expertise, capacity and independence in the Armed Forces' handling of whistleblowing.

The central unit is also intended to reduce the risk of differences in the consideration of whistleblowing cases or different principles being applied in dealing with similar whistleblowing cases. The Committee therefore emphasised how important it is that the NIS draws on experience and expertise developed in other parts of the Armed Forces when dealing with internal whistleblowing, with the Ministry of Defence's Internal Auditor Unit as an external notification body, in order to ensure the required expertise and considerations for equal treatment in connection with whistleblowing cases in the service.

4.13 The Anti-Discrimination Tribunal's consideration of cases where the underlying material is classified

A person submitted a complaint to the Anti-Discrimination Tribunal claiming unfair retaliation following whistleblowing in the NIS. The Tribunal dropped the case on the grounds that 'the submitted evidence fails to elucidate the case sufficiently', cf. the Equality and Anti-Discrimination Ombud Act Section 10 third paragraph. The Tribunal referred to the fact that 'a significant proportion of the documents concerning key evidence and reports in the case are classified as CONFIDENTIAL under the Security Act'. A case officer must hold security clearance in order to handle classified documents. The Anti-Discrimination Tribunal stated that none of their case officers have such clearance.

The person concerned contacted the EOS Committee. The Committee stated that if the Anti-Discrimination Tribunal is in practice prevented from considering a case because the underlying material/evidence is classified, there is reason to question whether it is possible for the Tribunal to fully fulfil its mission.

The EOS Committee can notify the relevant ministry of 'shortcomings in acts, regulations or administrative practice', cf. the Oversight Act Section 14 third paragraph. In this case, the Committee notified the Ministry of Labour and Social Inclusion that there appear to be shortcomings in the regulatory framework as regards retaliation cases where the underlying material/evidence is classified.

4.14 Complaint cases

The Committee accepted seven complaints against the NIS for consideration in 2024. Some of these complaints were against more than one of the EOS services. The Committee concluded six complaint cases against the NIS in 2024.

No complaint cases resulted in criticism against the NIS in 2024.

5.

The Norwegian Police Security Service

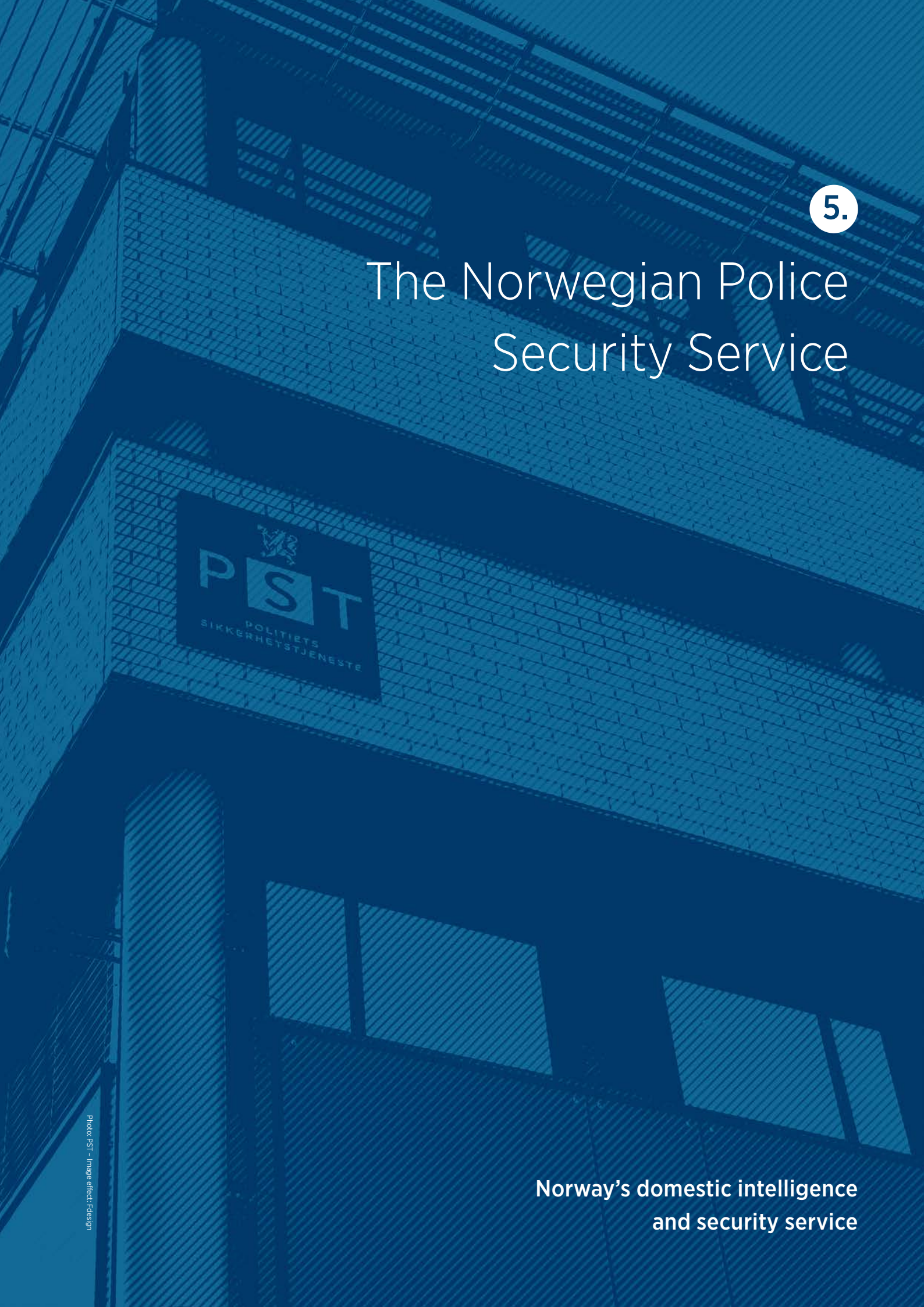


Photo: PST – Image effect: Fdesign

Norway's domestic intelligence and security service

5.1 General information about the oversight

In 2024, the Committee conducted four inspections of the Police Security Service's (PST) Headquarters. The Committee focused on PST's cooperation with Norwegian authorities. The PST entities in Western and Trøndelag police districts were also subject to oversight activities. The Committee also inspected the National Intelligence and Security Centre (NESS), cf. section 4.1.

During its inspections of PST, the Committee focuses on the service's:

- processing of personal data
- new and concluded prevention cases, averting investigation cases and investigation cases
- use of covert coercive measures
- handling of sources
- exchange of information with foreign and domestic partners.

5.2 Human intelligence

The EOS Committee investigated various issues related to PST's use of human intelligence (HUMINT) in 2024.

One of these issues was the service's use of financial compensation. The Intelligence Service Act Section 11-4 exempts compensation paid by the NIS to sources from both tax liability and the duty to provide information. In response to a question from the Committee, PST confirmed that it has not previously been clarified whether financial compensation paid to sources is subject to tax liability and/or a duty to provide information to other public authorities. The matter has been submitted to the relevant ministries, and the Norwegian Tax Act has been amended so that compensation and payments made by PST to sources and contacts in the course of the security service's protected intelligence activities are now defined as tax-exempt income from employment, cf. the Tax Act Section 5-15 subsection 1 letter r.

The Committee also looked into how PST acts when recruiting human intelligence sources and whether the service complies with its internal regulations for source recruitment. The Committee criticised PST for one recruitment process. The service acknowledged significant shortcomings in the source recruitment process in the case in question. The shortcomings related to legal and ethical assessments, risk assessment and the assessment of the relationship with the source's employer, among other things. In addition, no guidance had been provided to the source concerning duty of confidentiality and duty to provide information. PST has taken the issues uncovered seriously and states that the service has drawn valuable lessons from the case.

The Committee has also noted that PST is in dialogue with the Ministry of Justice and Public Security on incorporating special regulation of PST's source register in the Police Databases Regulations.

The Committee's other investigations in the case gave no grounds for further follow-up.

5.3 Review and registration of individuals

5.3.1 Failure to review information about 'positive contacts'

The Committee has previously criticised PST for failing to review information about contacts after five years, cf. the Police Databases Regulations Section 22-3 third paragraph. In its annual report for 2014,[16] the Committee expected PST to also review contacts, including what is known as 'positive contacts', after five years. In the annual report for 2015,[17] the Committee mentioned that PST had changed its practice so that the registration of contacts will also be subject to review after five years.

In response to a question from the Committee in 2023, PST found a non-conformity in the service's technical solution for identifying contacts due for review. Shortcomings were also identified in PST's internal procedures. This resulted in a large number of positive contacts not being reviewed.

16 Section 3.3.1 in the annual report for 2014.

17 Section 4.2.5 in the annual report for 2015.

Prevention case
A case opened for the purpose of investigating whether someone is preparing to commit a criminal offence that PST is tasked with preventing.

Averting investigation case
A case opened for the purpose of averting a criminal offence that falls within PST's area of responsibility.

Investigation case
A case opened for the purpose of investigating a criminal offence that falls within PST's area of responsibility.

Covert coercive measures
Police methods regulated by law that are used without the person targeted being aware of it, such as secret searches, lawful interception, video surveillance and equipment interference.

Positive contact
A person who has provided information to PST by virtue of their occupation or by reporting a matter.

The Committee considered this a major non-conformity and criticised PST both for the non-conformity and for the service's internal procedures not being in accordance with the regulatory framework on this point.

PST has amended its technical solution and will review its internal procedures.

5.3.2 Failure to review the registration of a person

Information registered in the course of PST's preventive activities, except for prevention cases, must be reviewed when five years have passed from the time of registration and no new information has subsequently been registered about the person in question, cf. the Police Databases Regulations Section 22-3 third paragraph first sentence. In 2024, the Committee criticised the service for not having reviewed an object in accordance with the five-year rule.

5.3.3 Continuation for documentation purposes

The Committee asked PST about the basis for keeping an object entry in its register for reasons of documentation. The service agreed with the Committee that documentation purposes alone do not constitute a legal basis for registration under the Police Databases Act, and the entry was deleted.

The Committee stated that the service should go through its system to identify any other object entries kept for more than five years purely for documentation purposes. PST stated that they will comply with the Committee's request.

5.3.4 Registration on grounds of 'special connection with an object of concern'

PST can register persons who have a 'special connection' with an object that PST has concerns about, cf. the Police Databases Regulations Section 21-2 nos 1 and 2. It is a condition that the connection must be assumed to be 'of significance'. The information must also be necessary and relevant for the purpose of the processing.

The Committee looked into an object registration where the object was registered with the above legal basis and criticised PST's basis for processing information about the person in question. The Committee could not see how the registration could be of significance to PST's ability to uncover any terror plans that the principal object might be making. PST had the option of monitoring the situation through surveillance of the principal object. The Committee's view was that since the service had no relevant concerns about the person in question, the registration did not appear to be necessary and proportionate in relation to the purpose of the processing.

Object
An object can be a person or an organisation etc. The object register entry contains identifiers such as personal data and a description of the object's roles.

5.3.5 Lacking basis for processing information

The Committee investigated whether PST could process information about a person's anti-government and conspiratorial statements. PST replied that the service did not have a basis for processing the information. The information was to be deleted, but this was not done. The service later received *new* information about the person in question. It was deemed necessary and relevant to process this new information in order to prevent politically motivated violence. The Committee criticised the service for having processed information about the person in question without a basis in law for four months, but not for the processing that took place after new information was received.

5.4 Registration of persons targeted by foreign intelligence activities

PST's duties include the prevention and investigation of unlawful intelligence activities. Therefore, PST can process information about persons who 'have been or whom there is reason to believe will be targeted by [...] foreign intelligence activities' when doing so is deemed necessary following a concrete assessment.[18]

The Committee has examined the registration of some persons for whom the basis for registration was given as 'targeted by foreign intelligence activities'. Several of them had not been reviewed by the five-year time limit stipulated in the Police Databases Regulation Section 22-3 third paragraph. PST deleted four entries after having reviewed them following the Committee's enquiry.

As regards the legal requirements for registration, the Committee was of the opinion that the key factor is whether a concrete assessment of the circumstances is carried out in each individual case. Not all contact with foreign intelligence should result in registration. Also, consideration for protection of the individual's privacy must be balanced against the service's need to register information. For oversight purposes, it is important that the grounds for registration are documented and described in sufficient detail.

5.5 Covert video surveillance

PST can request court approval for using covert video surveillance for purposes of prevention under the Police Act Section 17 d, cf. the Criminal Procedure Act Section 202 a. PST can only be given permission for covert video surveillance of

Photo: Fabian Helmensen / Norwegian Armed Forces – Image effect: Fotosign

18 The Police Databases Act Section 64 third paragraph letter b, cf. the Police Databases Regulations Section 21-2 first paragraph no 3.

private property 'when special reasons so indicate'.[19]

The Committee regularly requests access to court rulings in cases where PST has received permission for covert video surveillance. The Committee also asks to see images from the surveillance that show the camera view.

In one case, the Committee saw that the camera view covered parts of a social zone for residents and asked PST about this. The Committee remarked that it doubted whether the social zone could be deemed to be covered by the wording of the court's ruling and was of the opinion that PST had not given grounds for its need for surveillance of this zone. The Committee also remarked that if PST submits images to the court when requesting an extension of covert video surveillance, that could give the court a better basis for its decision and eliminate any doubts about what is covered by the court's permission. PST replied to the Committee that it would have been beneficial to give the court more detailed grounds for the necessity and proportionality of including this area.

5.6 Legal basis for processing personal data in police logs

During its work on a complaint case, the Committee asked PST about the legal basis for processing personal data in a police log. In particular, the Committee asked the service to give an account of whether the Police Databases Act Section 64 provides exhaustive regulation of when PST is permitted to process personal data.

The Committee agreed with PST that, pursuant to the Police Databases Act Section 10, the service is in principle obliged to keep a police log. The Committee stated that Section 64 does not limit the basis for processing personal data, but specifies the requirement that information must be necessary to PST's particular duties. It was therefore concluded that PST has legal authority to process personal data in its police log notwithstanding Section 64.

The Committee did not criticise PST, but expressed the opinion that Section 64 is poorly worded, as the provision appears to impose limitations on the processing of personal data for purposes as mentioned in the second and third paragraphs.

The Committee therefore encouraged PST to inform the Ministry of Justice and Public Security about the issue.

5.7 Processing of information in workspaces

PST uses workspaces to process information about national as well as local issues. The workspaces contain information and data deemed to be necessary and relevant to PST's performance of its duties. The case and work logs in the workspaces are to contain documentation of investigations targeting registered individuals. The Committee has looked into PST's processing of personal data in workspaces in two cases.

In one of these cases, the Committee had already asked PST about the processing of information in a workspace as early as in 2014. Information was registered about persons that PST no longer had any concerns about. In 2014, the Committee agreed with PST that it was unfortunate that no changes had been made and expected the service to review the entries to determine whether any could be deleted. During its oversight of PST in 2024, the Committee found that PST had not carried out such a review.

In the other case, the Committee found that personal data about persons not registered as separate objects had been processed in the case and work logs in a workspace. PST stated that the personal data were processed under the four-month rule set out in the Police Databases Act Section 65, but should have been deleted in early 2023.

The Committee stated that information processed under the four-month rule must be processed in such a way that it is assessed before the deadline expires. The Committee criticised PST for not having deleted the information in early 2023. In consequence, the information was processed by PST for over a year without a legal basis.

5.8 Duty to coordinate set out in the Intelligence Service Act Section 4-3

The Intelligence Service Act Section 4-3 imposes on PST and the NIS a duty to coordinate in connection with the NIS's

19 The Police Act Section 17 d second paragraph second sentence.

Workspace
A digital area where PST can process information about a common topic that is not linked to a specific case.

The four-month rule
A time-limited exception from the requirement for information processed by PST to meet the requirements regarding specification of purpose, necessity and relevance. PST can process information for up to four months in order to determine whether the information meets the requirements.

collection activities targeting foreign state activities in Norway under the Intelligence Service Act Section 4-2 first paragraph. If the case concerns a matter that also falls within PST's area of responsibility according to the Police Act Section 17 b first paragraph, the NIS must request PST's consent for collection. PST is to be informed of other collection activities under this provision.

The Committee has previously raised issues related to the duty to coordinate with both services. In 2022, the services drew up a joint policy for consent and information cases.

The Committee has since noted that the services appeared to hold different views regarding whether PST's consent was required in some coordination cases. In a specific case that the Committee raised with PST, the NIS's letter was sent to PST as an information case pursuant to under the Intelligence Service Act Section 4-3 second sentence. PST was of the opinion that collection in the case in question required PST's consent pursuant to Section 4-3 first sentence, meaning that its target also falls within the PST's area of responsibility according to the Police Act Section 17 b.

The Committee asked PST about the case. Based on the response received, the Committee has noted that PST and the NIS practise different interpretations of which matters 'also fall under the description of the Police Security Service's task in Section 17 b subsection 1 of the Police Act', and thus requires the NIS to obtain consent from PST for collection. The Committee has been informed that this has happened in a handful of cases.

The Committee has noted that in practice, PST resolves the problem by treating the NIS's information letters as consent letters when necessary and consenting to collection. In its comments to the preparatory works for the Intelligence Service Act,[20] PST stated that it would only refuse to consent if it was already collecting information about the intelligence target in question and involvement by the NIS could disrupt the operation.

In relation to PST, the Committee referred to the purpose of the duty to coordinate, which is to avoid intelligence failure, ensure operational security and facilitate efficient use of society's resources. It could be unfortunate for the duty to coordinate that views and assessments differ when it comes to which factors determine when the consent of PST is required. The Committee remarked that it does not seem to be a satisfactory long-term solution for PST to handle the issue by treating the NIS's information cases as consent cases.

The Committee remarked that the documents from 2023 does not appear to be enough to fulfil the need for the principles for coordination between the services to be put into writing. The Committee therefore encouraged PST and the NIS to raise the issue with the Ministry of Justice and Public Security as well as the Ministry of Defence for clarification. This suggestion also extended to any other challenges related to coordination, interaction and cooperation between the services.

The Committee has been informed that the services have agreed on a new policy that will clarify matters of principle relating to the issues pointed out by the Committee. PST stated that the relevant ministries will be informed about this policy.

5.9 Sharing of information for analysis by the NIS

According to the Police Act Section 17 f second paragraph letter a, PST can disclose information collected by means of preventive coercive measures to the NIS 'in order to prevent a criminal offence as mentioned in Section 17 b first paragraph'.

The Committee asked PST and the NIS to give an account of PST's sharing of information for analysis by the NIS and the NIS's processing of such information.

Both services agreed that PST can stipulate conditions for the NIS's processing of information disclosed to it by PST. The NIS must observe any limitations that follow from such conditions. The Committee agreed and stated that it is up to PST to consider whether to impose limitations of purpose or other conditions when sharing information.

The Committee pointed out that it is important for the services to have a shared understanding of the conditions PST imposes when disclosing information and what the conditions imposed by PST entails for the NIS's processing of the information. In order to avoid ambiguity, the Committee encouraged PST to stipulate clear conditions for the processing of information when necessary.

The Committee will oversee how the NIS complies with any limitations on purpose stipulated by PST and that any conditions for processing are observed.

5.10 Letter to the Ministry of Justice and Public Security about shortcomings in the Police Act Section 17 d

In December 2024, the Committee sent a letter to the Ministry of Justice and Public Security about incorrect references in

20 Proposition No 80 to the Storting (Bill) (2019–2020).

the Police Act Section 17 concerning coercive measures in prevention cases.

For searches, seizures, surrender orders and future surrender orders, the provision refers only to the Criminal Procedure Act's provisions on deferral of information, and not to the provisions that regulate the coercive measures themselves. The Committee pointed out that it is unclear which of the provisions in the Criminal Procedure Act Chapter 15 on searches and Chapter 16 on seizures and surrender orders apply in prevention cases. The Committee made particular reference to the provision on prohibition against seizure in the Criminal Procedure Act Section 204. The Committee's letter can be read in the Norwegian version of the annual report.

5.11 Conclusion of prevention case and restriction of access to information

In its annual report for 2023,[21] the Committee mentioned that PST had corrected a non-conformity related to the conclusion of prevention cases. PST informed the Committee that the work to correct the non-conformity will also be subject to internal control by the service.

The Committee has noted that PST has updated its system with a new function that highlights which cases are restricted. This helps to simplify the Committee's oversight. The Committee assumes that the time when access is restricted will be logged so that the information is available for oversight purposes.

5.12 Follow-up of insufficient deletion in PST's registers

In 2023,[22] the Committee criticised PST for breach of the Police Databases Act Section 50 first paragraph and the Police Databases Regulations Section 22-3 first paragraph. The Committee followed up PST's work to correct the non-conformity in 2024 and will continue to follow it up in 2025.

The Committee is aware that the service has introduced artificial intelligence as an aid to help it to comply with the requirements set out in the Police Databases Act for deletion of information from PST registers. PST states that the new technology has made the service's work on deleting historical and future information significantly more efficient. PST also states that it has reviewed and deleted a considerable amount of historical information and that this work will progress systematically, but that some manual work will still be required for this task.

5.13 Complaint cases

The Committee has accepted eight complaints against PST for consideration in 2024. Some of these complaints were against more than one of the EOS services. The Committee concluded ten complaint cases against PST in 2024. Complaints against PST's security clearance authority are discussed in section 5.14.

In 2024, the Committee expressed criticism against PST in three complaint cases.

One case concerned PST's processing of a case under the Immigration Act Chapter 14. In such cases, PST submits an assessment giving reasons for its recommendation to the Norwegian Directorate of Immigration (UDI). According to the Immigration Act Section 127, UDI shall as a rule apply the assessment received from PST. In the case in question, the Committee criticised PST for giving very brief reasons. This gave rise to doubts as to whether the service had considered all relevant elements. The Committee also criticised PST for having omitted on five occasions to inform UDI that the service's assessment was based on classified information. In the Committee's assessment, this constituted a breach of the Immigration Regulations Section 19A-4 first paragraph.

In the second case, the basis for criticism was that PST neglected to follow up the deletion of information that the service had stated in writing that it would delete.

In the third case, the Committee asked PST for an account of the legal basis used to obtain information about a complainant from the health service, and of whether the dialogue had been documented. When the case was concluded, the Committee emphasised how important documentation of the case processing is to show the assessments made by the service and to provide a basis for oversight of regulatory compliance.

5.14 PST's security clearance authority

The Committee has investigated whether the security clearance authority could withhold from the vetted person information that parts of the grounds for denying security clearance had been left out, cf. the Security Act Section 8-13

21 Section 5.3 in the annual report for 2023.

22 Section 5.2 in the annual report for 2023.

second paragraph letter a. The Committee concluded that, in keeping with good administrative practice, the security clearance authority's written grounds should clarify which factors have formed part of the basis for the decision and which have not. This is also important for the Committee's oversight, as it will make it easier to review the assessments made by the security clearance authority.

The Committee expressed criticism against PST's security clearance authority in two complaint cases in 2024.

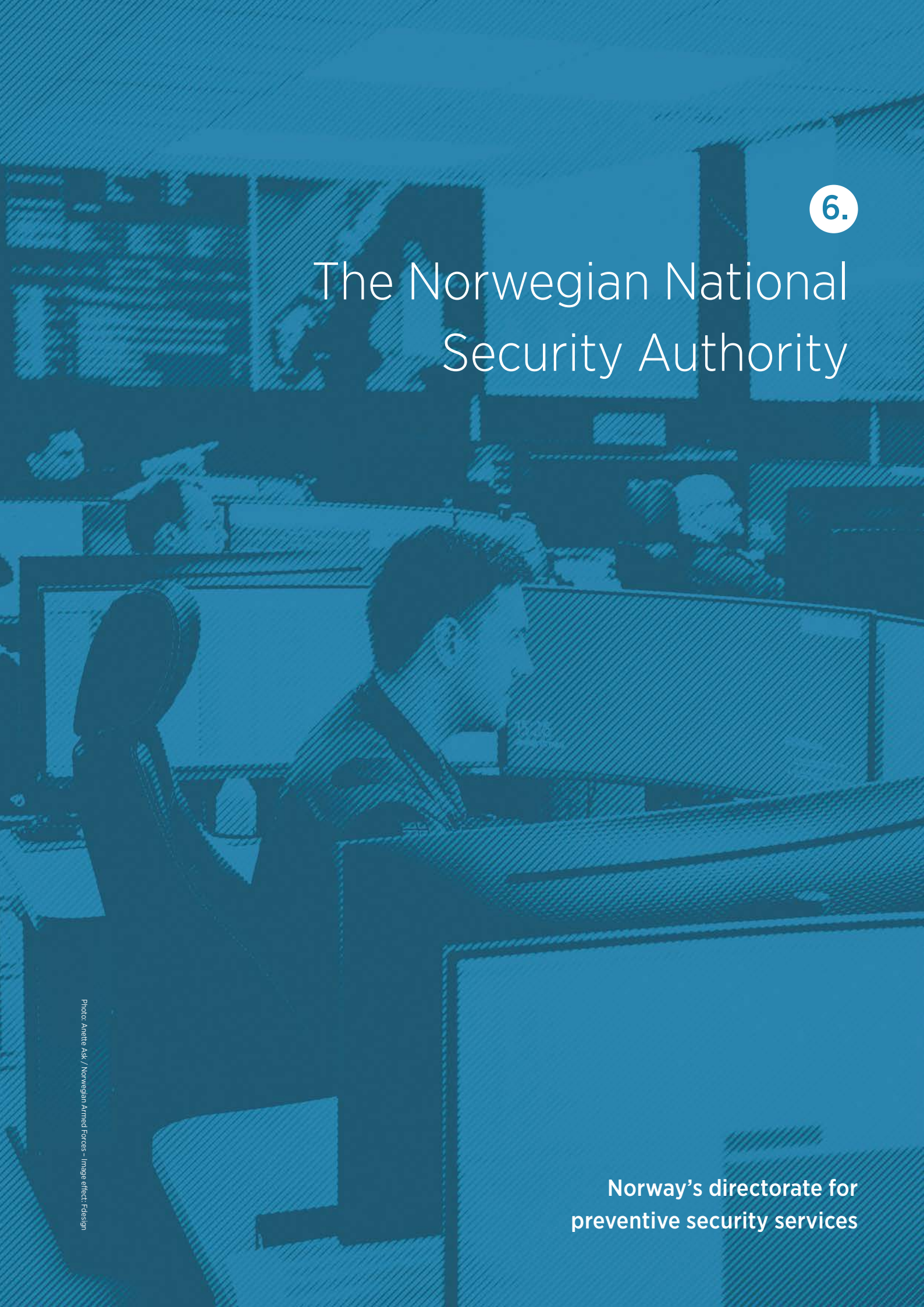
In one case, the Committee found that PST had not to a sufficient extent distinguished between the service's functions as a security clearance authority and as an employer. PST had acted in breach of good administrative practice in the case.

In another case, the Committee expressed criticism against the security clearance authority for misapplication of the law. The security clearance authority had incorrectly assumed that the Security Act Sections 8-4 and 8-5 provided legal authority for ordering health data to be disclosed. The security clearance authorities' right to access health data is based on the provisions on consent found in the Health Personnel Act Section 22 and the Patient Records Act Section 20. The Committee also criticised the security clearance authority for having assumed that the person whose consent is required for health data to be disclosed does not need to know which data the request for disclosure concerns when consent is given.

The Committee also pointed out that knowing the type of data that will be disclosed by the health service is a condition for valid consent to be possible. Therefore, the security clearance authority cannot on a general basis consider it a negative factor in the security clearance case that the person being vetted is aware of what information the health service has disclosed.

NSM was also criticised for these matters, see section 6.3.4.

The Committee also referred to the fact that, according to the Security Act Section 8-4 third paragraph, PST's security clearance authority has an independent responsibility for elucidating the legal aspects of a security clearance case. The Committee also criticised the security clearance authority for having attempted to collect health data without valid consent.



6.

The Norwegian National Security Authority

Photo: Anette Ask / Norwegian Armed Forces – Image effect: Fdesign

Norway's directorate for preventive security services

6.1 General information about the oversight

In 2024, the Committee conducted two inspections of the National Security Authority (NSM). The Committee's oversight has focused on NSM's operational duties as well as the use of conditions in security clearance cases. One inspection targeted NSM's security clearance authority, while the other 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 National Intelligence and Security Centre (NESS), cf. section 4.1.

During its inspections of NSM, the Committee focuses on the NSM's

- processing of cases where security clearance has been denied, reduced or suspended by the security clearance authority, and its processing of appeals in such cases
- case processing times in security clearance cases
- cooperation with other EOS services
- processing of personal data
- use of technical capabilities.

6.2 The specially appointed lawyer arrangement set out in the Security Act

In its annual report for 2023, the Committee concluded that the interim lawyer arrangement established in March 2023 was not suitable for balancing the interests of the vetted person's due process protection against the interests of national security in appeal cases. The Committee asked the Ministry of Justice and Public Security to consider discontinuing the arrangement. The Ministry has informed the Committee that the arrangement is undergoing evaluation.

6.3 Complaint cases

6.3.1 Introduction

The Committee has accepted 14 complaints against NSM for consideration in 2024. Some of these complaints were against more than one service. The complaint cases concerned surveillance and security clearance issues. The Committee concluded 14 complaint cases in 2024. The Committee expressed criticism against NSM in twelve of the complaint cases, all of which concerned security clearance issues.

6.3.2 Access to information in security clearance cases

In 2024, the Committee expressed criticism against NSM in two cases for having denied the complainants access to information in their security clearance case.

According to the Security Act Section 8-14, a person who has been assessed for clearance is entitled to examine the case documents. Section 8-14 second paragraph first sentence provides an exception from this right for documents which contain information as specified in Section 8-13 second paragraph letters a-e and for documents prepared as part of the internal case preparations. However, the exception in Section 8-14 second paragraph does not apply to 'factual information or summaries or other processed forms of factual information'. Access shall be granted to such information.

In its annual report for 2020, the Committee criticised NSM for having denied access to factual information. NSM informed the Committee that it disagreed with the Committee's understanding of the regulatory framework and had requested clarification of the applicable law from the Ministry of Justice and Public Security.[23]

In the two complaints cases considered in 2024, the Committee made reference to the fact that the Security Act remains unchanged on this point and provides a right of access to factual information. Therefore, NSM had no legal authority to deny the complainants access to factual information, neither facts in documents prepared as part of the internal case preparations or in a written summary from a security interview. The Committee criticised NSM based on this and expected the directorate to grant access to information in accordance with the Security Act Section 8-14 in future cases concerning access to information.

In one of the cases, NSM had also denied access to certain information because the information might reveal circumstances 'which are relevant to national security interests', cf. Section 8-14 second paragraph, cf. Section 8-13 second paragraph letter a. The Committee requested an account from NSM of how the withheld information – which consisted of factual information or summaries or other processed forms of factual information – might reveal circumstances relevant to national security interests. NSM referred to the fact that the documents were classified and that the issuer saw no reason to declassify them.

According to the Security Act Section 5-3 second paragraph, security classification shall not be used to a greater extent or for longer than necessary. The Committee expected NSM to follow up the public administration in cases where it comes to the directorate's attention, for example through oversight,

23 In 2021, NSM informed the Committee that the Ministry of Justice and Public Security was working to harmonise the Security Act's provisions on right of access with the provisions of the Public Administration Act.

that security classification is used to a greater extent or for longer than necessary.

In both cases, the Committee criticised NSM for withholding certain categories of information. The Committee was of the opinion that the exception in the Security Act Section 8-14 second paragraph did not provide a general legal basis for withholding the information, and found it difficult to see that the information could be withheld on the grounds given by NSM.

Finally, the Committee criticised NSM in both cases for having denied the complainants access to their own health data. The Committee referred to the exception from the vetted person's right of access to information provided for in the Security Act Section 8-13 second paragraph letter c for information 'of which the person should not gain knowledge in the interests of their health'. NSM had not invoked this exception in the two complaint cases in question. Therefore, the Committee was of the opinion that there was no legal basis for denying access to the information pursuant to the Security Act Section 8-14 second paragraph.

6.3.3 Inadequate elucidation of a security clearance case

In one complaint case, security clearance was denied following an assessment of the complainant's connection to another state. The Committee concluded that NSM had not ensured that the case was elucidated as well as possible, cf. the Security Act Section 8-4 third paragraph. The Committee asked NSM to reconsider the security clearance case.

The Committee also asked NSM to reconsider what information to give when informing the complainant of the decision and what information could not be communicated to the complainant pursuant to the Security Act Section 8-13 second paragraph.

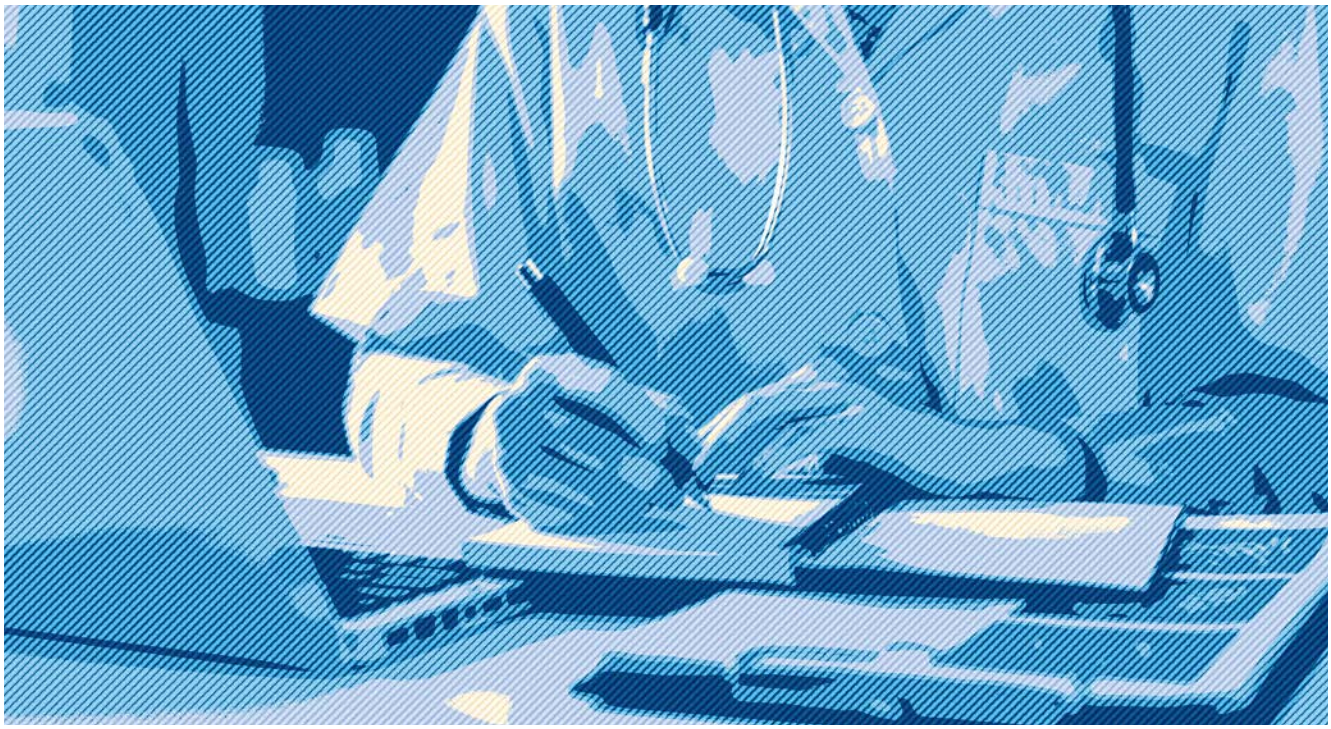
NSM stated that the appellate body would review the security clearance case based on the Committee's statement. In connection with its review, NSM would invite the complainant for a security interview and also consider whether other case processing steps were justified to better elucidate the case. NSM would also reconsider what information to give the complainant once it completed its reconsideration of the case.

The overall case processing time in this case was five years and nine months, of which the appeal case accounts for two and a half years. The Committee criticised both the Norwegian Civil Security Clearance Authority (SKM) and NSM for the very long case processing time.

6.3.4 The security clearance authority's access to health data

In one case, the Committee criticised both NSM and PST's security clearance authority for misapplication of the law. See section 5.14.

The Committee also pointed out that NSM should have based its assessment of the complainant's contributions to the elucidation of the case on a correct understanding of the relationship between the vetted person's consent and health



personnel's right to provide information. The Committee stated that NSM's decision to confirm the revocation of the security clearance was invalid.

Information about people's health could be crucial in many security clearance cases. The Committee pointed out that NSM, being the national expert authority, has a responsibility for seeing the provisions of the Security Act in conjunction with other legislation and providing guidance to security clearance authorities in such cases. The Committee also encouraged NSM to improve the guidance it provides to security clearance authorities.

Moreover, the Committee asked NSM to review similar cases.

6.3.5 Complaint case concerning security clearance and long case processing times

In one complaint case, the Committee criticised NSM for long case processing times, both for its processing of the appeal case and the associated request for access. NSM was also criticised for not having responded to the Committee's questions about its case processing times.

The Committee criticised NSM for breach of the Public Administration Act Section 11 a in its preliminary reply to the complainant. This provision requires 'the reason why the application cannot be dealt with earlier' to be explained, among other things. Good administrative practice dictates that the preliminary reply should, if relevant, be followed by messages providing adjusted and realistic information about the expected case processing time.

The complainant had more than once received messages notifying them of further delays after a deadline set by NSM itself had already expired. No reasons were given for the delays. The Committee was of the opinion that NSM should be able to give the complainant an unclassified reason why it took so long to process the case, as it had become public knowledge that NSM had had considerable backlogs for a long time and had been criticised for its long case processing times. If this was not possible, NSM should have informed the complainant that part of the reason contained classified information and therefore could not be disclosed to them.

The Committee also stated that it had reason to doubt whether NSM's practice of not stating the name of the case officer in e-mails, decisions in security clearance cases and appeal cases is in accordance with good administrative practice and the Public Administration Act's impartiality provisions. The Committee encouraged NSM to raise the issue with the Ministry of Justice and Public Security for clarification.

6.3.6 Long case processing times

The other seven complaint cases concerned long case processing times.

Three of the cases had not been decided by NSM when the Committee concluded its consideration of the complaints concerning long case processing times. In the first case, NSM's response to the Committee was that more than one year and eleven months had passed since the directorate received the case. NSM had only carried out the initial steps of case processing, despite claiming that the case was a priority. The case had already had a long case processing time in Civil Security Clearance Authority (SKM), see section 8.2. The overall case processing time from the request for security clearance until the final decision was made exceeded four years. The Committee stated that when the case processing time becomes this long, it undermines trust in the security clearance system. In any case, the processing time warrants strong criticism.

In the other case, NSM replied to the Committee that more than one year and two months had passed since NSM received the case. In this case as well, NSM had only carried out the initial steps of case processing, despite claiming that it was a priority case. The Committee criticised the long case processing time. The Norwegian Armed Forces Security Department (FSA) was also criticised in this case, see section 7.4. When the Committee concluded its case, the overall processing time in the case had reached two years and five months.

In the third case, more than 17 months passed after NSM received an appeal for consideration. All that was done in the case during this period was an initial review, before a new security interview was conducted towards the end of the period. NSM gave no reason for the long processing time in the case other than the general backlog. The Committee criticised NSM for the long processing time.

In 2023,[24] the Committee criticised NSM for long processing time in a case. The vetted person filed another complaint with the Committee. The Committee stated that although any further processing time will warrant criticism, a certain threshold must be applied before repeating criticism in the same case. Another five months passed before NSM reached a decision in the case. NSM had thus taken one year and four months to process the appeal, and the overall processing time had reached two years and five months. The Committee stated that a processing time of one year and four months for an appeal warranted strong criticism.

NSM took a year to process one case. The case was left untouched in the queue of cases waiting to be processed for one year. Once the case processing started, it was completed

24 See section 6.3 in the annual report for 2023.

in four days. The case was not processed sooner because older cases were given priority. The Committee understands that a challenging resource situation will affect case processing times, but this cannot justify a processing time of more than a year. FSA was also criticised in this case, see section 7.4.

In another complaint case, the Committee criticised NSM for a processing time of one year and nine months. The case had been left in the queue of cases waiting to be processed for just over one year and eight months. The case processing was then completed within a month. The complainant had also complained about the outcome of the security clearance case, but the Committee found no reason to criticise the actual decision. This case is also discussed in section 7.4.

One case had already had a long processing time in SKM, see section 8.2. NSM informed the Committee that the directorate made the case a priority, but that only initial case processing steps had been carried out. When the Committee expressed its criticism, the case had been under processing by NSM for four months. NSM has subsequently informed the Committee that a decision was made in the case six weeks after the Committee's criticism.

6.4 Case processing times in NSM's security clearance cases

The processing time for cases concerning access to information has decreased compared with 2023. For cases concerning requests for security clearance, the processing time has increased in 2024. This case category was transferred to SKM with effect from 1 May 2024. The directorate states that since 1 May 2024, it has only processed cases from its backlog.

The average processing time for second-tier appeals has decreased in 2024. NSM informed the Committee that many old cases had been concluded during the first half of 2024. The average processing time for cases concluded during the last half of the year was 161 days. NSM also stated that 44 per cent of appeal cases were decided with a processing time of less than 12 months, while 16 per cent of appeal cases were decided within 90 days. In 2023, the Ministry of Justice and Public Security asked NSM to reduce the processing times for appeal cases to 90–120 days. NSM stated that it continues to work towards this target in 2025.

Below is a table of case processing times for 2024 as provided by NSM.[25]

CASE PROCESSING TIMES NSM 2024	Average case processing time overall	Average case processing time, positive decisions[26]	Average case processing time, negative decisions
Request for access to information	22 days (7 cases)		
Request for security clearance	158 days (78 cases)	149 days (62 cases)	249 days (8 cases)
First-tier appeals	644 days (1 case)		644 days (1 case)
Second-tier appeals	393 days (138 cases)[27]	464 days (16 cases)	421 days (114 cases)

25 The statistics are based on the date on which NSM received the security clearance request or appeal case.

26 Figures for appeals granted in part are included under 'positive decisions'.

27 This figure includes dropped cases, overturned decisions and appeals concerning dismissed cases.

7.

The Norwegian Armed Forces Security Department

The Security Department has the overall responsibility for preventive security work in the Norwegian Armed Forces

Photo: Norwegian Armed Forces – Image effect: Fdesign

7.1 General information about the oversight

The Committee conducted two inspections of the Norwegian Armed Forces Security Department (FSA) in 2024. One inspection focused on FSA's processing of security clearance cases and the other on FSA's performance of operational security services. In 2024, the Committee has focused on FSA's exercises and training with international partners.

During its inspections of FSA, the Committee focuses on FSA's:

- processing of cases where security clearance has been denied, reduced or suspended by the security clearance authority
- case processing times in security clearance cases
- operational security activities
- processing of personal data
- cooperation with other EOS services.

7.2 The procedure for security clearance of persons with a connection to other states in preparation for national service

On 12 December 2024, the Committee published its criticism against FSA for the department's work under this procedure in order to contribute to the factual basis for the public debate about the Armed Forces' practice of annulling individuals' call-up for national service.

The Armed Forces introduced this procedure in 2020 to avoid having to discharge persons with a connection to other states after they start their national service because they are denied security clearance. The purpose of this procedure was to ensure that the processing of security clearance cases concerning persons with such connections would be completed before the persons in question started their national service. The start of their national service is therefore deferred for at least one year to allow the security clearance authority enough time to process the cases before these persons report for service.

The Committee investigated FSA's processing of security clearance cases that fell within the scope of this procedure during the period from 1 June 2020 to 11 August 2023. During the period in question, the Norwegian Armed Forces HR and Conscription Centre withdrew requests for security clearance of 290 persons because the security clearance cases had not been decided in time. FSA then discontinued the security clearance cases. The Committee has reviewed 314 cases registered to the 290 persons in question.[28]

The review of 266 cases showed that an average of 281 days, or more than nine months, passed from the case was opened until it was discontinued. In 133 of the 314 cases, FSA had asked the person vetted to give an account of their connection with other countries. This was the first activity registered in the cases. On average, these requests were sent 148 days, or nearly five months, after the case was opened. In 164 security clearance cases, no activity was registered other than the personal data form and sources received. FSA stated that no otherprocessing steps had been taken in these cases. The cases were discontinued after an average of 222 days, in effect without having been processed.

In response to a question from the Committee, FSA replied that the department had no written procedures for the processing of security clearance cases under the procedure for security clearance of persons with a connection to other states in preparation for national service.

The Committee was of the opinion that FSA had, over a period of several years, failed to ensure the satisfactory processing of security clearance cases that fell within the scope of this procedure. In the Committee's opinion, FSA should have taken steps when the procedure was introduced to ensure that initial assessments of the need for information were carried out in time for the cases to be decided before the persons reported for national service. The Committee criticised FSA for having failed to do so.

FSA shall decide cases without undue delay, cf. the Public Administration Act Section 11 a. Cases shall be elucidated as well as possible. The Committee stated that in many of the cases, the work carried out was not sufficient to elucidate the case in a timely manner. The processing of these cases is therefore in breach of good administrative practice.

In its statement to FSA, the Committee pointed out that it gives cause for concern that so many people did not have their case tried on its merits by FSA. The fact that this applies

28 Of the 290 persons concerned, 24 had two cases each registered in the security clearance authority's case processing to ol. Consequently, a total of 314 cases have been examined. The remaining 266 persons were registered with one case each.

Operational security service
Identifying and counteracting activity that poses a threat to security targeting Norwegian or foreign military activities, objects or personnel, or force protection measures.

to one group only, namely persons with a connection to foreign states, is particularly unfortunate. This practice could affect the population's support for and trust in the concept of universal national service.

The Committee found that it warrants strong criticism that FSA did not reach a decision in the cases of 290 persons, resulting in them not being called up for national service. It makes matters worse that these were cases that fell within the scope of the procedure introduced specifically to ensure that security clearance is in place before the persons start their national service. The Committee emphasised that the long case processing times could not be explained by reference to necessary case processing steps.

In 2024, FSA gave an account of a new procedure for processing of such cases in response to a question from the Committee. The Committee assumed that if this procedure is observed, it could help to ensure that cases are processed in a timely manner. The Committee also expressed the view that this procedure should be put into writing. A written procedure could provide some protection against violation of the rights of individuals, as well as simplify oversight of FSA.

The Committee's statement in full can be read in the Norwegian version of the annual report.

7.3 Deletion of personal data from visitor control

In December 2023, the Committee was informed of plans to introduce a new system for registering visits to military units. After the inspection, the Committee asked FSA about its processing of personal data about foreign military visitors.

FSA identified a non-conformity related to the storage period for personal data while following up the Committee's question. A new digital solution for registering such visits to Norway was introduced in 2019. Based on internal assessments, the storage period for personal data in the digital solution had been set to a maximum of three years. However, no personal data had been deleted since the solution's introduction in 2019. FSA deemed the non-conformity to constitute a violation of the GDPR Article 33, but concluded that it had not resulted in a risk to the rights and freedoms of natural person. The non-conformity was reported to the Armed Forces' data protection officer. The Committee emphasised the importance of ensuring that personal data are not processed for longer than is required for the purpose of the processing. The Committee took a positive view of the fact that the non-conformity was identified and that FSA had already started the process of deleting visitor control information registered before 2021.

7.4 Complaint cases

The Committee accepted nine complaints against FSA for consideration in 2024. Some of these complaints were against more than one service. Seven complaint cases against FSA were concluded in 2024. The complaint cases concerned surveillance and security clearance issues. The Committee expressed criticism against FSA in five of the complaint cases, all of which concerned security clearance issues.

In one case, the Committee criticised FSA for parts of its case processing in a security clearance case. The complainant received a negative security clearance decision from the FSA, which was upheld by the NSM following an appeal. The complaint filed with the Committee concerned both the outcome

Photo: Anette Ask / Norwegian Armed Forces - Image effect: Fdesign

and the case processing. FSA was criticised for giving inadequate grounds to the person vetted in the security clearance case. FSA was also criticised for inadequate case processing in relation to the question of the right to be assisted by a specially appointed lawyer pursuant to the Security Act Section 8-15, including the fact that the correspondence between the complainant and FSA was neither logged nor archived. Criticism was also expressed on the grounds that FSA did not grant the complainant the right to be assisted by a specially appointed lawyer. Finally, FSA was criticised for not having observed confidentiality considerations when granting access to information about the security interview. In the same case, NSM was criticised for long case processing time for its consideration of the appeal, see section 6.3.6.

The other complaint cases concerned long case processing times. In one case, the Committee criticised FSA because more than one year and eight months had passed since it received a request for security clearance for processing without a decision being made. FSA referred to inadequate case processing capacity and the fact that it took time to obtain information in the case. The Committee stated that even if the period for which FSA was waiting for information is disregarded, the overall case processing time is still disproportionately long.

In the second case, just over a year passed from FSA received a request for security clearance until a decision was made. FSA referred to inadequate case processing capacity.

The Committee appreciated that the resource situation is challenging, but did not consider that it justified such a long case processing time. The case was also left on hold for about ten months from the security interview took place before a decision was made. In the Committee's opinion, the case had been on hold for a disproportionately long time.

In one case, 13 months passed from FSA received a request for security clearance until the person vetted filed a complaint with the EOS Committee. The case processing had not yet been completed at the time of the complaint. The case was left without active processing for several periods of time. The Committee was of the opinion that the case had remained inactive for a disproportionately long time.

In the final case, a year passed from the request for security clearance was made before FSA reached a decision. Six months of this period passed after the case was transferred to a new case officer with a comment requesting that a new vetting be ordered.

7.5 Case processing times in FSA's security clearance cases

The average case processing times for all types of cases have increased compared with 2023.

Below is a table of case processing times for 2024 as provided by FSA.[29]

CASE PROCESSING TIMES FSA 2024	Average case processing time overall	Average case processing time, positive decisions[30]	Average case processing time, negative decisions
Request for access to information	28 days (16 cases)	28 days (16 cases)	
Request for security clearance	57 days (21,325 cases)	40 days (20,893 cases)	366 days (119 cases)
First-tier appeals	182 days (25 cases)	252 days (1 case)	140 days (16 cases)

29 The statistics are based on the date on which FSA received the request or appeal.

30 Figures for appeals granted in part are included under 'positive decisions'.

Vetting
Obtaining information of relevance to assessment of a security clearance case.

8.

The Civil Security Clearance Auhority

The Civil Security Clearance Auhority is the largest clearance authority in the civil sector

8.1 General information about the oversight

The Committee carried out one inspection of the Norwegian Civil Security Clearance Authority (SKM) in 2024. The main topic of the inspection was the use of conditions in security clearance cases.

8.2 Complaint cases

The Committee received five complaints against SKM in 2024. Some of these complaints were against more than one of the EOS services. Five complaint cases against SKM were concluded in 2024. The Committee has criticised SKM in four complaint cases.

In one case, the Committee criticised SKM for rejecting the complainant's request for assistance from a specially appointed lawyer pursuant to the Security Act Section 8-15 in 2020. Since the decision was later appealed, the Committee assumed that this error was not significant to the processing of the complainant's case. The case is also discussed in section 6.3.6. In addition, both SKM and NSM were criticised for long case processing times.

The other complaint cases concerned long processing times. In one complaint case, the Committee criticised SKM for an overall processing time of one year and seven months. A year passed from SKM received information until it made a decision. It then took six months for SKM to forward the appeal to the appellate body. In another case, it took SKM one year and four months to process a request for security clearance. Collection of information, a security interview and assessments were required in both cases. The Committee nevertheless found the overall case processing time to be too long.

In the final case, more than 16 months passed from the request for security clearance was submitted until a decision was made. SKM referred to the fact that it was a complex case, as well as to the authority's total caseload. The Committee appreciated the complexity of the case, but nevertheless considered that the time it had taken from the security interview took place until the decision was made was too long.

8.3 Case processing times in SKM's security clearance cases

The average case processing time has increased in 2024 compared with 2023. SKM stated that it is primarily the case processing times for access clearance and security clearance cases that have increased, and that this is due to the reduction in the backlog of older cases in 2024. The case processing time for first-tier appeals has continued to decrease in 2024 compared with 2023 and 2022. Also, the majority of security clearance cases were decided within six weeks.

Below is a table of case processing times for 2024 as provided by SKM.[31]

CASE PROCESSING TIME SKM 2024	Average case processing time overall	Average case processing time, positive decisions	Average case processing time, negative decisions[32]
Request for access to information	12 days (54 cases)	11 days (53 cases)	36 days (1 case)
Request for security clearance	76 days (7,663 cases)	58 days (7,205 cases)	363 days (458 cases)
Request for security clearance	81 days (1,106 cases)	52 days (1,005 cases)	367 days (101 cases)
First-tier appeals	86 days (58 cases)	92 days (5 cases)	86 days (48 cases)

31 The statistics are based on the date on which the case was registered in SKM's case processing system.

32 Persons who have been granted conditional security clearance are included under 'negative decisions'.

9.

A case which should be put before the Storting

The Committee has called attention to the long case processing times in security clearance cases in its annual reports to the Storting since 2011. The Oversight Act does not confer on the Committee powers to issue instructions or impose sanctions. The Committee notes that the long case processing times in security clearance cases remain a persistent challenge.

The security clearance system must strike a balance between important considerations for the individual's due process protection and national security. It is important that the security clearance authorities perform their duties properly to ensure that security clearance cases are processed on their merits and in a timely manner. The Committee considers that the long case processing times contribute to undermining trust in the security clearance system.

It is the Committee's opinion that the matter of the persistently long case processing times should be put before the Storting, cf. the Oversight Act Section 17 fourth paragraph no. 7.

10.

Oversight of other EOS services

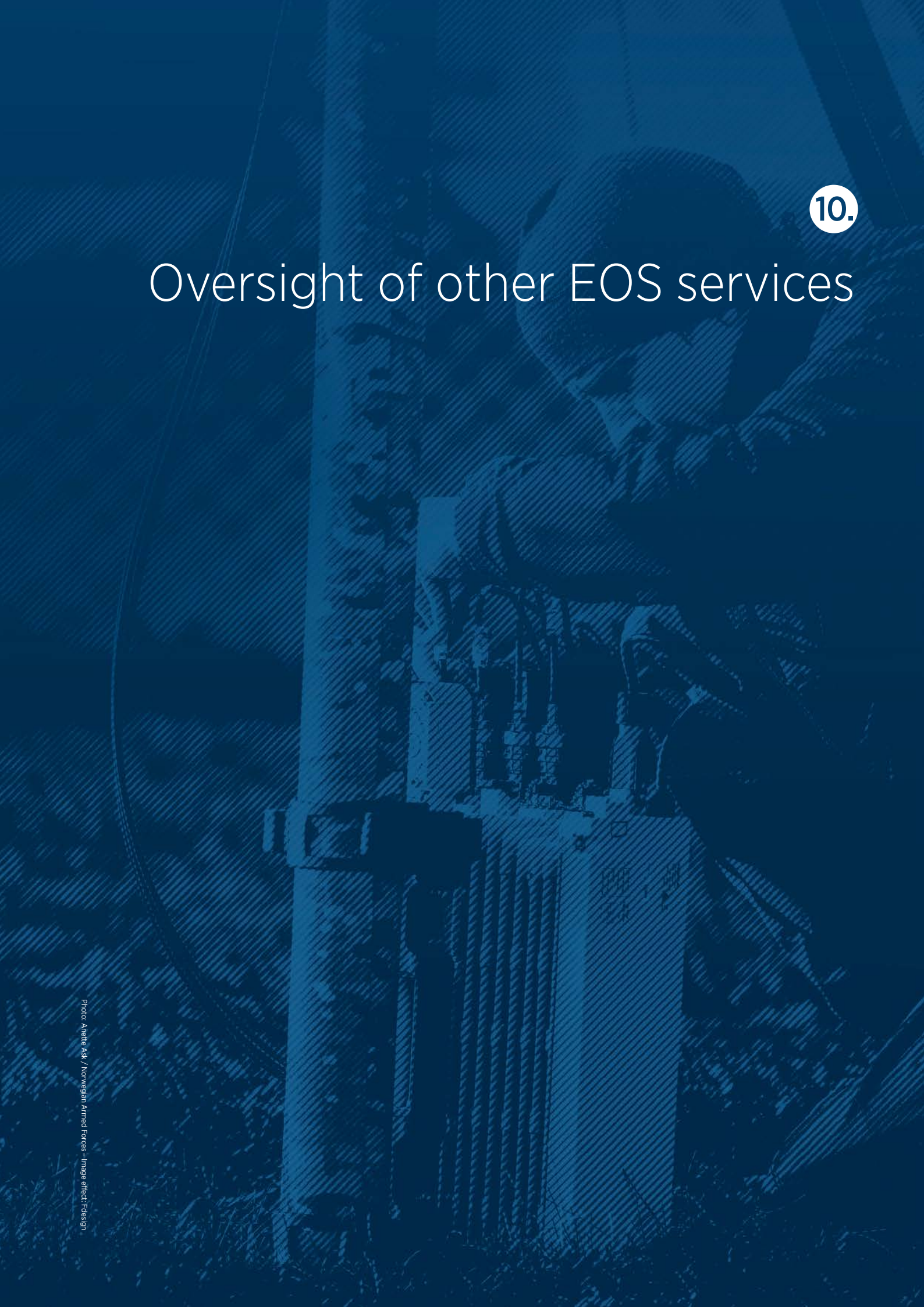


Photo: Anette Ask / Norwegian Armed Forces – Image effect: Fdesign

10.1 General information about the oversight

The Committee oversees EOS services regardless of which part of the public administration the services are carried out by. The oversight area encompasses all public bodies that carry out intelligence, surveillance or security services, and the oversight is not limited to specific organisational entities. The oversight area also encompasses parties that carry out such services under the control of or on the authority of the public administration, such as electronic communication providers.

10.2 Complaint cases

10.2.1 Introduction

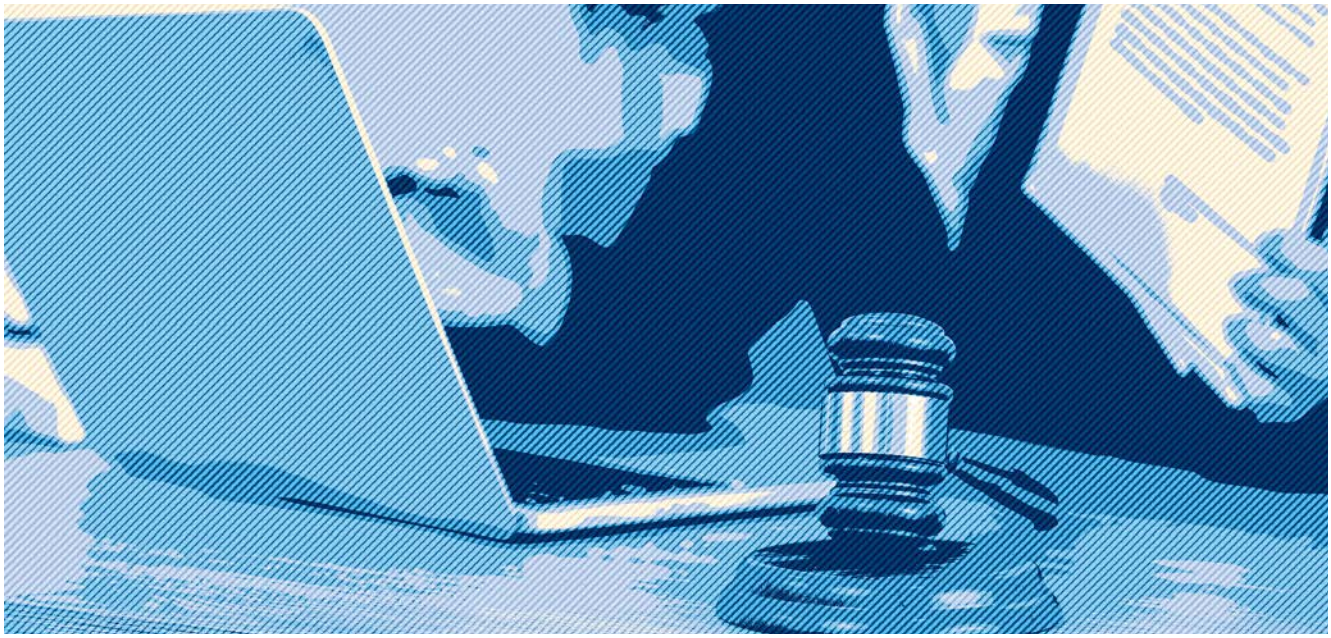
The Committee has accepted two complaints against other EOS services for consideration in 2024. One of these complaints was against more than one of the EOS services. One complaint case against another EOS service was concluded in 2024.

10.2.2 Potential abuse of security classification of documents in civil proceedings

The Committee has considered a complaint concerning the potential abuse of security classification of documents in a civil action involving the complainant and the government, represented by the Ministry of Justice and Public Security. The complainant argued that it in the course of the proceedings, it emerged that documents that had been prohibited from being presented as evidence pursuant to the Dispute Act because they were classified, apparently partly contained unclassified information. This information was discussed in open court. The complainant believed that the security classification of documents was used as a means of preventing access to evidence in the case.

According to the Security Act, the use of security classification is a form of protective security work that is subject to the control and oversight of the EOS Committee, cf. the Security Act Section 11-1. The EOS Committee refrains from investigating matters that have been subject to legal review by a court of law.[33] In the case in question, it was not possible for the court to check for itself whether or not the documents actually contained classified information, cf. the Dispute Act Section 22-3, cf. Section 26-7 subsection 2. The Committee, however, can check, and decided to ask the Ministry of Justice and Public Security about the grounds on which the documents in the case in question had been classified, cf. the Oversight Act Section 10 third paragraph.

The Ministry stated that following a request from the court pursuant to the Dispute Act Section 22-3 subsection 2, the issuer considered whether more sections of the document could be declassified. It emerged that the basis for the documents' classification was not individual pieces of information, but the fact that they formed part of a context which could reveal the method and weighting of the security clearance



33 The Oversight Act contains no provisions to this effect, but the Committee has adopted this policy based on analogous interpretation of the Act relating to the Parliamentary Ombudsman for Public Administration Section 4 second paragraph letter b.

authority in a manner that could harm national security interests, cf. the Security Act Section 5-3 first paragraph letter d.

The Committee agreed that, generally speaking, the collation of detailed security assessments and methods could harm national security interests if they become known to unauthorised persons. However, a real potential for such harm must be shown to exist following a concrete assessment.[34] The Committee was of the opinion that in this case, there was reason to doubt whether the overall nature of the information withheld was such that it had a certain potential for harm and thus had to be classified. The Committee's view was that the Ministry should conduct an independent review to determine if adverse consequences could result to some extent if the information was to become known to unauthorised persons. The Committee also remarked that investigations should be conducted to ensure that the issuer did not use security classification to a greater extent or for longer than necessary. The Committee stated that inadequate access to crucial documents, information and evidence in a case could encroach on an individual's right to a fair trial, cf. the European Convention on Human Rights (ECHR) Article 6.

10.3 The Army Intelligence Battalion

The Committee inspected the Army Intelligence Battalion (Ebn) in 2024. During the inspection, the Committee was briefed on Ebn's operations. Ebn also gave a demonstration of some of its technical equipment.

10.4 The Norwegian Armed Forces Special Operations Command

The Committee inspected the Norwegian Special Operations Commando (FSK) at Rena in 2024. During the inspection, the Committee received a briefing on FSK's activities and its cooperation with domestic and international partners. FSK also gave a demonstration of some of its technical equipment.

10.5 The Norwegian Armed Forces' Joint Headquarters

The Committee inspected the Norwegian Armed Forces' Joint Headquarters (NJHQ) in Bodø in 2024. The inspection included a briefing on NJHQ's activities, plans and legislation, as well as exercises and training with international partners. The Committee also had a guided tour of NJHQ.

10.6 Kripos' passenger information unit

The Committee inspected Kripos' passenger information unit in 2024. The unit was established in 2022 and serves as the national point of contact for PNR (Passenger Name Record) information. PST and the NIS are both 'competent authorities' that can request and receive PNR information, cf. the Police Databases Regulations Section 60-4 first paragraph no 6. The Committee inspected the unit to oversee its cooperation with and disclosure of information to PST and the NIS. During the inspection, the Committee received a briefing on the unit's activities.

34 Official Norwegian Report (NOU) 2016:19 Chapter 8.2.1.

11.

Appendices

APPENDIX 1 – Meetings, visits, lectures and participation in conferences

- In March, the Committee met with members of the Ukrainian parliament, Verkhovna Rada, at the Storting. See section 3.5.
- Secretariat staff attended meetings of the International Oversight Working Group in Brussels in April and in Stockholm in October. The group is a forum for cooperation between the intelligence oversight bodies of Sweden, Denmark, Norway, the UK, the Netherlands, Belgium and Switzerland. The Canadian oversight body also attended these meetings.
- In May, the Secretariat had a meeting with the Parliamentary Ombud for Scrutiny of the Public Administration regarding oversight of cases in the Armed Forces.
- The committee chair gave a lecture on the EOS Committee's oversight work for the Norwegian Association of Judges' human rights committee in May.
- The Secretariat met with the director of the office of the Parliamentary Ombud's Committee for the Norwegian Armed Forces in June and December.
- The Secretariat met with the Danish Intelligence Oversight Board (TET) in Denmark in August to discuss oversight methodology.
- In September, the Committee met with the German oversight body Parlamentarisches Kontrollgremium (PKGr) in Oslo. See section 3.5.
- The Committee and the Secretariat attended the Nordic meeting for the oversight bodies of Norway, Sweden, Denmark and Finland held in Copenhagen in September. See section 3.5.
- The committee took a study trip to Canada in October. See section 3.5.
- In October, the Secretariat gave a lecture on the EOS Committee's oversight of security clearance cases at the University of Oslo's Department of Private Law.
- In October, the Secretariat had a digital meeting with the Inspector General of Intelligence and Security (IGIS) of New Zealand.
- The Secretariat gave a lecture in October for the National Ombudsman and Ombudsman for Veterans of the Netherlands.
- In November, the Secretariat gave a digital talk about the EOS Committee for a conference on Security Sector Governance and Oversight held in Armenia. The conference was organised by DCAF – Geneva Centre for Security Sector Governance.
- In November, the committee chair met with the committee appointed to review NSM's portfolio to discuss the EOS Committee's experience of overseeing NSM.
- The committee chair gave a lecture on the Committee's work for the Norwegian Defence University College's course on politics, society and intelligence in November.
- The Committee met with the Norwegian Defence Research Establishment (FFI) in December. The Committee was briefed on FFI's work and the establishment's national and international cooperation.

Six of the then Committee members visited Canada for a study trip to meet the National Security and Intelligence Review Agency (NSIRA) and others. The photo is taken outside the Canadian Security Intelligence Service (CSIS).
Photo: NSIRA

APPENDIX 2 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 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

35 The act was last changed on 1 January 2023.

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 Armed Forces 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 Armed Forces 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.

Photo: Fabian Helmersen / Norwegian Armed Forces – Image effect: Fdesign

EOS COMMITTEE

THE PARLIAMENT APPOINTED COMMITTEE FOR INTELLIGENCE OVERSIGHT

Photo: Anette Ask / Norwegian Armed Forces – Image effect: Fdesign

fdesign.no

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

www.eos-utvalget.no