EOS COMMITTEE

THE PARLIAMENT APPOINTED COMMITTEE FOR INTELLIGENCE OVERSIGHT

ANNUAL REPORT FOR 2025

DOCUMENT 7 (2025–2026)

Photo: Kristian Kapelrud / 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 2025 to the Storting.

The annual report is unclassified. Pursuant to the Security Act, the issuer of information decides whether or not it is classified. The respective EOS 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 on 18 March 2026.

Grete Faremo

Kristin Krohn Devold | Olav Lysne | Jan Arild Ellingsen

Hege Solbakken | Åsa Elvik | Geir Sunde Haugland

Henrik Gudmestad Magnusson

The EOS Committee's members from left to right: Jan Arild Ellingsen, Kristin Krohn Devold (deputy chair), Olav Lysne, Grete Faremo (chair), Hege Solbakken, Geir Sunde Haugland and Åsa Elvik.

Contents

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, cf. the Oversight Act Section 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,
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 that fall 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. Subsequent oversight (ex-post) is practised in relation to individual cases and operations. However, the Committee may be informed about, and state it's 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 encourage 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.

In its annual report, the EOS Committee informs the Storting about circumstances that have come to the Committee's attention in the course of its oversight activities that it feels the Storting should be aware of. This is particularly relevant in relation to cases where, based on its purpose as set out in Section 1 of the Oversight Act, the Committee has found reason to criticise the services or otherwise express its opinion on matters within the oversight area, cf. the Oversight Act Section 14. The annual report is not intended to provide a complete overview of the Committee's oversight activities or the work carried out by the services.

The Committee is independent of both the Government and the Storting. The Storting may, however, 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 a term 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.

On 4 February 2025, committee chair Astri Aas-Hansen was appointed Minister of Justice and Public Security and withdrew from the Committee. Grete Faremo has chaired the Committee since 18 March 2025. Geir Sunde Haugland has been a member since 1 July 2025. He replaced Erling Johannes Husabø.

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.

Subsequent oversight (ex-post)
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.

Below is a list of the committee members in 2025 and their respective terms of office.

The Committee during the first six months of 2025:

Astri Aas-Hansen, Asker, chair
1 July 2019 – 4 February 2025

Grete Faremo, Oslo, chair
18 March 2025 – 30 June 2027

Kristin Krohn Devold, Oslo, deputy chair
1 July 2021 – 30 June 2029

Erling Johannes Husabø, Bergen
1 July 2019 – 30 June 2025

Jan Arild Ellingsen, Saltdal
1 July 2021 – 30 June 2029

Olav Lysne, Bærum
1 July 2021 – 30 June 2029

Hege Solbakken, Bergen
1 July 2024 – 30 June 2027

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

The Committee during the last six months of 2025:

Grete Faremo, Oslo, chair
18 March 2025 – 30 June 2027

Kristin Krohn Devold, Oslo, deputy chair
1 July 2021 – 30 June 2029

Jan Arild Ellingsen, Saltdal
1 July 2021 – 30 June 2029

Olav Lysne, Bærum
1 July 2021 – 30 June 2029

Hege Solbakken, Bergen
1 July 2024 – 30 June 2027

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

Geir Sunde Haugland, Våler in Østfold
1 July 2025 – 30 June 2029

Of the seven members currently on the Committee, five have political backgrounds from different parties. The other two possess special legal and technological expertise.

As stated in the annual report for 2024, the Committee has in 2025 considered the best structure for its organisation and work going forward. Following this review, the Committee sees no need to propose any amendments to the Oversight Act at present.

2.

Overview of the Committee's activities in 2025

Photo: Ørjan Andreassen / Norwegian Armed Forces – Image effect: Fdesign

The EOS Committee's inspections in 2025

2.1 Key figures

The Committee's expenses amounted to NOK 52,254,000 in 2025. The total budget, including transferred funds, was NOK 53,069,000. The Committee has applied for permission to transfer unused funds to its budget for 2026. The Committee refers to the administrative annual report published on its website for further details.

The workload of the chair of the Committee corresponds to about 30 per cent of a full-time position. The office of committee member is equivalent to about 20 per cent of a full-time position. The Committee is supported by a secretariat headed by a director.

2.2 Oversight activities

In 2025, the Committee conducted 18 inspections.

The Committee held twelve regular committee meetings in 2025, as well as working meetings on site in connection with inspections. During the internal meetings, the Committee discusses inspections, complaints and cases raised on the Committee's own initiative, reports to the Storting and administrative matters.

In 2025, the Committee raised 26 cases on its own initiative. It concluded 34 cases raised on its own initiative in 2025.

The Committee investigates complaints from individuals and organisations. In 2025, the Committee considered 38 complaints against the EOS services. The Committee concluded 35 complaint cases in 2025.

2.3 Main findings from oversight activities carried out in 2025

The Committee oversees the Norwegian Intelligence Service's (NIS) use of the method of facilitated bulk collection. The oversight has been intensified in 2025 compared to previous years. The Committee has experienced challenges in carrying out its oversight activities. In November 2025, the Committee submitted a special report to the Storting concerning unlawful storage of content data by the NIS, see section 3.2.1. In this report, the Committee highlighted oversight challenges resulting from the distinction between metadata and content data set out in legislation, as well as how the NIS approached this by using acquired software that was not tailored for the NIS's requirements. The Committee considers it important to resolve these challenges as soon as possible, out of consideration for the NIS's performance of its mission and the Committee's possibility to oversee it.

The persistent security clearance issues are a source of concern for the Committee. Complaints received by the Committee, cases raised on the Committee's own initiative and information obtained in connection with inspections all combine to form a consistent picture of a security clearance situation characterised by long case processing times and inadequate coordination, procedures and digitalisation. This situation is detrimental to the due process protection of individuals, cause people's careers to be put on hold and could also be harmful to national security and preparedness.

In March 2024, the Committee criticised the Norwegian Armed Forces Security Department (FSA) for failing to ensure satisfactory progress in security clearance cases concerning persons with a connection to other states in preparation for national service. Two years later, there are few signs of improvement, see section 7.2. The Committee has informed the Ministry of Defence of its concerns.

At the same time, the Committee sees a troubling increase in The Norwegian National Security Authority's (NSM's) case processing times and their backlog of facility security clearance cases in 2025, see section 5.2. Unless this development is reversed, the situation could require the Committee to consider whether it unduly harms the interests of society. The Committee has informed the Ministry of Justice and Public Security of its concerns.

On 19 December 2025, the Government announced its intentions to established a joint security clearance authority for civil and military purposes, provided the Storting's approval. The Committee will keep informed about the work to modernise the security clearance system.

In the course of its oversight of PST in 2025, the Committee has observed several non-conformities that could be linked to a lack of adequate digital tools to facilitate compliance with regulatory requirements. One example from 2025 is the failure to review approximately 6,500 registrations within the five-year deadline, see section 4.7.

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

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.

The Committee notes that the National Audit Office of Norway also pointed out weaknesses and shortcomings in PST's current IT portfolio in its report submitted in December 2025.[1]

If the Committee's investigations result in statements or criticism, the matter will be mentioned in the Committee's annual report to the Storting or in a special report.

2.4 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, their use of methods and the processing of personal data. The services are asked to include in the briefing any matters they deem to be relevant to the Committee's oversight, such as non-conformities that they themselves have identified. The Committee asks verbal questions during the briefings and, if needed, sends written questions afterwards.

The Committee has wide rights of inspection and far-reaching access to information held by the services and may conduct searches directly in the services' systems. The services are not told which searches the Committee carries out.

The Committee's approach to the oversight work is thematic, and the focus of its oversight activities is based on assessments of where the greatest risks are assumed to be found. During the oversight year, the Committee has focused on certain topics in its oversight of PST, the NIS, the security clearance authorities and FSA.

The Committee raises cases on its own initiative based on findings made during its inspections and other investigations. Such cases may also be raised on the basis of notifications received 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 is always given the opportunity to express it's opinion on issues raised in cases that may result in criticism or other statements from the Committee in advance.

In its statements, the Committee may express its opinion on matters within the oversight area. For example, it may criticise the service if an error has been committed or if the Committee believes that a decision should be deemed invalid or clearly unreasonable.

2.5 The Committee's consideration of complaints

Complaints that fall within the Committee's scope 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 must not contain classified information. Information that a person is under surveillance and information that a person is not under surveillance both constitute classified information.[2] If the Committee's investigation shows that the complainant's rights have been violated, the Committee will criticise the service or services in question and inform the complainant that the complaint contained valid grounds for criticism.[3]

If the Committee is of the opinion that a complainant should be given a more detailed explanation, it may propose this to the service in question or to the responsible ministry. The decision of the service or ministry 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.

2.6 Consultation statements

The Committee submitted seven consultation statements in 2025. One concerned the proposed new special act on access to information etc. for the Committee for the Evaluation of the Norwegian Intelligence Service Act. The other concerned amendments to

- **i.** the Data Centre Regulation
- **ii.** the Security Act Section 8-4 on security clearance decisions
- **iii.** the regulatory framework for the Norwegian Anti-Discrimination Tribunal
- **iv.** the Electronic Communications Act and Electronic Communications Regulation concerning disclosure of IP data for the purpose of preventing serious crime

1 See the National Audit Office of Norway's Document 3:6 (2025–2026) *Resource utilisation and efficiency in the Norwegian Police Security Service (PST)*, p. 16 section 5.5.

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

3 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 complaint cases concerning surveillance.

v. the Police Register Act on testing and development of information systems and PST's processing of openly available information etc.
vi. the Mental Health Care Act etc. on exchange of information between the health service and the police and PST concerning persons with mental health problems and assumed risk of violence.

You can read the consultation statements on the Committee's website.[4]

The chair of the EOS Committee, Grete Faremo, submitted the Committee's annual report for 2024 to the first vice president of the Storting, Svein Harberg (Conservative Party), on 26 March 2025.
Photo: Peter Mydske / The Storting

The EOS Committee's 2025 annual conference brought together the heads of the EOS services for a discussion about artificial intelligence and oversight. From left to right: Arne Christian Haugstøyl, Director General of the Norwegian National Security Authority (NSM), Beate Gangås, Director General of the Police Security Service (PST), panel chair Siri Lill Mannes and Nils Andreas Stensønes, head of the Norwegian Intelligence Service (NIS).

2.7 Meetings and external activities

The Committee submitted its annual report for 2024 to the Storting on 26 March 2025. The committee chair met with the first vice president of the Storting, and the Committee met with the Standing Committee on Scrutiny and Constitutional Affairs. The Committee hosted its annual conference, this year on the topic of artificial intelligence and oversight, the following day. The conference was open to the public and available via streaming. The programme included the heads of PST and the NIS, the Director General of NSM, a representative of the British oversight body IPCO and one from the British intelligence service GCHQ.

The EOS Committee had two meetings with the Committee for the Evaluation of the Norwegian Intelligence Service Act. The EOS Committee gave a briefing on the special report it submitted to the Storting on 12 November 2025.

The Committee continued its international cooperation within the Intelligence Oversight Working Group (IOWG) in 2025. Meetings were held in Copenhagen and in Zurich. A new member, the Canadian oversight body NSIRA, joined the group this year. Other members of the group are the EOS oversight bodies in Sweden, Denmark, Belgium, the Netherlands, Switzerland and the UK. During these meetings, the group members discuss various issues relating to oversight and oversight methodology at an unclassified level.

There are two other established international conferences for oversight of intelligence and security services. In 2025, the committee chair attended the European Intelligence Oversight Conference (EIOC) in Zurich. This conference brings together oversight bodies from most European countries where EOS services are subject to oversight.

The Committee's deputy chair attended the International Intelligence Oversight Forum (IIOF) in Austin, USA. In addition to oversight bodies, this forum is also attended by scientists and representatives of NGOs as well as government and intelligence service employees.

The Committee met with representatives of Oslo District Court, Borgarting Court of Appeal and the Supreme Court on 11 December 2025.

A more detailed overview of the EOS Committee's external activities in 2025 is provided in Appendix 1.

4 See eos-utvalget.no/hjem/aktuelt/horingsuttalelser

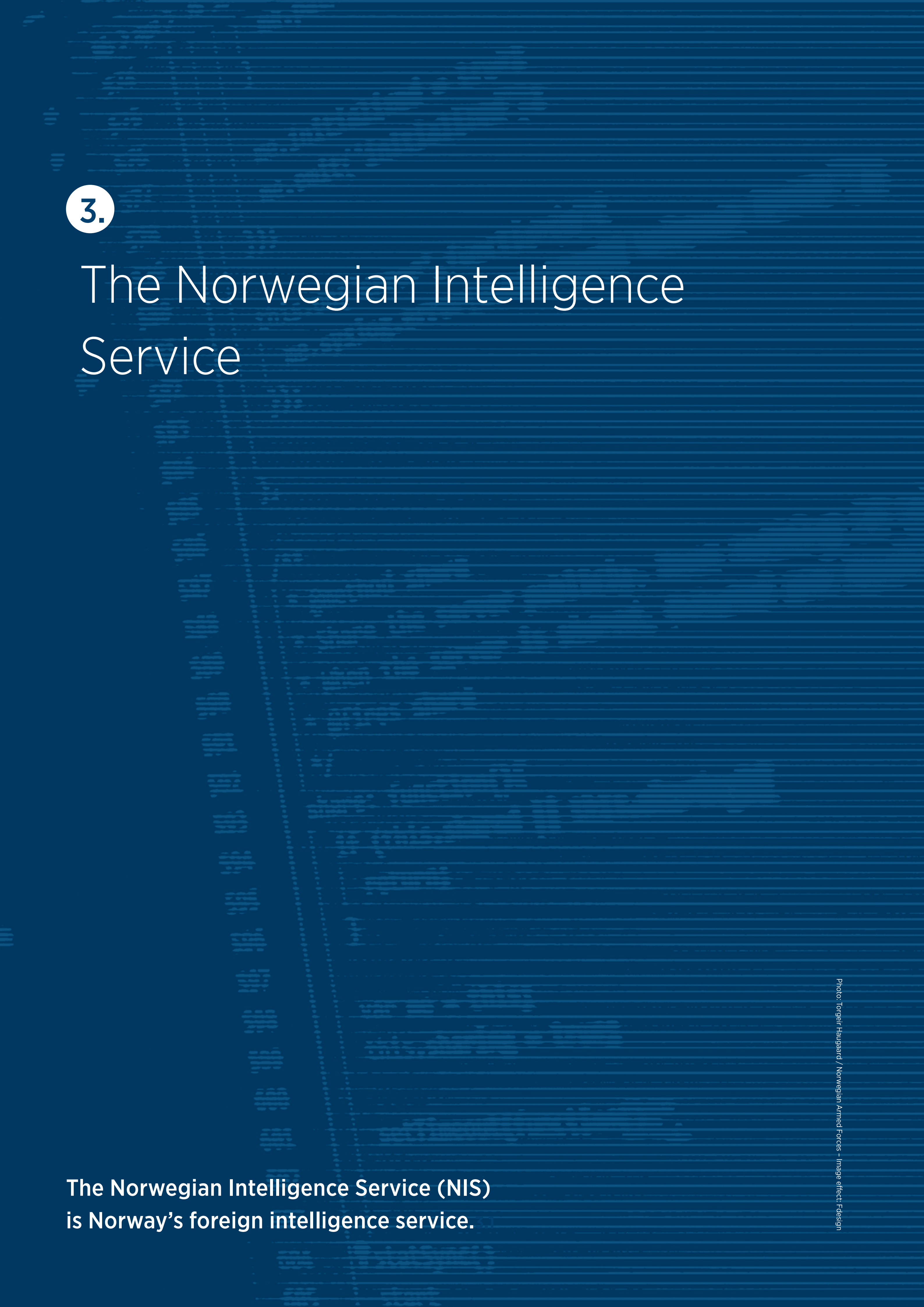


Photo: Torgeir Haugaard / Norwegian Armed Forces – Image effect: Fdesign

3.

The Norwegian Intelligence Service

The Norwegian Intelligence Service (NIS) is Norway's foreign intelligence service.

3.1 General information about the oversight

The Committee conducted four inspections of the NIS headquarters in 2025. The Committee has paid particular attention to the use of artificial intelligence by the NIS in its oversight activities. The Committee has also inspected the service's station in Ringerike.

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
- facilitated bulk collection of transboundary electronic communication
- whether the NIS's stations, equipment, methods and collection of information are subject to national control
- exchange of information with foreign and domestic partners
- cases that have been submitted to the Ministry of Defence[5]
- internal approval cases.

The Committee's right of inspection does not extend to the NIS's particularly sensitive information.[6] 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.

3.2 Facilitated bulk collection

The EOS Committee is charged with continuously overseeing the NIS's compliance with the provisions of the Intelligence Service Act on facilitated bulk collection of transboundary electronic communication. The provisions entered into force on 1 October 2023. Following these ammendments, the NIS can use the facilitated bulk collection method for intelligence production.

The facilitated bulk collection system has still been under construction and development in 2025, but has nevertheless been used for data collection and metadata searches. The system procurement is scheduled to be completed in 2026. The Committee has previously requested that the NIS develop functions in its systems to facilitate the Committee's oversight of facilitated bulk collection as required by the Intelligence Service Act Section 7-11.[7] The Committee has followed up the ongoing development of these oversight functions in 2025.

The Committee's oversight has been intensified compared with previous years. The oversight has focused on the testing and development of facilitated bulk collection as well as the NIS's operational use of the method. The Committee has conducted oversight of the service's storage of metadata based on court authorisations for mirroring of data. The Committee has reviewed the NIS's use of the head of the NIS's power to make urgent decisions allowing facilitated bulk collection and the NIS's facilitated bulk collection activities based on ordinary authorisation by the courts. The investigation covered the NIS's searches in stored metadata, and collection and storage of content data.

5 Pursuant to the Intelligence Service Act Section 2-5.

6 See the EOS Committee's annual report for 2013–2014 (Dokument 7:3 – 2013–2014) p. 31 section 2.2, as well as Document No 16 (1998–99), Recommendation No 232 to the Storting (1998–99) and minutes from and decisions by the Storting dated 15 June 1999. In its 1999 plenary decision, the Storting decided that a special procedure should apply in disputes about access to NIS documents. The decision was based on the particular sensitivity associated with some of the NIS's sources, the identity of persons with roles in occupation preparedness and particularly sensitive information received from foreign partners. In 2013, the EOS Committee asked the Storting to clarify whether the Committee's right of inspection as enshrined in the Act and Directive shall apply in full in relation to the NIS, or if the Storting's decision from 1999 shall be upheld. At the request of the Storting, this matter was considered in the report of the Evaluation Committee for the EOS Committee, submitted to the Storting on 29 February 2016, see Document 16 (2015–2016). When the Evaluation Committee's report was considered in 2017, the limitation on access to 'particularly sensitive information' was upheld, but without the wording of the Act being amended.

7 See the annual report for 2024 section 4.3.

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.

Intelligence production
Compiling and analysing information collected for intelligence purposes.

Mirroring
Mirroring entails the NIS receiving a copy of data transmitted through selected cross-border cables. The mirrored data are processed in accordance with the Intelligence Service Act, for example by storing metadata from the communication.

In the course of its oversight, the Committee has gained experience of the NIS's use of facilitated bulk collection and the legal basis for this method.

Certain aspects of the Intelligence Service Act present oversight challenges in relation to the NIS's use of this method. This was emphasised in the Committee's special report mentioned in section 3.2.1 below. The Committee will continue its oversight work in relation to these issues in 2026.

3.2.1 Special report on the NIS's unlawful storage of data obtained through facilitated bulk collection

On 12 November 2025, the Committee submitted a special report to the Storting concerning unlawful storage of data from facilitated bulk collection by the NIS (Document 7:1 (2025–2026)). When using facilitated bulk collection, the NIS may store metadata from transboundary electronic communication in bulk on a continuous basis, subject to certain conditions. The metadata may be stored for up to 18 months, and the NIS can later conduct searches in these data subject to court authorisation. The NIS can also be given permission to store future content data from a time set by the court. Storage of content data must take place in a targeted manner within the scope of the court's authorisation, and content data may not be stored in bulk.

Grete Faremo submitted the EOS Committee's thirteenth special report to the Storting to President of the Storting Masud Gharahkhani on 12 November 2025.
Photo: Peter Mydske / The Storting

In its special report, the Committee criticised the NIS for having stored email subject fields in bulk in its metadata store. The service and the Committee agree that email subject fields constitute content data and that the storage was thus unlawful. The Committee referred to the fact that the distinction between storage of metadata in bulk and targeted storage of content data is fundamental to due process protection. The Committee criticised the NIS for shortcomings in the service's work to prevent unlawful storage. The NIS had not implemented sufficient measures to ensure compliance with the Intelligence Service Act in the system where metadata were stored. The Committee expected a quicker response from the service to the need for measures to prevent unlawful storage of metadata than in the present case. In its report, the Committee pointed out oversight challenges related to the current statutory list of the types of metadata that may be stored. The Committee highlighted that the distinction between metadata and content data set out in the Act presented challenges for the oversight, and that the Committee would continue to work on these issues in the time ahead.

3.2.2 Questioning whether urgent decisions to use facilitated bulk collection were passed by the right person

In one case the decision regarding facilitated bulk collection was made by the head of the NIS's deputy. To eliminate any doubt that the deputy actually holds the legal power to make such decisions, the Committee stated that the NIS should consider clarifying the internal deputy function in relation to use of the power to make urgent decisions regarding facilitated bulk collection. The Committee expected the requirements for use of these powers in future urgent decision cases, would be easy for the Committee to carry out oversight with.

3.2.3 Unlawful testing in the facilitated bulk collection system

The Intelligence Service Act imposes restrictions on the use of data obtained through facilitated bulk collection by the NIS and stipulates procedural requirements. By mistake, the NIS had implemented a test collection in relation to actual data obtained through facilitated bulk collection instead of test data for use in simulations. The Committee criticised the NIS for unlawful testing, but noted that it was not a serious offence. The collection took place in relation to an email address that was controlled by the NIS and set up for the sole purpose of testing. No data had been collected from the email address. The NIS has since introduced control mechanisms that the Committee believes will contribute to prevent similar errors in future.

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

3.3 The NIS's and PST's processing of confidential communication between lawyers and clients

As a rule, the NIS may not process information that concerns individuals confidential communication with members of special professions. Exceptions apply in cases where interests of national security must take precedence over the protection of confidential information. In such cases, the decision must be made by the head of the NIS in accordance with a special procedure, cf. the Intelligence Service Act Section 9-5.

The NIS had processed confidential information between a Norwegian lawyer and client. This was done without a decision by the head of the NIS and without complying with the other procedural requirements stipulated in the Act. The Committee pointed out that good procedures are crucial to ensuring that the NIS performs its duties in a lawful manner. The Committee criticised the NIS for processing confidential information in breach of the Act. The NIS stated that the information would be deleted.

3.4 Collection and disclosure of information about a Norwegian citizen by the NIS and PST

PST shared information about a Norwegian citizen with a foreign service, see section 4.5.

It was the NIS that passed the information on to the foreign service. At the same time, the NIS shared information of its own and requested that the foreign service refrain from taking operational action that could impact the NIS's use of methods. The Committee asked the NIS to give an account of its contact with the foreign service in light of the requirements stipulated in the Intelligence Service Act Section 10-6 regarding the NIS's role when passing on information. The Intelligence Service Act Section 10-6 requires the NIS in these cases to 'not add information of its own or ask the recipient to act in any particular manner in light of the information received'. After receiving feedback from the NIS, the Committee agreed that the NIS's role in passing on information did not bar the service from performing its duties within its own remit. The Committee emphasised though the importance of the NIS making it clear to recipients when the service is acting on behalf of another party and when it is acting within its own capacity.

Whether valid authorisation from the head of the NIS had been obtained for the specific use of methods in relation to the Norwegian citizen abroad was also an issue in the case.[8] The NIS was of the opinion that the head of the NIS's annual collection plan for the method in question constituted a sufficient and valid decision-making basis. The Committee disagreed and found that this use required a specific decision in the case in question by the head of the NIS as explicitly laid down in the annual collection plan for the method.

3.5 The NIS's procedures for collection cooperation with partners

The Committee asked the NIS about its procedures for disclosure of information to a partner when the partner is to collect information on behalf of the NIS. The conditions stipulated in the Intelligence Service Act for use of intrusive methods must still be met, even when the actual collection is carried out by a partner.

The Committee reviewed the service's procedures for initiating and concluding such collection and the service's procedures for registering non-conformities. It was the Committee's opinion that a partner's collection activities in relation to the target must stop more or less in real time to prevent the partner from collecting information on behalf of the NIS in breach of the Intelligence Service Act.

The Committee stated that the Intelligence Service Act regulates the use of intrusive methods, and that the use of intrusive methods without the statutory requirements being met, constitutes a breach of the law, regardless of what results such collection produces. If no information is collected, this will make the breach less serious, though.

The Committee stated that partners should report non-conformities to the NIS if they had used intrusive methods in relation to a target in conflict with the service's instructions. This will allow the NIS to identify and remedy shortcomings in its own system. Such reporting will also make it easier for the EOS Committee to oversee whether the rights of Norwegian citizens have been violated.

With reference to the Oversight Act Section 14 third paragraph final sentence, the Committee encouraged the NIS to make 'improvements in administrative and

8 See the Intelligence Service Act Sections 6-12 and 6-13.

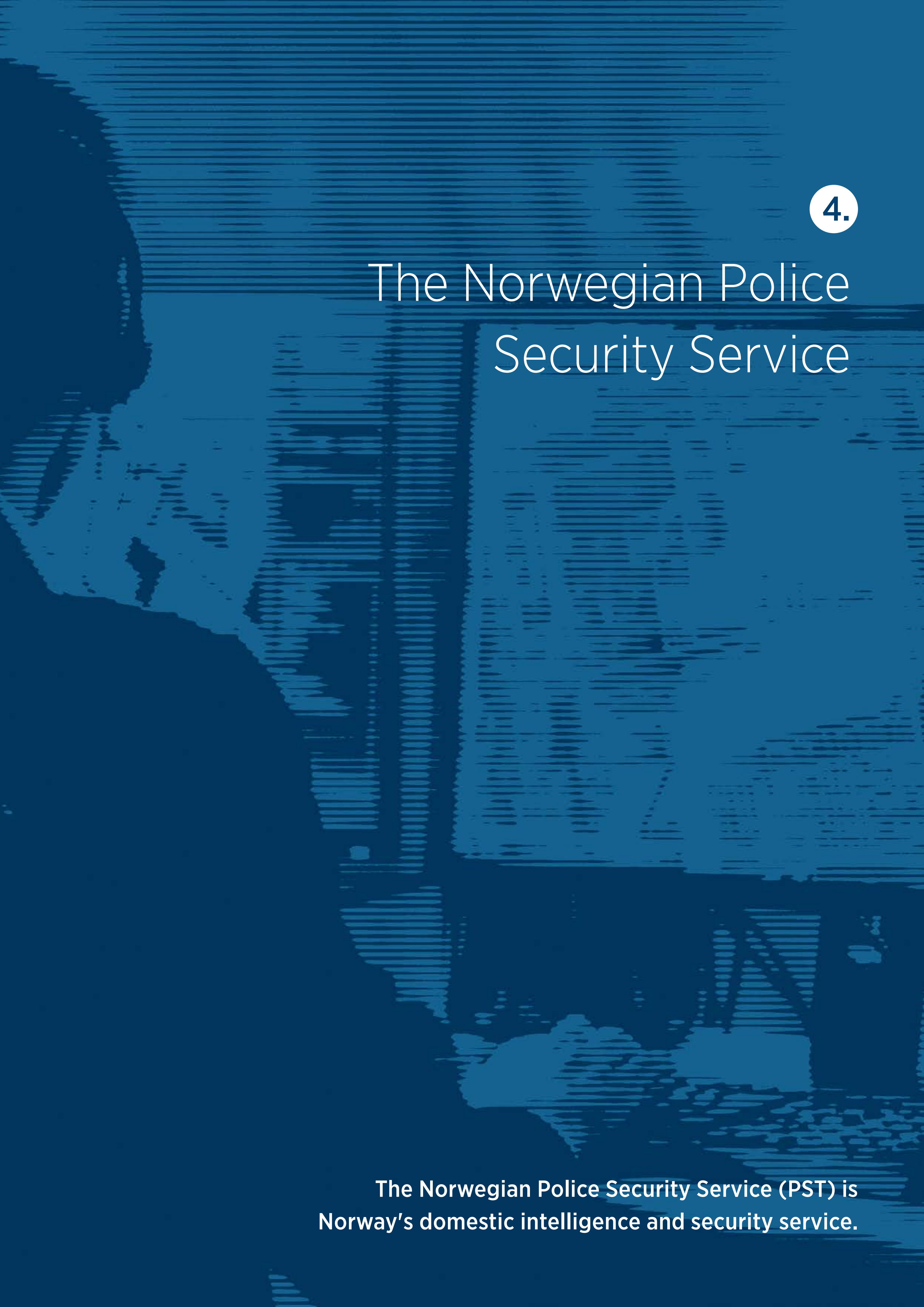
organisational arrangements and procedures' in order to 'make oversight easier' and 'safeguard against violation of someone's rights' by

i. ensuring that a partner's collection activities in relation to a target are discontinued more or less in real time
ii. ensuring that the use of intrusive methods against a target in breach of the Intelligence Service Act is recorded as a non-conformity, even if the use of such methods has not yielded any results
iii. ensure non-conformity reporting by partners.

The Committee asked to be kept informed about the improvements that the service stated were underway.

3.6 Complaint cases

The Committee accepted three complaints against the NIS for consideration in 2025. All of these also concerned other EOS services. The Committee concluded three cases in 2025 without criticising the NIS.



4.

The Norwegian Police Security Service

The Norwegian Police Security Service (PST) is Norway's domestic intelligence and security service.

4.1 General information about the oversight

In 2025, the Committee conducted four inspections of the PST Headquarters (DSE). The PST entities in Møre og Romsdal and East police districts were also inspected.

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.

In its inspections of DSE in 2025, the Committee has focused on PST's internal control, with the requirements regarding the service's processing of personal data set out in the the Police Register Act and the the Police Register Regulation as a starting point.

4.2 Investigation of PST's use of covert coercive measures and the counsel arrangement under the Criminal Procedure Act Section 100 a

4.2.1 Introduction

Unlike the rest of the police, PST can use covert coercive measures in its preventive activities subject to court authorisation, cf. the Police Act Section 17 d. The standard of suspicion under this provision is 'reason to investigate whether someone is preparing for an act', which is lower than the Criminal Procedure Act's requirement for 'probable cause' for an investigation. The criminal offences that justify the use of covert coercive measures are listed in the provision and include serious crimes such as terrorist offences and unlawful intelligence activities. The courts can authorise the use of coercive measures for up to six months at a time, cf. the Police Act Section 17 e first paragraph. This is longer than the period for which the use of coercive measures is permitted for investigation purposes.[9] The justification for this is that preventive work often has a longer time horizon than corresponding use of coercive measures in an investigation.

4.2.2 The execution of the investigation

The Committee has investigated the outcomes of PST's petitions to the court for authorisation to use covert coercive measures in prevention cases and investigation cases, including averting investigation. The investigation was based on all Oslo District Court's rulings concerning use of covert coercive measures in counterintelligence and counterterrorism cases during a limited period of time in recent years. The Committee has also looked at comments and any appeals filed by official counsel. Lawyers appointed as official counsel are tasked with safeguarding the interests of a person targeted by the coercive measures without communicating with the person in question. They are also tasked with safeguarding the interests of third parties.

4.2.3 Findings from the investigation

Of the petitions that form the basis for the rulings reviewed in the course of the investigation, 91 per cent related to PST's preventive work. The intention expressed in the preparatory works to the Police Act Section 17 d was to give the service permission to use covert coercive measures 'to a very limited extent' in its preventive work.[10] During the Storting's consideration of the bill, it was stated that the strict conditions would make the use of covert coercive measures in prevention cases a safety valve, to be used only if the rules for investigations could not be applied.[11]

PST has asked the Committee to include the service's comments to the investigation into PST's use of covert coercive measures in its annual report. The letter has been included as Appendix 2.

9 See, for example, the Criminal Procedure Act Section 202 a sixth paragraph, which states that video surveillance may be permitted for a maximum of four weeks at a time.

10 Proposition No 60 to the Odelsting (2004–2005) pp. 12 and 112.

11 Recommendation No 113 to the Odelsting (2004–2005) p. 35.

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.

Official counsel
When the courts consider and rule in cases concerning the use of covert coercive measures or investigative steps for preventive or averting purposes, the suspected person is entitled to have an official counsel appointed pursuant to Criminal Procedure Act Section 100 a first paragraph.

4.2.4 Observations regarding the official counsel arrangement

The Committee notes that the official counsel have submitted few objections to the petitions. In 84 per cent of cases, the official counsel had no objections.[12] Only in 6 per cent of the cases did they object to the petition as a whole. Partial objections were submitted in only 10 per cent of cases. The objections filed concerned the duration of the authorisation for use of coercive measures or that such use constituted a disproportionate interference, for instance due to third parties being affected.

Appeals were filed against two per cent of the district court decisions. In one case, PST appealed because the service was of the opinion that the period for which the district court had authorised the use of the coercive measure, was too short. The court of appeal found in favour of the service. The remaining appeals were filed by the official counsel. These concerned matters such as whether the use of coercive measures was in breach with the prohibition against audio surveillance of private homes, the duration of the use of coercive measures and insufficient specific information to justify the use of coercive measures. Several of the appeals concerned minors. The appeals from the official counsel did not succeed in any of the cases investigated.

The investigation showed that the requirement stipulated in the Criminal Procedure Act Section 100 a that, if possible, the same lawyer should be appointed when PST requests extended duration or more extensive use of coercive measures, was rarely met.

4.3 Use of covert coercive measures

4.3.1 Elucidation of court decisions and the establishment of an experience archive

The information that form the basis for the court's decision when the service requests authorisation for the use of covert coercive measures, is presented by PST. Much of the underlying documentation is withheld as it is deemed to be sensitive. This imposes a great responsibility on the service to ensure that the cases are sufficiently elucidated. The Committee considers it to be of fundamental importance to due process protection that PST describes the facts of a case as far as possible in unclassified form, clarifies uncertainties and distinguishes clearly between opinions and facts. In 2025, the Committee looked into whether the service's guidelines for these cases safeguard such considerations, and found no reason to criticise PST.

The EOS Committee used to manage an experience archive of previous court decisions for the use of official counsel and judges. This archive was discontinued in 2006 because it was not much used and its upkeep required a lot of PST's resources.[13]

In response to a question from the Committee, PST stated that it had undertaken work in 2025 to put in place an updated, comprehensive experience archive of security cases for the use of official counsel and judges. The courts had requested such an archive, and the work took place in continuous dialogue with the courts. The Committee stated that the parties having access to relevant and up-to-date information is a prerequisite for an elucidated legal process. The PST's efforts to put such a resource in place constituted an important contribution to due process protection in these cases.

4.3.2 Inadequate information to the courts on the use of covert video surveillance

The Committee regularly requests access to court decisions in cases where PST has received authorisation for covert video surveillance. The Committee also asks to see images showing the camera angle used in the surveillance.

In one case, the Committee found that the camera angle included a social meeting place which was not mentioned in the decision. PST stated that it was necessary to include the social meeting place, and explained why in its response to the Committee. However, the petition that was submitted to the

12 A corresponding investigation conducted in 2006 into investigation cases showed that counsel objected to the petition in 45 per cent of cases.

13 See Document No 20 (2006–2007) p. 8.

Security cases
Security cases are cases that concern fundamental national interests. This includes rulings concerning whether PST is permitted to use covert coercive measures for investigative, preventive or averting purposes, as well as rulings to deny access to information pursuant to the Criminal Procedure Act Section 242.

court by PST contained no information that the social meeting place was included. Nor did it provide an explanation as to why PST considered this necessary. Lacking this information, the court could not make a just assessment of whether it was necessary and proportionate to include the social meeting place in the video surveillance or not. The Committee criticised PST for providing inadequate information to the court.

4.3.3 Use of covert audio recording of conversations in which the services themselves take part

The Committee has considered whether PST and the NIS have a sufficient basis in the Police Register Act and the Intelligence Service Act, respectively, for using covert audio recording of conversations in which the services themselves take part. The recordings in question are based on security considerations or intended to provide documentation and fulfil information quality requirements.

It is not a criminal offence to make covert audio recordings of conversations in which oneself participates, cf. the Criminal Procedure Act Section 205 first paragraph letter a. The authorities, however, cannot use covert audio recordings of conversations with private individuals based on general freedom of action, as this constitutes an infringement on individuals' right to privacy that requires a basis in law, cf. the Norwegian Constitution Article 113.

The Committee concluded that the rules governing PST's processing seemed to be sufficiently clear, accessible and predictable to allow covert audio recordings in cases as mentioned above, provided the use had a legitimate purpose and was not disproportionately intrusive in the case in question.

4.4 Processing of lawyer – client communication

The Committee found that PST had failed to fulfil its duty to delete information about conversations between lawyers and clients obtained through lawful interception.

The Committee discovered metadata linked to hundreds of conversations between lawyers and their clients registered along with metadata linked to communication between doctors and their patients. One occurrence of registered health data related to conversations with public sector employees was also discovered by the Committee.

The Criminal Procedure Act Sections 117–120 and 122 contains exceptions from a witness' duty to give information on these types of data, also referred to as prohibition against giving evidence. The Committee criticised PST for being in breach of the prohibition against seizure and duty of deletion pursuant to the Criminal Procedure Act Sections 204 and 216 g second paragraph. In December 2025, PST informed the Committee that the information in question had been deleted.

4.5 Collection and disclosure of information about a Norwegian citizen by PST and the NIS

PST has legal authority to disclose information to foreign services to avert or prevent criminal offences, or if it is necessary in order to verify the information. PST is required to assess the necessity and proportionality of such disclosures in advance, and certain other conditions must be met. The assessment shall particularly consider whether the information is 'communicated to a recipient subject to a duty of confidentiality, what use the recipient can be expected to make of the information and whether there is uncertainty associated with the information due to its nature or source'.[14]

PST disclosed information about a Norwegian citizen to a foreign service on the condition that the information shared was only to be used for intelligence purposes. The service deemed the disclosure necessary, relevant and proportionate in the case in question, and was of the view that the advance assessments of any human rights consequences had been sufficiently thorough.

Information in the case suggested that the foreign service did not comply with the conditions stipulated for the disclosure by PST. The Committee expressed reasonable doubts regarding whether the service's proportionality assessment had been sufficiently thorough. These doubts concerned assessment of risk reduction measures and what use the receiving service could be expected to make of the information disclosed. Previous critical remarks by the Committee regarding the exchange of information and cooperation with the foreign service in question, were among the factors taken into consideration.[15]

It was the NIS that communicated the information from PST to the foreign service. In the same case, the Committee asked the NIS to provide an account of the service's contact with the foreign service, see section 3.4.

4.6 Collaboration and exchange of information between PST and Norwegian Customs

The Committee oversees the EOS services' exchange of information with other public authorities. In 2025, the Committee questioned Norwegian Customs' disclosure of ANPR data from the agency's number plate recognition system to PST with reference to an incorrect basis in law. When Norwegian Customs disclosed the data, the agency referred to its general right to disclose data to public authorities and not to the special provision concerning ANPR data, which is stricter.[16] ANPR data are considered personal data because they can be linked to the owner of the vehicle. As a rule, ANPR data are not to be disclosed to other public authorities unless specific conditions are met and Norwegian Customs has conducted a concrete proportionality assessment of the disclosure. The Committee stated to Norwegian Customs that it disagreed with the agency's assessment that its right to share ANPR data was as extensive as its right to disclose other information to the police and PST within Norwegian Customs' administrative area.[17]. The Committee also stated that outside Norwegian Customs' administrative area, a concrete proportionality assessment is required before sharing APNR data with PST. The Committee informed PST of its opinion.

4.7 Failure to review registered personal data

PST is to review and reconsider the need to keep information registered by the service as part of its preventive activities, outside prevention cases, when five years have passed since the time of registration.[18] This applies when no new information about the person in question has been registered during the five-year period. In the course of its oversight, the Committee has repeatedly found non-conformities in PST's compliance with the requirement for review.[19] Several of these non-conformities were due to faults in or a lack of

14 See the Police Register Act Section 27 third paragraph, cf. Section 22 first paragraph final sentence, cf. the Police Register Regulation Section 9-9 third and fourth paragraphs.

15 See the EOS Committee's annual report for 2020 section 4.2 pages 18–19.

16 When disclosing the information, Norwegian Customs referred to the Movement of Goods Regulation Section 7-11-1 subsection 2 letter f second sentence. The correct legal basis is the Movement of Goods Regulation Section 8-9-1 first paragraph letter f second sentence. The texts under letter f of the two provisions are identical, but their starting point differ.

17 Norwegian Customs' administrative area comprises the regulatory framework for customs and the cross-border movement of goods, and includes preventing illegal and dangerous good such as drugs and weapons from being brought into Norway.

18 Cf. the Police Register Regulation Section 22-3 third paragraph first sentence.

19 See, for example, the EOS Committee's annual reports for 2013–2017, 2021 and 2024.

ANPR
Automatic number plate recognition (ANPR) is used to monitor and collect information about transborder traffic on roads and ferry terminals, and the Movement of Goods Act Section 8-9 provides the legal basis for its use.

sufficient digital tools to facilitate compliance with regulatory requirements.

During an inspection in May 2025, PST demonstrated an oversight function in one of its systems to the Committee. It included a script listing registrations that had not been reviewed in accordance with the five-year rule. The demonstration showed that, at the time of the inspection, more than 6,500 registrations were overdue for review. In August 2025, in response to a question from the Committee, PST informed the Committee that it had implemented measures and reduced the number of registrations overdue for review to 2,000. The Committee nevertheless found that the number of non-conformities warranted criticism and stated that without regular reviews, there is a high risk that information will be stored for longer than required in violation of the Police Register Act Section 50. PST put in place an automatic solution in the autumn that helped to simplify the work of identifying registrations that are due for review. In December 2025, PST informed the Committee that the service was up to date with its reviews.

Faults in the digital solution was also the reason for a non-conformity that PST informed the Committee about in 2023, involving a considerable number of positive contacts not being reviewed. The Committee criticised PST for this non-conformity and for the service's internal procedures not complying with the regulatory requirements on this point. In autumn 2024, the Committee checked whether the service had rectified the non-conformity following the Committee's criticism. This resulted in PST identifying another fault in its technical solution that caused positive contacts to still not be reviewed in accordance with the regulatory requirements.

The service's internal procedures remained unchanged. When concluding the case in 2025, the Committee criticised PST for the new non-conformity identified as well as for not having changed its internal procedures. The Committee expected PST to make sure that the changes implemented to satisfy the statutory requirements actually worked. PST stated that the non-conformity had been rectified and that the service's internal procedures would be revised.

In 2025, the Committee's oversight activities identified new cases of registrations of deceased persons not having been reviewed. In 2016, the Committee criticised PST for failing to conduct reviews and for having processed data about registered persons for several years after their death without this being necessary. At the time, PST stated that the service was working on a technical solution to ensure that registrations would be reviewed shortly after the service received information about the death of a registered person. A new script intended to resolve this problem was introduced on 1 January 2017. In 2025, when the Committee asked about the new cases of registrations of deceased persons that had not been reviewed, PST stated that these non-conformities were caused partly by incorrect registration and partly by a fault in the above-mentioned script. The fault caused information about deceased persons not to be flagged for review when a death was confirmed. The Committee once again criticised the service, but noted that PST had identified the source of the problem and rectified faults. The Committee expected that PST would investigate whether the faults had affected more registrations than those specifically raised by the Committee.

4.8 Disclosure of information subject to access restrictions on PST's intranet

PST published an article on its intranet containing information originating from the service's handling of a former source. Access to such information should be restricted and the information subject to strict access control within PST.

The information was disclosed without a legal basis, and the disclosure constituted a personal data protection non-conformity. The Committee raised the special protection that applies to source information. PST was criticised for breach of both the regulation on restriction of access to source information and the internal confidentiality regulation concerning 'someone's personal matters' and special categories of personal data pursuant to the Police Register Act Section 7. The Committee expected that PST removed the information from its intranet and implemented measures to reduce the risk of negative consequences for the service's former source.

PST stated that the service took the non-conformity seriously and that the lessons learned would be applied in the service's ongoing internal control activities.

Two months after receiving this statement, the Committee discovered that the article was still available on the intranet

Script
A program used regularly to find a certain type of information or make regular lists. For example, it could be used to identify registrations that are due for manual review under the PST's five-year rule or produce statistics concerning various types of information or activities.

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

and raised the matter with PST. The Committee emphasised that it expects the service to act quickly to follow up serious non-conformities.

In a new response, PST stated that it had taken down the article in question shortly after the Committee's subsequent oversight and also undertaken a comprehensive and thorough review of all similar articles to make sure that they did not contain source information. The service has subsequently informed the Committee that technological challenges encountered in the process caused the delay in rectifying the matter that warranted criticism.

4.9 Non-conformity management

For the benefit of the oversight, PST regularly informs the Committee about non-conformities identified by the service itself and their follow-up. During an inspection in 2024, PST informed the Committee of two non-conformities related to the use of covert coercive measures that the Committee found reason to ask more detailed questions about.

In one of the cases, PST had initiated audio surveillance of several persons on the basis of an urgent decision that applied to the collection of historical traffic data only. The service's internal decisionmaker was notified of the non-conformity too late, and the necessary immediate measures were therefore not implemented until the following day.

In the other case, historical traffic data was collected from a person not covered by the urgent decision. Even after identifying the error, it took the service more than two months to rectify it and process the information in accordance with the requirements set out in the Police Register Act.

The Committee criticised PST for its management of both non-conformities.

4.10 PST's security clearance authority

4.10.1 Connection to certain countries

The Committee has investigated PST's processing of security clearance cases in which connection to countries of considerable importance to Norwegian security interests[20] was among the factors taken into consideration.

Security clearance may only be granted if there are no grounds for doubting that the person concerned is suited for security clearance. In the suitability assessment, matters relevant to evaluating the reliability, loyalty and sound judgement of the person concerned are assessed.

In its investigation, the Committee discovered that the grounds given by PST in some cases placed particular emphasis on the vetted person's tasks being of importance to PST's operational capabilities. The Committee stated that considerations of operational capabilities in themselves are not to be a factor in the assessment of granting a person security clearance. In the Committee's opinion, emphasising the needs of the service as an independent factor could lead to a higher risk acceptance in connection with security clearance, as well as to unwarranted differential treatment. PST informed the Committee that the security clearance authority had corrected its practice since the cases in question were decided.

The Committee expected PST to set necessary conditions for security clearance in cases where a certain risk involved in granting a person security clearance could be reduced by internal circumstances within PST. One such condition could be for the security clearance to be restricted to a certain position, or an assignment, for PST.

The Security Act Section 8-4 fourth paragraph letter m states that 'inability to perform satisfactory vetting' may be given weight when determining whether security clearance can be granted. In order to use vetting in a security clearance case, the security clearance authority must have access to registered information about the person in question covering the past ten years.

The investigation revealed weaknesses in PST's practice when it comes to elucidating cases where the personal history

20 NSM prepares security assessments of the importance of relevant states to Norwegian security interests in clearance cases, cf. the Security Clearance Regulation Section 18. The Committee's investigation covered three of the states specifically mentioned in PST's National Threat Assessment: Russia, China and Iran.

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

was incomplete. In two cases, PST had neither obtained further details from the persons being vetted nor conducted a security interview to learn more about their stays abroad. The investigation showed that PST accepted a higher level of risk associated with incomplete personal history compared to other security clearance authorities, despite the fact that the service grants the highest level of security clearance.

The Committee urged PST to implement measures ensuring the processing of cases concerning persons who have stayed in countries of considerable importance to Norwegian security interests in the past ten years complies with the Security Act's requirements for elucidation of cases and includes adequate assessment of the persons' suitability for security clearance.

The investigation also showed that PST did not sufficiently elucidate all of its security clearance cases and that there were shortcomings in PST's documentation of the assessments made. The Committee noted that PST had implemented measures to clarify their assessments, and emphasised the elucidation of cases and documentation of assessments in writing as key elements in ensuring due process protection and verifiability in the processing of security clearance cases.

PST agreed and stated that the security clearance authority had corrected its practice in the time since the cases in question were decided. PST implemented a practice memo to address the considerations pointed out in the Committee's statement.

4.10.2 Information from PST in security clearance cases

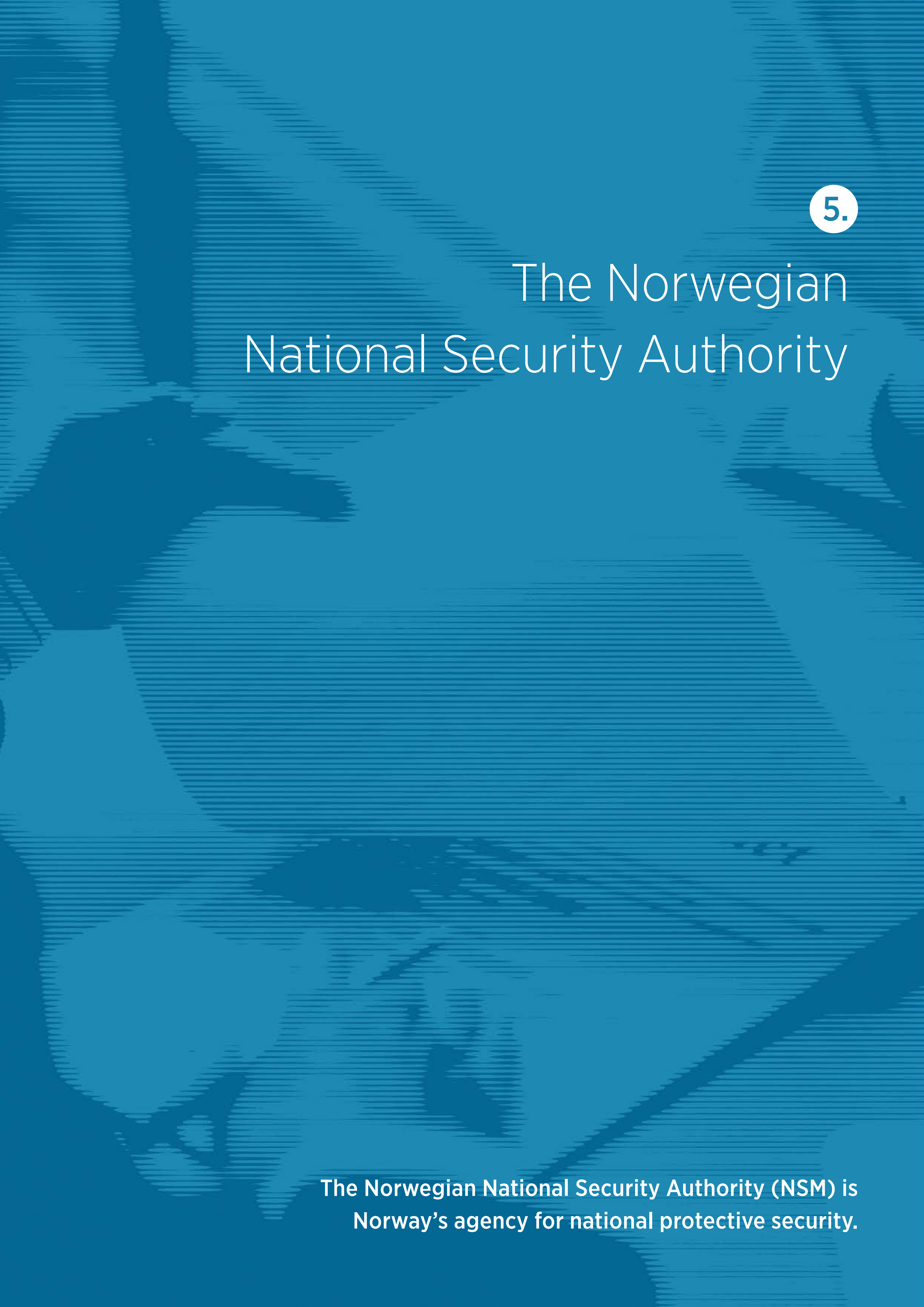
The National Security Authority (NSM) can obtain information from PST as part of its vetting process when considering a security clearance case. The outcome of the vetting is a factor in the overall assessment that the security clearance authority conducts pursuant to the Security Act Section § 8-4. When disclosing information, the Police Register Regulation Section 11-3 first paragraph requires PST to make sure, as far as possible, whether the 'information is correct, sufficient and up to date.

In one case, the Committee found that PST had provided an incomplete assessment of the person concerned. The information was registered some time ago. The Committee stated that the service should have provided information about the time of the last registration and about the person's subsequent development. The Committee emphasised how important it is that information provided by PST in security clearance cases is sufficient and up to date.

4.11 Complaint cases

The Committee has accepted 22 complaints against PST for consideration in 2025. Some of these complaints concerned more than one of the EOS services. The Committee concluded 18 complaint cases against PST in 2025 and expressed criticism against PST in one of them.

In one case, the Committee proposed that the complainant should be given a more detailed explanation in accordance with the Oversight Act Section 15 first paragraph fourth sentence. PST did not comply. The service's decision regarding classification of information is binding on the Committee, cf. the Oversight Act Section 11 third paragraph.



5.

The Norwegian National Security Authority

The Norwegian National Security Authority (NSM) is Norway's agency for national protective security.

5.1 General information about the oversight

The Committee focused on general principles of administrative law and case processing rules in its oversight of NSM in 2025. The Committee conducted two inspections of NSM in 2025, one of NSM's security clearance authority and one of the 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.

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.

5.2 Work on facility security clearances

The Committee was briefed on NSM's work on facility security clearances during its inspection of the security clearance authority in 2025. Afterwards, the Committee requested a written account.

Facility security clearance is a measure used in connection with classified procurements, for the purpose of ensuring control of and confidence in suppliers of goods or services that could have a bearing on national security. The number of facility security clearance cases has increased significantly in 2025, from 13 to 17 cases a year during the period 2022–2024 to 69 cases in 2025. The average case processing time increased from 349 days in 2023 to 531 days in 2025. Of the cases whose processing was concluded in 2025, 40 per cent were dropped because the facility security clearance was no longer needed. NSM has informed the Committee that there is some uncertainty associated with these figures.

The Committee advised NSM that the long case processing times and the backlog that accumulated in 2025 concerned the Committee.

The security clearance system must balance the important considerations of due process protection and national security. Long case processing times in facility security clearance cases could be detrimental to both these considerations, and could be problematic both for entities that need to make a classified procurement and for potential suppliers. It is particularly problematic if the reason for requests for security clearance being withdrawn is that the case processing takes too long. The purpose of the Committee's oversight is to ascertain whether rights are violated and to prevent such violations. Case processing times as shown above could affect the interests and rights of individual enterprises as well as harm the interests of society. The Committee stated that the present situation could require it to assess whether these circumstances unduly harm the interests of society, cf. the Oversight Act Section 2 first paragraph (2).

Based on the above, NSM was early in the second quarter of 2026 asked to brief the Committee on the status of the backlog and concluded facility security clearance cases, specifying the outcomes and average case processing times. Due to the seriousness of the case, the Committee informed the Ministry of Justice and Public Security of its statement.

5.3 Investigation of the security clearance authorities' use of clearance on conditions concerning to travel

5.3.1 Differences in practice in wording and restrictions

In some cases, security clearance may be granted subject to specific conditions, cf. the Security Act Section 8-6. The conditions set should be aimed at reducing the risk associated with granting the person in question a security clearance.

An investigation conducted by the EOS Committee in 2025 found that practices differ between security clearance authorities when it comes to conditions concerning travel.

A review of 172 cases from the Norwegian Civil Security Clearance Authority (SKM), FSA, PST and the NIS showed the following:

i. two security clearance authorities mainly set conditions imposing a duty to notify them of travel to specific countries, while the other two phrased their conditions as a travel ban
ii. two security clearance authorities set conditions that applied only to the person granted security clearance, while the conditions set by the other two also covered the travel activities of close relatives/family.

Statements that the Committee requested from the security clearance authorities showed that there were no grounds to warrant the differences in the conditions set for travel. The Committee nonetheless found the categories of conditions applied to be within what the law permits.

In response to a question from the Committee, NSM, which is the expert authority for security clearance matters, stated that the directorate had also noted differences in practice. In 2025, NSM therefore prepared a manual on the use of conditions for security clearance and access clearance with a view to reducing unwarranted differences in the conditions applied.

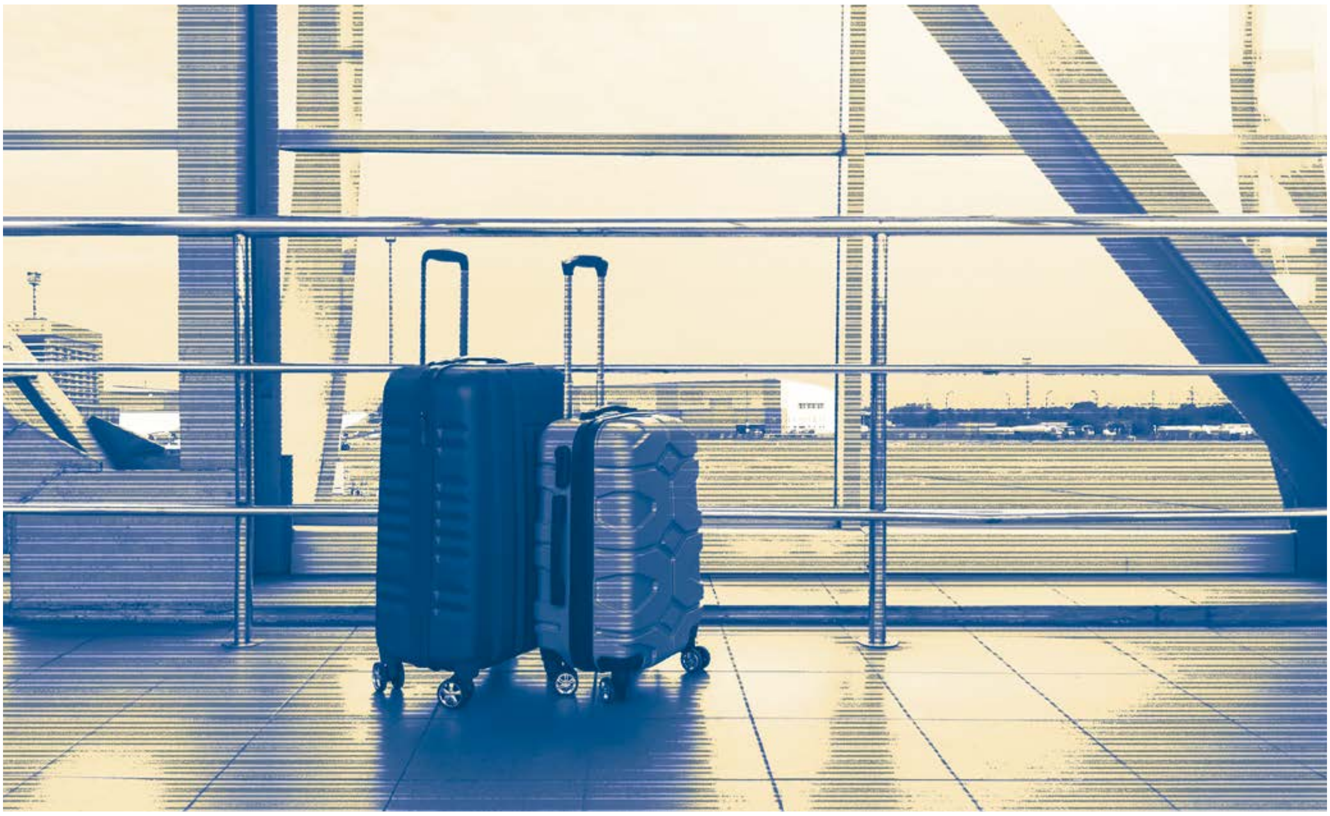
Variation between security clearance authorities in terms of case processing and outcomes could be detrimental to the due process protection of the persons concerned.[21] The Committee therefore emphasised the importance of NSM promoting consistent practice in the use of conditions in security clearance going forward. The Committee encouraged the security clearance authorities to engage in dialogue about the use of conditions at a general level so that the thresholds for applying different types of conditions can be coordinated.

5.3.2 Duty to give notice and notification

The EOS Committee's investigation also gave reason to comment on the relationship between the duty to give notice and the condition of notification in connection with travel, as well as the level of precision for conditions that apply to close relations/family.

One security clearance authority referred to the Security Act Section 8-11 and considered that, as a general rule, a duty to provide notification if the person concerned, or persons closely related to them, travel to states of a certain importance to Norwegian security interests is a direct consequence of security clearance and authorisation. Neither NSM nor the Committee agreed with this interpretation. According to the Security Act Section 8-11, it is up to the person in question to determine whether circumstances are relevant to their suitability to hold security clearance. The person granted security clearance has no such discretion in cases where the duty to give notice is set out in the form of a condition. The Committee stated that, in order to eliminate uncertainty and improve predictability, a duty to give notice should only be set as a condition for security clearance if information about such travel is necessary to hold a security clearance.

Another security clearance authority had in some cases worded the conditions in such a manner that it was unclear to whom they applied. According to these conditions, the



21 Cf. the Oversight Act Section 2.1.

Access clearance
An access clearance grants access to critical national objects and infrastructure.

person vetted was to give notice if persons closely related to them, 'family members' etc. wished to travel to specific countries. The Committee questioned whether this was a sufficiently precise definition of the group of persons to whom the conditions applied. The security clearance authority realised that the phrasing could be misunderstood and cause uncertainty about who it referred to. The security clearance authority stated that it would change its practice to clarify to whom the conditions applied. The Commission endorsed this assessment.

5.4 The right to process a new request for security clearance in parallel with an appeal case

During an inspection in 2024, the Committee identified ten cases where the quarantine period had expired before NSM had processed the appeal. In these cases, the persons concerned withdrew their appeal in order to allow for another request for security clearance to be considered.

This raises the question of whether the right of individuals to have public administration cases considered in two tiers is safeguarded when the case processing drags on and this prevents or delays the processing of a new request for security clearance.

NSM has stated that new requests for security clearance cannot be accepted for processing if the person concerned has an appeal pending. This rule applied even if the quarantine period in the appeal case had expired. The grounds given by NSM was that a person can only have one case on the same issue processed by the public administration at any one time.

The Committee did not agree with the view that all new request for security clearance submitted while an appeal case was under consideration were to be considered part of the same case. The Committee referred to the fact that the requests for security clearance could concern different levels of security clearance, different entities and different scopes of access to critical information. Personal matters with a bearing on a person's suitability for security clearance could also have changed.

The Committee considered there was no legal basis for rejecting new requests for security clearance or putting them on hold as a general rule simply because a person had a security clearance case under consideration by the appellate body. This would have to be assessed on a case-by-case basis.

The Committee stated that many had already waited a long time for the outcome of their appeal case, with no real option to put their employer's request for security clearance for them on hold, by persisting with their appeal. Under the circumstances, to withdraw their appeal might feel as their only option, with the consequence of them loosing their opportunity to have their appeal reviewed. This could be detrimental to individuals' due process protection.

The Committee asked NSM to review its interpretation of the law to ensure that no one suffers a wrongful loss of legal rights and to provide guidance to the security clearance authorities on how to deal with new requests for security clearance.

Quarantine period
If security clearance is not granted for the level requested, the security clearance authority shall set a quarantine period of up to five years. The person may not be assessed for security clearance again until the quarantine period has expired.

NSM agreed that there is no clear legal basis for rejecting new requests. NSM will provide guidance to the security clearance authorities instructing them to make a concrete assessment of whether new requests can be accepted for processing or must be put on hold.

5.5 The right to share information from VDI and non-conformity management

The Committee has considered the legal basis for sharing information from the national warning system for digital infrastructure (VDI) pursuant to the Security of Undertakings Regulation Section 65 second paragraph.[22] Neither the Security Act Section 2-4 nor the regulation explicitly state that information can be shared with foreign authorities and international organisations when handling a specific incident in VDI. By comparison, the NIS and PST have a clear legal basis to share information in the Intelligence Service Act Section 10-3 and the the Police Register Act Section 22.

The Committee referred to the fact that the Norwegian Constitution Article 102 and the European Convention on Human Rights Article 8 require a clear, accessible and predict able basis in law to justify interference with the protection of privacy. In the Committee's opinion, the Security of Undertakings Regulation Section 65 second paragraph does not in its present form provide a sufficiently clear basis for sharing information with foreign authorities and international organisations. The Committee asked NSM to inform the Ministry of Justice and Public Security of this.

The Committee also criticised NSM for its management of a non-conformity related to VDI. Several VDI members had used a specific technical solution where, as a result of this non-conformity, personal data that should not have been there were found in VDI. NSM dealt with the case as a non-conformity, deleted the personal data and notified the provider of the solution in question. The VDI members affected were not notified. NSM stated that the directorate had refrained from notifying the members due to low capacity.

The Committee pointed out that the object of non-conformity management is to re-establish a normal state, eliminate the cause of the non-conformity and prevent it from recurring. The purpose of non-conformity management thus indicates that the VDI members should have been notified of the issue, so that they could consider whether they needed to implement measures in their own systems. If NSM did not have the capacity to notify them when the non-conformity was identified, the undertakings should have been notified shortly thereafter.

5.6 Complaint cases

5.6.1 Introduction

The Committee has accepted five complaints against NSM for consideration in 2025. Four of the complaint cases concerned security clearance issues and one concerned surveillance. Some of these complaints concerned more than one of the services.

The Committee concluded seven complaint cases against NSM in 2025 and criticised NSM in four of them.

5.6.2 Insufficient elucidation and information

In a complaint case concerning security clearance, the Committee criticised NSM for several case processing errors.

The Committee found that NSM had included information about the vetted person's lawful social engagement in the assessment of suitability for security clearance. This is in breach of the Security Act Section 8-4 fifth paragraph and Section 8-5 seventh paragraph. The Committee also regarded that NSM had not fulfilled its duty to ensure the security clearance case had been sufficiently elucidated. Relevant circumstances with a bearing on the complainant's suitability for security clearance had not been taken into consideration. No attempt had been made to clarify what the security clearance authority described as 'apparent inconsistencies' in statements provided to the Norwegian authorities by the complainant. Key circumstances with a bearing on the outcome of the case had been emphasised as negative factors, without sufficient clarification.

In the Committee's opinion, NSM should have conducted a security interview with the complainant to elucidate the case. NSM was also criticised for not having given the complainant sufficient information on factors counting in the complainant's disfavour and for limiting the information given further than permitted under the Security Act. The Committee stated that NSM should reconsider the security clearance case.

NSM disagreed.

The Committee took note of NSM's reply, but pointed out that the unwillingness to comply with its criticism seemed to conflict with the Storting's assumption that the EOS services would follow up criticism and recommendations made by the EOS Committee.[23]

22 The Security of Undertakings Regulation Section 63 states that NSM shall operate the warning system. The VDI system consists of sensors deployed with undertakings in order to identify and give warning of cyber-operations targeting critical Norwegian infrastructure or functions.

23 Recommendation No 418 to the Storting (2016–2017), page 18.

After reassessing the matter, NSM stated it would reconsider the case. NSM has later informed the Committee that the outcome of the case remained the same following its reconsideration.

5.6.3 Denied access and delay to a security clearance case caused by a request for a specifically appointed lawyer

In one complaint case concerning security clearance, the Committee criticised SKM and NSM for having denied access to a summary of the security interview. The Committee criticised NSM for the same thing in 2024.[24]

The Committee pointed out that it was highly unfortunate that the time taken to process the vetted person's request for a specifically appointed lawyer had delayed the consideration of the appeal approximately nine months. This delay came in addition to what was already a long case processing time.

5.6.4 Long case processing times

The other complaints against NSM concerned long case processing times.

In one of the cases the Committee had already strongly criticised NSM for the long case processing time.[25] Another four months elapsed from the Committee's initial criticism until a final decision was reached. A total of two years and three months passed from NSM received the case until it was concluded. NSM explained this by referring to its considerable backlog. The Committee criticised NSM for the long case processing time. SKM was criticised in the same case for giving inadequate access to information, see section 8.2.

In another case, NSM took twelve months to consider a second-tier appeal in a security clearance case. NSM explained the time spent by referring to the need to carry out examinations whilst considering the case and review documentation, along with the complexity of the case.

The Committee criticised NSM for the long case processing time. SKM was also criticised for the long case processing time in this case, see section 7.2.

5.7 Case processing times in NSM's security clearance cases

The case processing time for cases concerning requests for security clearance has increased in NSM in 2025. This in spite of the case category being transferred to SKM with effect from 1 May 2024.

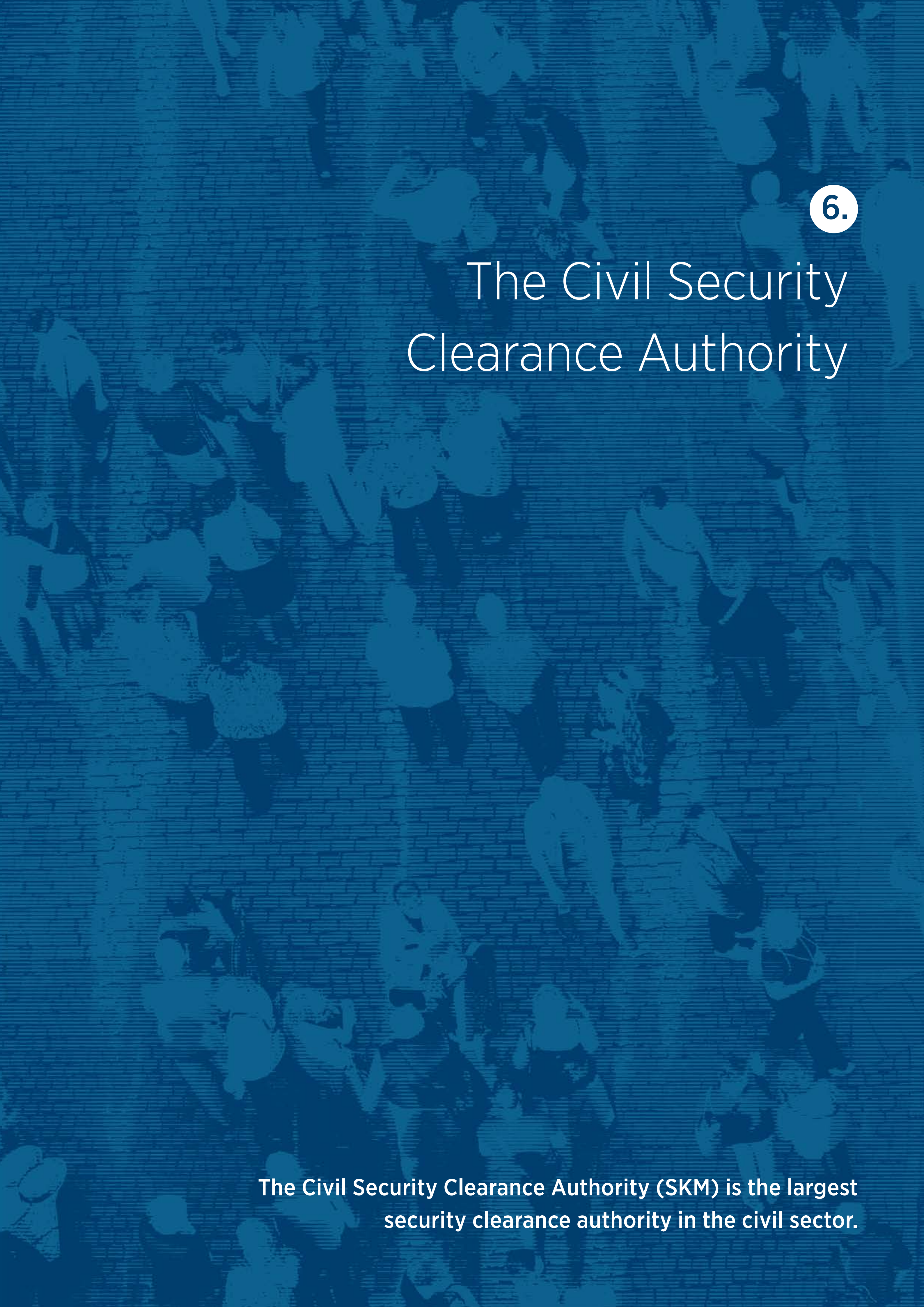
The average case processing time in cases concerning access to information has increased significantly, from 22 days for seven cases in 2024 to 57 days for 18 cases in 2025. This far exceeds NSM's internal deadline of eight days. In the Committee's opinion, these times are unacceptably long.

Below is a table of case processing times for 2025 as provided by NSM.

NSM	AVERAGE CASE PROCESSING TIME			
	Positive decisions		Negative decisions	
	2025	2024	2025	2024
Request for security clearance	311 days (3 cases)	149 days (62 cases)	294 days (2 cases)	249 days (8 cases)
Request for access clearance	-	-	712 days (2 cases)	-
First-tier appeals	-	-	24 days (1 case)	644 days (1 case)
Second-tier appeals	246 days (4 cases)	464 days (16 cases)	158 days (50 cases)	421 days (114 cases)

24 See section 6.3.2 in the annual report for 2024.

25 See section 6.3 in the annual report for 2023.



6.

The Civil Security Clearance Authority

The Civil Security Clearance Authority (SKM) is the largest security clearance authority in the civil sector.

6.1 General information about the oversight

The Committee conducted one inspection of SKM in 2025. The main focus of the inspection was case processing rules and the general principles of administrative law.

The Committee also conducted an investigation in 2025 into SKM's conditions concerning travel, see section 5.3.

6.2 Complaint cases

The Committee received three complaints against SKM in 2025. One of these complaints concerned more than one of the EOS services. The Committee concluded four complaint cases against SKM in 2025 and expressed criticism in all of them.

In two of the cases, the Committee criticised SKM for having denied the vetted person access to the written summary of the security interview. In one case, SKM was also criticised for having denied access to SKM's summaries of documents that the vetted person had shared with SKM during the security interview. SKM made reference to guidelines issued by NSM and justified the exemptions from access by stating that the summaries could reveal information about the security clearance authorities' methods and reveal circumstances 'which are relevant to national security interests', cf. the Security Act Section 8-4 second paragraph, cf. Section 8-13 second paragraph letter a.

According to the Security Act Section 8-14, a person who has been assessed for clearance is entitled to examine the case documents, except for certain information and documents as specified in the Act. The Committee realised that a summary could show what the security clearance authorities consider to be relevant information in the security clearance case through the selection of information included. However, the Committee could not see how the summaries in question could reveal information about the security clearance authorities' methods or circumstances relevant to national security interests. The Committee therefore concluded that there was no legal basis for exempting the summaries from access and criticised the service. The Committee has previously levelled similar criticism at NSM.[26]

SKM and NSM were criticised for long case processing times in the same two cases. In one case, this was partly caused by the amount of time taken to process the person being vetted's request for a specifically appointed lawyer, particularly by NSM, see section 5.6.3.

In a third security clearance case, SKM by mistake included information about substance abuse from another person's security clearance case in its notification to the vetted person about the security clearance decision. The Committee found this non-conformity to constitute a matter that warrants criticism. SKM had apologised for the error, corrected the notification of the decision and implemented measures to ensure that such errors would not happen in the future. SKM had also made changes to its internal procedure for review and approval of security clearance and authorisation decisions. The Committee urged SKM to request guidelines from NSM as the expert authority concerning how to deal with the information wrongfully included in the documents in the security clearance case. The Committee expected the consideration of the complaint concerning the issues of the case to be based on the correct facts.

26 The annual report for 2024 section 6.3.2.

The fourth complaint case concerned long case processing time. It took SKM eight months to process a request for security clearance, after which the first-tier appeal took another four and a half months. SKM referred to a large number of incoming cases, internal priorities and a filing error as reasons for the long case processing time. The Committee criticised SKM for the long case processing time.

6.3 Case processing times in SKM's security clearance cases

The average case processing time for requests for access to information has decreased from 12 days for 54 cases in 2024 to 9 days for 48 cases in 2025.

Below is a table of case processing times for 2025 as provided by SKM.[27]

SKM	AVERAGE CASE PROCESSING TIME			
	Positive decisions[28]		Negative decisions[29]	
	2025	2024	2025	2024
Request for security clearance	48 days (7,841 cases)	58 days (7,205 cases)	263 days (274 cases)	363 days (458 cases)
Request for access clearance	60 days (811 cases)	52 days (1,005 cases)	281 days (79 cases)	367 days (101 cases)
First-tier appeals	130 days (5 cases)	92 days (5 cases)	80 days (45 cases)	86 days (48 cases)

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

28 Appellants in first-tier cases whose appeal was granted in part are included under 'positive decisions'.

29 This category covers all cases in which security clearance was not granted as requested. As well as cases where security clearance was denied, this could also include cases where security clearance was granted at a lower level or for a shorter period of time than requested, only for a certain position or subject to other conditions.

7.

The Norwegian Armed Forces Security Department

Photo: Joakim Salmelid / Norwegian Armed Forces – Image effect: Fdesign

The Norwegian Armed Forces Security Department (FSA) has overriding responsibility for the Norwegian Armed Forces' protective security work.

7.1 General information about the oversight

The Committee conducted two inspections of FSA in 2025, one focusing on FSA's processing of security clearance cases and the other on FSA's performance of operational security services. In 2025, the Committee focused on general principles of administrative law and case processing rules in its oversight of FSA as of the other security clearance authorities.

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

In 2024, the Committee criticised FSA for failing to ensure satisfactory progress in security clearance cases concerning persons with a connection to other states being called up for national service. The start of their national service had been deferred for twelve months in order to allow the security clearance authority enough time to process the cases before they report for service. Still the cases were not decided in time.[30] FSA gave an account of a new procedure for processing of such cases that the Committee viewed might help to ensure that these cases were processed in a timely manner.

The Committee requested an updated account of FSA's case processing after the media published several stories in the summer of 2025 about annulments made in individuals call-up for national service due to their security clearance status not being clarified in time. In response to this request, FSA stated that the Armed Forces had annulled call-ups for national service for 115 persons in 2024 and 105 persons in 2025 as a consequence of FSA not having processed their cases in time for them to report to service. The majority of these persons were offered the opportunity to serve in the Armed Forces in another role that did not require a security clearance.

The Committee criticised FSA for the number of annulled call-ups for national service remaining too high, and stated that FSA's lack of overview of procedures introduced to improve case management was unfortunate.

The Committee reiterated the criticism it expressed against FSA on 18 March 2024. The number of security clearance cases not processed in time by FSA indicates in the Committees opinion inadequate case management. The Committee was strengthened in this view by the fact that this remained an issue 18 months after the Committee had pointed it out. The Committee emphasised the importance of satisfactory case processing. Considerations of individual and equal treatment must be safeguarded, and the case processing steps required to elucidate the case must be taken within a reasonable time.

The Committee expressed concern about the persistent security clearance challenges and notified the Ministry of Defence about its statement.

7.3 Complaint cases

The Committee has accepted 15 complaints against FSA for consideration in 2025 and concluded twelve cases. One of the complaints concerned surveillance and more than one service. The case was concluded without criticism of FSA.

The other fourteen complaints concerned security clearance cases. All of the eleven security clearance cases concluded concerned long case processing times and resulted in criticism.

In three of the complaint cases, FSA stated that the cases had been left unassigned after a case officer left. The Committee criticised FSA and, in February 2025, it asked the service to ensure that procedures are in place for progression and reassignment of cases when a case officer leaves. In one of the cases, more than two years had elapsed since FSA received the case. Failure to reassign the case when the case officer left accounted for eight months of inactivity. When the Committee expressed its criticism, the case was still under processing by FSA. In another case, two years and two months elapsed before FSA processed the case and forwarded it to NSM for consideration of the appeal. This case processing time includes three separate periods, with a total duration of one

30 See Appendix 3 to the annual report for 2024, as well as section 7.2.

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

year and five months, during which the case was not being actively processed. The Committee criticised FSA for the unreasonably long case processing time in this case. In the third case, FSA's case processing took more than one year and eight months.

In five other complaint cases where the Committee criticised FSA, the service cited insufficient case processing capacity as the reason for case processing times ranging from nine months up to one year and four months. One case was left in the queue for processing for more than seven months. The case was dropped because the vetted person's job offer was withdrawn as a result of the long case processing time and the security clearance was thus no longer needed. In another case, the Committee criticised FSA for failing to send the complainant preliminary replies and otifications of delays, as well as for the long case processing time.

In one case, the Committee had already criticised FSA for its long case processing time in 2024.[31] The vetted person filed another complaint with the Committee. The Committee stated that although any further case processing time would warrant criticism, a certain threshold must be reached before repeating criticism in the same case. Another five months passed before FSA reached a decision in the case. A total of two years and three months had then elapsed from FSA received the case until the service reached its decision. The Committee repeated its criticism against FSA for the long case processing time.
In another case, eight months passed from FSA received the case until it reached a decision.

In another case, eight months passed from FSA received the case until it reached a decision. The person concerned had then appealed the decision, and twelve months elapsed from FSA received the appeal until the Committee accepted and considered a complaint concerning the case processing time.

The Committee criticised FSA for the long case processing times, both for the processing of the original request for security clearance and the consideration of the appeal against the decision. The case had been left inactive for two separate periods after a case officer left FSA. FSA had yet to complete its processing of the case when the Committee expressed its criticism. The vetted person later filed another complaint with the Committee about long case processing time in the same case. About six and a half months had passed from the Committee's initial criticism until it considered the new complaint. Again the Committee criticised FSA for the long case processing time.

In the final case, FSA had still not reached a decision one year and eleven months after receiving a request for reclearance. Only the initial steps of case processing had been carried out. The Committee criticised FSA for the long case processing time. When the Committee expressed its criticism, the case was still under processing by FSA.

7.4 Case processing times in FSA's security clearance cases

The average case processing time for requests for security clearance has increased significantly in 2025 compared to 2024. The Committee considers this development unacceptable.

The average case processing time for requests for access to information has decreased from 28 days for 16 cases in 2024 to 21 days for 7 cases in 2025.

Below is a table of case processing times for 2025 as provided by FSA.

FSA	AVERAGE CASE PROCESSING TIME			
	Positive decisions		Negative decisions	
	2025	2024	2025	2024
Request for security clearance	63 days (20,935 cases)	55 days (21,192 cases)	406 days (76 cases)	366 days (119 cases)
First-tier appeals	385 days[32] (5 cases)	252 days (1 case)	322 days (14 cases)	140 days (16 cases)

31 See section 7.4 in the annual report for 2024.

32 These positive decisions in 2025 were appeals where the appellate body found partly in favour of the appellant.

8. Oversight of other EOS services

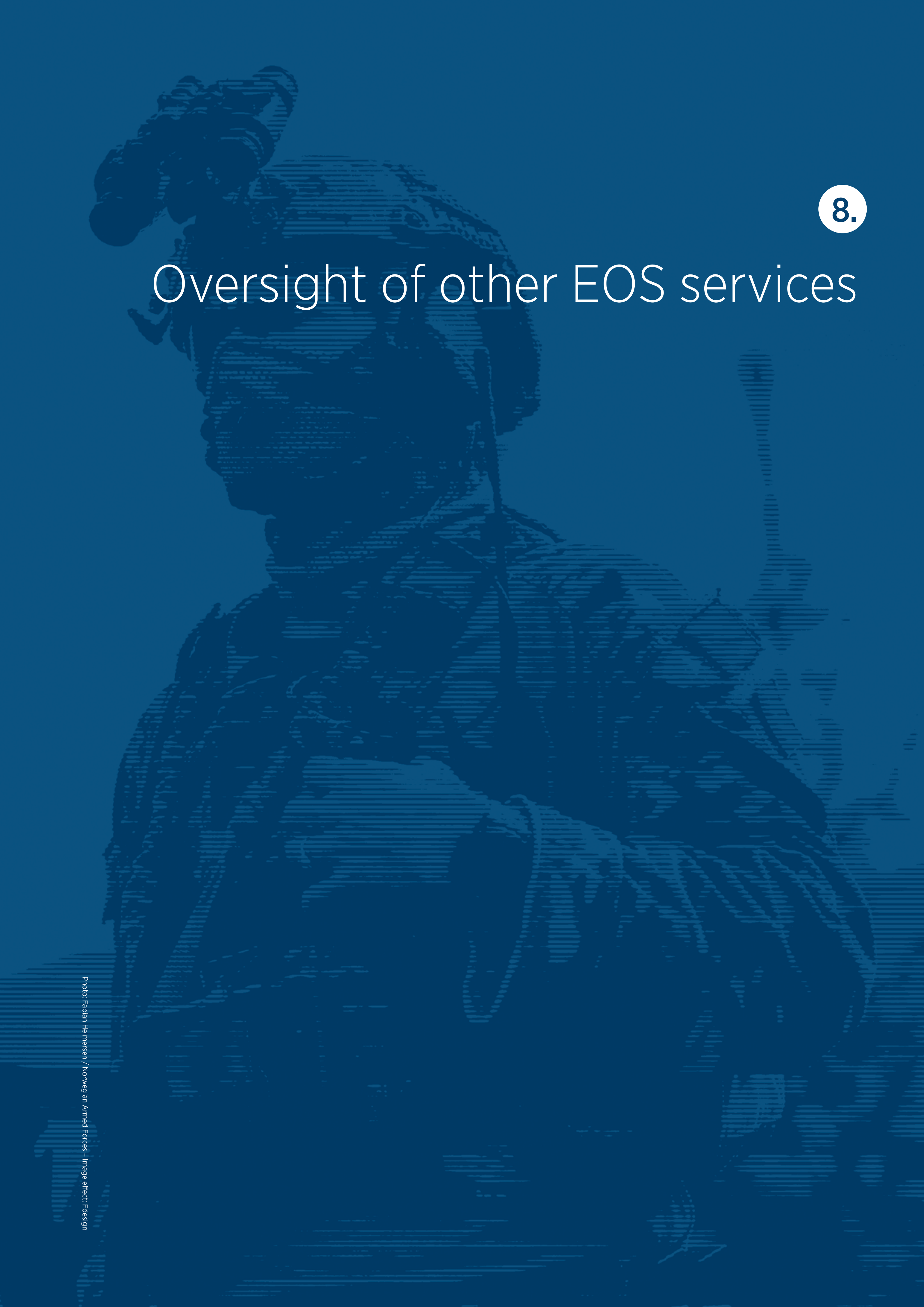


Photo: Fabian Helmersen / Norwegian Armed Forces – Image effect: Fdesign

8.1 General information about the oversight

The Committee's oversight area encompasses all public bodies that carry out intelligence, surveillance or security services. It 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.

The Committee has accepted one complaint against other EOS services for consideration in 2025.

In the complaint case, the Committee levelled criticism at the Ministry of Justice and Public Security for long case processing times. The Committee also criticised SKM and NSM in the same case, see sections 5.6.3 and 7.2.

8.2 The Military Intelligence Regiment

The Army Intelligence Battalion became the Military Intelligence Regiment (*Nordenfjeldske etterretningsregiment*, abbreviated EREG) with effect from 24 April 2025. The Committee inspected EREG in 2025. During the inspection, EREG briefed the Committee about its activities. The inspection did not give grounds for follow-up.

8.3 The Norwegian Armed Forces Special Operations Command

In 2025, the Committee inspected the Norwegian Naval Special Operations Commando in Bergen. The Committee was briefed on the unit's organisation, tasks and capabilities. The inspection did not give grounds for follow-up.

8.4 Legal basis for the Norwegian Armed Forces' use of methods

The Committee has looked into the legal basis for processing of personal data by the Norwegian Armed Forces, except for the Intelligence Service, in connection with exercises and training in Norway. It is clear that the Intelligence Service Act Section 4-6 authorises the NIS to collect information about persons in Norway if strictly necessary for purposes of training, exercises or equipment testing.

Based on responses from the NIS, the Military Intelligence Regiment, the Norwegian Special Operation Forces and the Ministry of Defence, to the Committee's questions, the Committee concluded that the Norwegian Armed Forces units do not have a basis in law for processing personal data in connection with exercises and training without obtaining consent in advance. The Committee considered this a shortcoming in acts or regulations and notified the Ministry of Defence in accordance with the Oversight Act Section 14 third paragraph. The Committee requested a reply from the Ministry.

The Ministry stated that in cases where a legal basis for collecting personal data in connection with training and exercises is deemed necessary, the Armed Forces' practice is based on consent. They make an exception for information collected from open sources, which will, in the Ministry's opinion, not normally constitute interference in relation to individuals and thus require a basis in law. The Ministry also wrote that collection of someone's personal data could nevertheless, based on the circumstances, reach a scope where there is reason to question whether it constitutes interference in relation to the person in question. In the Ministry's opinion, the threshold for it constituting interference would depend on the situation, scope and method used, among other factors. The Ministry wrote in its reply to the Committee that '[it is], however, difficult to specify exactly where to draw the line as regards what constitutes interference in a human rights sense'.

When the Intelligence Service Act was drawn up, the Ministry of Defence acknowledged that information collection from open sources could constitute interference in a human rights sense of the word. The method was enshrined in law to prevent any doubts about whether or not it was legal.

The scope of personal data on the internet, seen in conjunction with technological developments, particularly in the field of artificial intelligence, might lead to collection from open sources constituting an interference with the right to privacy. In the course of its oversight activities, the Committee has come across concrete examples in the Armed Forces that could, in the Committee's assessment, involve such interference.

The Ministry stated in its reply that personal data can also be collected in the course of electronic surveillance, but that such information will be considered surplus information and deleted. The Committee understands this to mean that information is deleted in such cases because the Armed Forces have no basis for processing it.

The Armed Forces need a basis for all processing of personal data. In cases where consent forms the basis for processing, clear requirements apply regarding the quality of the consent. Consent must be freely and actively given. It must be informed, specific and sufficient to cover all of the processing. Informed consent requires the person in question to know the identity of the data controller, what kind of information will be processed, and the scope and purpose of the processing. Consent must also be documented and revocable.

A practice of extensive processing of personal data based on consent in which data protection assessments are left to individual units in the Armed Forces, is unfortunate. This could result in differences in practice within the Armed Forces, make the Committee's oversight more difficult and – in extreme cases – have a detrimental effect on individuals' data protection and right of privacy.

The Committee is of the opinion that the legal basis for all processing of personal data by the Armed Forces should be regulated as far as possible.

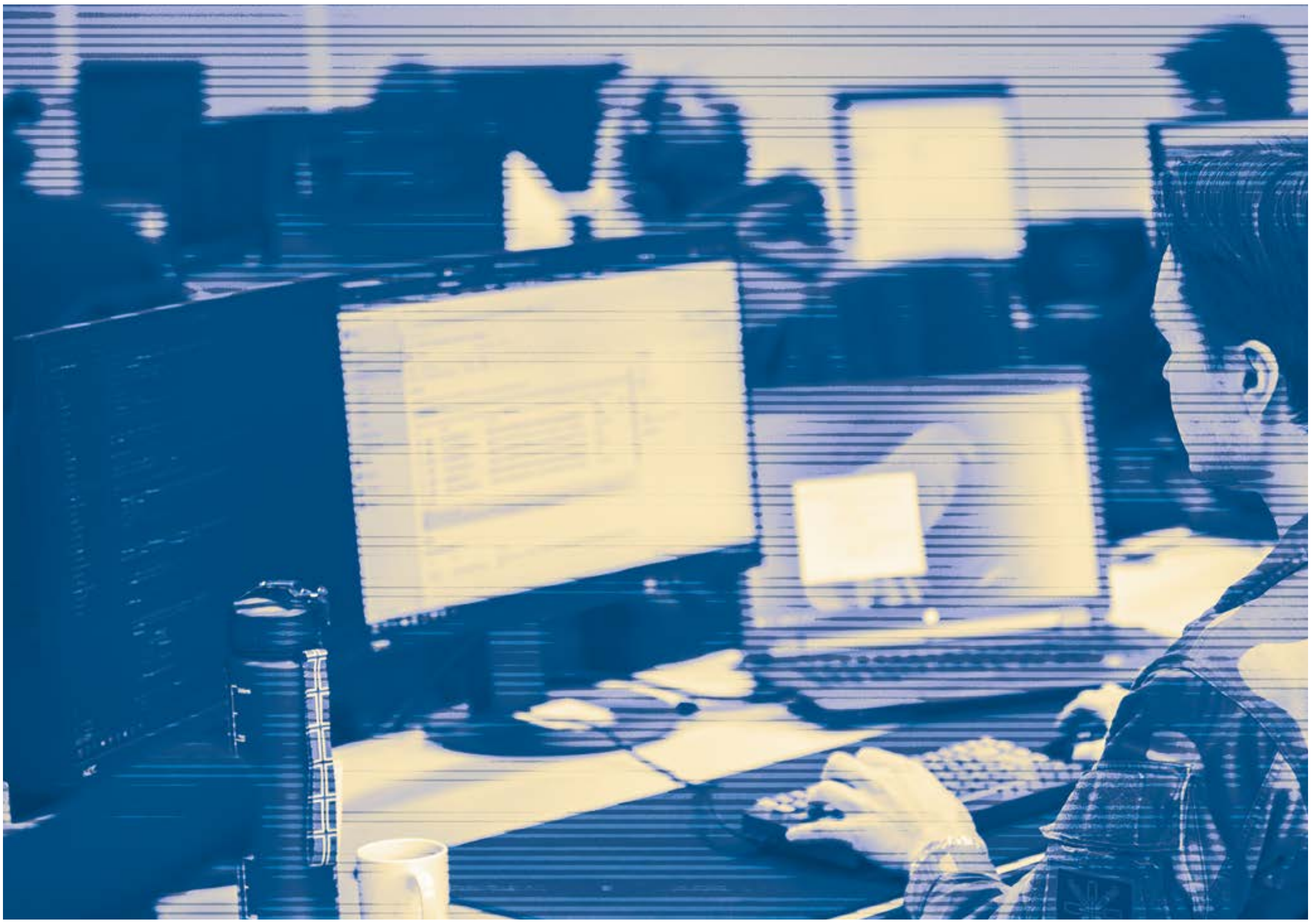


Photo: Anette Ask / Norwegian Armed Forces – Image effect: Fdesign

Appendices

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

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

- In February, the Director of the Secretariat gave a lecture on democratic oversight of the secret services at the University of Oslo's Faculty of Law.
- In May, the Director of the Secretariat gave a lecture on the EOS Committee's oversight to the Office of the Attorney General.
- In May, the Secretariat met with the trade union Tekna to discuss the Committee's oversight of the Norwegian Intelligence Service's (NIS's) use of facilitated bulk collection.
- The head of the technology department attend a workshop on oversight of commercially sourced datasets in Brussels in May. The workshop was hosted by the think tank interface.
- In May, the Secretariat attended a meeting of the Intelligence Oversight Working Group (IOWG) in Copenhagen.
- In June, the Director of the Secretariat gave a lecture on the EOS Committee's oversight to a delegation from the Ukrainian parliament at the premises of the think tank Geneva Centre for Security Sector Governance (DCAF) in Switzerland.
- During a country visit by the UN Counterterrorism Executive Directorate (CTED) in June, the Director of the Secretariat gave a talk on the EOS Committee's oversight of PST and the NIS's counterterrorism work.
- The Committee had two meetings with the Committee for the Evaluation of the Norwegian Intelligence Service Act. Several issues were dealt with in the meeting that took place in August, and the topic of the December meeting was the EOS Committee's special report on the NIS's unlawful storage of data obtained through facilitated bulk collection.
- The committee chair met with the chair of the Communications Control Oversight Committee in September.
- The Director of the Secretariat gave a lecture on democratic oversight of the EOS services to students at the School of Intelligence's advanced intelligence programme in September.
- The Director of the Secretariat visited the Danish Intelligence Oversight Board in October and gave a lecture to the staff.
- The committee chair gave a lecture on the EOS Committee's oversight to students at the Norwegian Defence University College's course on intelligence, politics and society.
- In November, the committee chair gave a digital lecture on the Committee's oversight in connection with the Internet Forum conference hosted by Norid and the Norwegian Communications Authority (Nkom).
- In November, the committee chair and the Secretariat took part in a meeting of the IOWG held in Zurich, Switzerland.
- The committee chair and the Secretariat also attended the European Intelligence Oversight Conference (EIOC) in Zurich in November
- The Committee's deputy chair and the Director of the Secretariat attended the International Intelligence Oversight Forum (IIOF) in Austin, USA, in November.
- In December, the head of the technology department gave a talk on the EOS Committee's oversight to a delegation from Armenia at the premises of the think tank DCAF in Geneva, Switzerland.
- The committee chair gave a lecture on the Committee's work to students at the School of Intelligence in December.
- The Committee met with judges and representatives of Oslo District Court, Borgarting Court of Appeal and the Supreme Court in December. The topic of discussion was advance and subsequent oversight of PST's use of covert coercive measures and the NIS's use of facilitated bulk collection.

The heads of the oversight bodies that make up the collaborative group IOWG (Intelligence Oversight Working Group) met in Zurich in November.
From left to right: Vanessa Samain (Committe I, Belgium), Gunnel Lindberg (SIN, Sweden), Marie Dechamps (NSIRA, Canada), Sir Brian Leveson (IPCO, the UK), Prisca Fischer (OA-IA, Switzerland), Hugo Hillenaar (CTIVD, the Netherlands), Grete Faremo (the EOS Committee, Norway), Lars Bay Larsen (TET, Denmark) and Monika Sörbom (SIUN, Sweden).
Photo: OA-IA

APPENDIX 2 – Letter from PST to the EOS Committee dated 13 February 2026

PST

UNCLASSIFIED

The Parliament Appointed Committee for Intelligence Oversight, the EOS Committee
P.O. Box 84 Sentrum
NO-0101 OSLO

Date:
13 February 2026

The EOS Committee's investigation into PST's use of covert coercive measures

1. Introduction

The EOS Committee has reviewed PST's petitions to the courts for authorisation to use covert coercive measures in prevention cases and investigation cases, including averting investigation. The investigation covered all rulings from Oslo District Court during a limited period of time in recent years, and it shows that 91 per cent of the rulings related to PST's prevention cases.

The EOS Committee states that the intention expressed in the preparatory works to the Police Act Section 17 d was that the service would be given permission to use covert coercive measures 'to a very limited extent' in its preventive work, and that, at the time, the Storting stated that the strict conditions would make the use of covert coercive measures in prevention cases a safety valve, to be used only if the rules for investigations could not be applied.

2. PST's comments

There are several reasons why the majority of PST's use of coercive measures takes place as part of our preventive activities. The prevention aspect is particularly important in relation to the criminal offences that PST is charged with preventing and investigating. The potential harm if such an act is carried out, makes it crucial to detect potential threats against public safety at the earliest possible stage before the threat is translated into action. The serious developments in the threat situation in recent years further emphasises the necessity of clarifying threats at an early stage and taking action accordingly – often long before the conditions for initiating an averting investigation have been met.

Crime is becoming increasingly international, and information from cooperating services is increasingly contributing to the basis for PST's work. Much of the information received by PST is highly classified and comes with clear conditions regarding how it can be used and with whom it can be shared. Examples include provisions that information received by PST can only be used for intelligence purposes and not as evidence in a criminal case. Such conditions limit PST's scope of action to open averting and investigation cases. Use of information in breach of such conditions would be harmful to intelligence cooperation and our access to information.

Several official documents published over a number of years have dealt with the fact that the majority of PST's use of methods takes place as part of PST's preventive activities. The Methods Evaluation Committee's report (NOU 2009:15 "Skjult informasjon – åpen kontroll" (Hidden information – open oversight – in Norwegian only) section 22.2 referred to the fact that the rules on the use of coercive measures for prevention and averting purposes were practised in a way that deviated somewhat from the legislators' intentions. It was also stated, however, that there was nothing to suggest that PST's use of coercive measures exceeded what is permitted under the Criminal Procedure Act and the Police Act. The matter was also raised in Prop. 68L (2015–2016) to the Storting, considered by the Storting in Innst. 343 L (2015–2016) to the Storting. At the time, the Ministry stated that «the current threat situation differs from that of 2005, and preventive work has become far more prominent since then».

The EOS Committee has overseen PST's use of coercive measures throughout the period that coercive measures have been available to PST in its preventive work (from 2005 to the present day). During the period 2006–2013, the EOS Committee oversaw all use of coercive measures by PST on an annual basis. The annual reports consistently noted that the Committee had observed a trend towards increasing use of coercive measures for prevention purposes and that the methods were used to a greater extent than intended by the legislators, without expressing criticism.

The Higher Prosecuting Authority as the expert authority has a special responsibility for overseeing PST's choice of track when using coercive measures as part of averting investigation cases versus for prevention purposes. The Higher Prosecuting Authority has consistently not found any reason for saying that PST should have used averting methods rather than preventive methods.

3. Conclusion

In PST's assessment, the development in the scope of its use of coercive measures for prevention purposes has proven necessary in light of developments in the threat situation and the premises for international intelligence work. Moreover, this development is in line with what the oversight authorities have been aware off, has been assessed and commented on in multiple official documents submitted to the Storting, and is based on more than 20 years of case law.

Beate Gangås (sign.)

Beate Gangås
Director General PST

APPENDIX 3 – Act relating to Oversight of Intelligence, Surveillance and Security Services[33]

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

33 Act No 7 of 3 February 1995 relating to the Oversight of Intelligence, Surveillance and Security Services (the Oversight Act). The Act was most recently amended 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 Norwegian 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 Norwegian 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 Armed Forces Special Operations Command.
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 Norwegian 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 Regulation 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: Synne Nilsson / Norwegian Armed Forces – Image effect: Fdesign

EOS COMMITTEE

THE PARLIAMENT APPOINTED COMMITTEE FOR INTELLIGENCE OVERSIGHT

fdesign.no

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

www.eos-utvalget.no