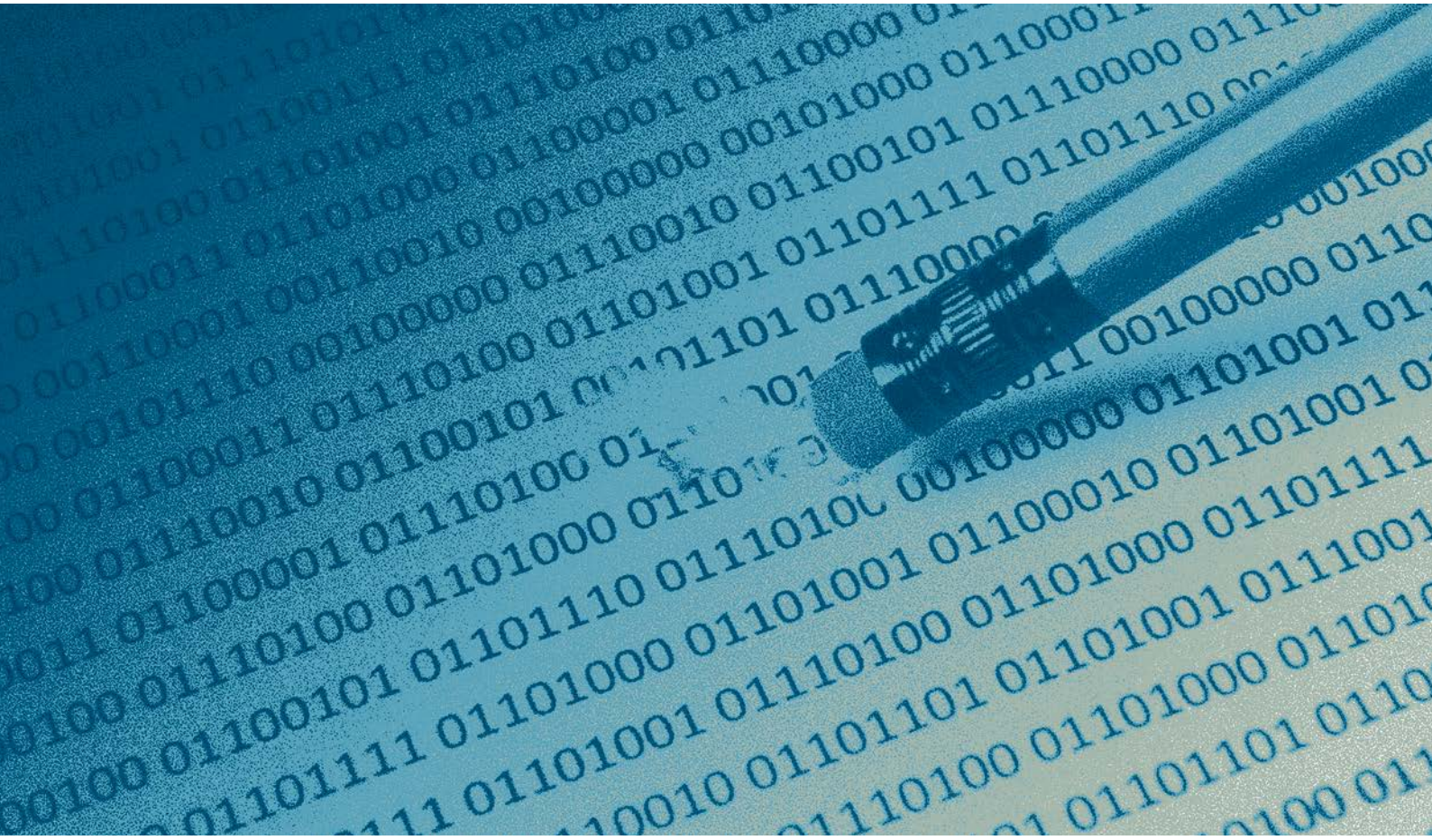
EOS COMMITTEE

NORWEGIAN PARLIAMENTARY OVERSIGHT COMMITTEE
ON INTELLIGENCE AND SECURITY SERVICES



ANNUAL REPORT 2023

DOCUMENT 7 (2023-2024)

Photo: Kristian Kapelrud / Norwegian Armed Forces

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 2023 to the Storting.

The annual report is unclassified, cf. the Oversight Act Section 17 third paragraph. Pursuant to the Security Act, the issuer of information decides whether or not it is classified. The respective services have been sent text excerpts concerning the service in advance in order to meet this requirement. The services have also been given the opportunity to check for factual errors and misunderstandings in the text.

Oslo, 20 March 2024

Astri Aas-Hansen

Kristin Krohn Devold

Magnhild Meltveit Kleppa

Erling Johannes Husabø

Camilla Bakken Øvald

Jan Arild Ellingsen

Olav Lysne

Henrik Magnusson

Photo: Anki Grøthe

The EOS Committee in 2023. From left: Camilla Bakken Øvald, Jan Arild Ellingsen, Olav Lysne, Astri Aas-Hansen (chair), Magnhild Meltveit Kleppa, Kristin Krohn Devold (deputy chair) and Erling Johannes Husabø.

Contents

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

1.

The Committee's remit and composition

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

The purpose of the oversight is:

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

The Committee may express its opinion on matters within the oversight area. It shall not seek more extensive access to classified information than warranted by the oversight purposes. The Committee's oversight shall cause as little inconvenience as possible to the services' operational activities. The Committee shall show consideration for national security and relations with foreign powers. Ex-post oversight is practised in relation to individual cases and operations. However, the Committee is entitled to be informed about and express an opinion on the services' current activities. The Committee may not instruct the EOS services it oversees or be used by them for consultations, but may request the services to implement measures or make decisions. The Committee's remit does not comprise reviewing the services' effectiveness, how they prioritise their resources etc.

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

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

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

Below is a list of the committee members in 2023 and their respective terms of office:

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

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

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

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

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

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

Olav Lysne, Bærum
1 July 2021 - 30 June 2025

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

1 Cf. the Oversight Act Section 1.

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

Classified information
Information that shall be protected for security reasons pursuant to the provisions of the Security Act. The information is assigned one of the following security classifications: RESTRICTED, CONFIDENTIAL, SECRET or TOP SECRET.

Plenary decisions
A decision made by the Storting in plenary session. Such a decision may, for example, constitute a set of instructions.

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.

2.

Key figures

The Committee's expenses amounted to NOK 40,813,849 in 2023. The total budget, including transferred funds and salary compensation through rebalancing throughout the year, has been NOK 43,990,000. The Committee has applied for permission to transfer parts of the unused funds to its budget for 2024. The Committee refers to the administrative Annual Report published on the EOS Committee's website for further details.

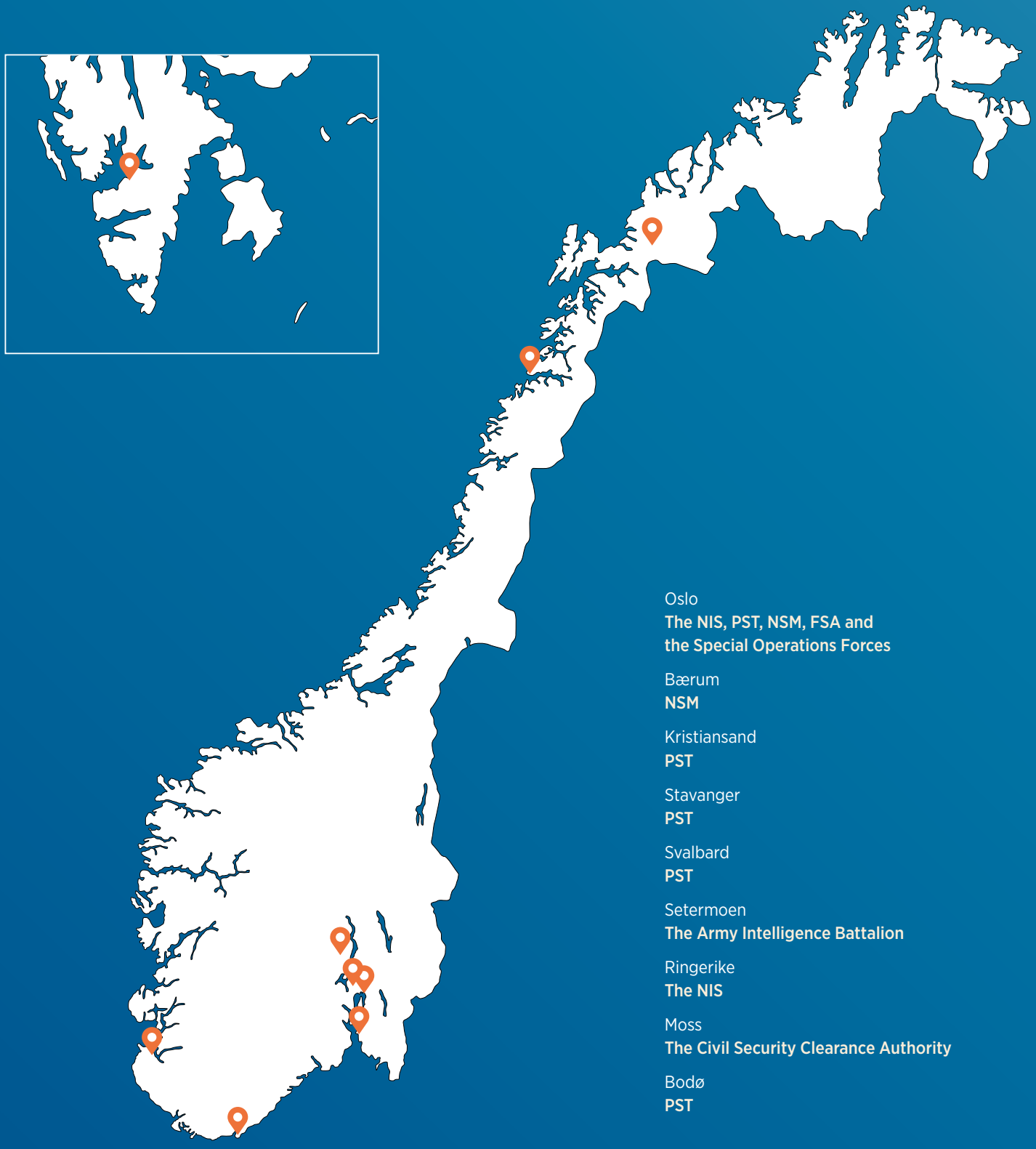
The workload of the chair of the committee corresponds to about 30 per cent of a full-time position, while the office of committee member is equivalent to about 20 per cent of a full-time position.

The Committee is supported by a secretariat, which at year-end 2023 consisted of 26 full-time employees. The Secretariat consists of the head of the secretariat, a legal unit with 13 employees, a technological unit with seven employees and an administrative unit with five employees. At year-end 2023, three employees were on parental leave and one employee was on unpaid leave.

3.

Overview of the Committee's activities in 2023

The Committee's inspections in 2023



Oslo
The NIS, PST, NSM, FSA and the Special Operations Forces

Bærum
NSM

Kristiansand
PST

Stavanger
PST

Svalbard
PST

Setermoen
The Army Intelligence Battalion

Ringerike
The NIS

Moss
The Civil Security Clearance Authority

Bodø
PST

3.1 Oversight activities

In 2023, the Committee conducted 25 inspections. Some inspections were directed against several of the services. In 2023, the Committee held ten internal committee meetings, in addition to internal working meetings on site in connection with inspections. During our internal meetings, we discuss inspections, complaints and cases raised on the Committee's own initiative, reports to the Storting and administrative matters.

The Committee raised 20 cases with the services on its own initiative in 2023. It concluded 12 cases raised on its own initiative in 2023.

The Committee investigates complaints from individuals and organisations. In 2023, the Committee considered 28 complaints against the EOS services. The Committee concluded 33 complaint cases in 2023.

3.2 The Committee's oversight methods and statements

A key part of the Committee's activities is to carry out inspections of the EOS services. The Committee's inspections consist of a briefing part and an inspection part. The topics of the briefings are mostly selected by the Committee. The Committee is briefed about the services' ongoing activities, national and international cooperation, the use of methods and the processing of personal data and other topics. The services are also asked to brief us on any matters they deem to be relevant to the Committee's oversight, including non-conformities that they themselves have identified. The Committee asks verbal questions during the briefings and sends written questions afterwards.

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

In recent years, the Committee has increased its use of a thematic approach to oversight. In addition to inspections, the Secretariat conducts regular investigations of the services' data systems. This enables the Committee to conduct more targeted and risk-based inspections.

The Committee raises cases on its own initiative based on findings made during its inspections. 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 must always be given the opportunity to state its opinion on the issues raised in the case before the Committee submits a statement that may result in criticism or other comments.

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

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

3.3 The Committee's consideration of complaints

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

The Committee's statements to complainants should be as complete as possible, but may not contain classified information. Both information that a person is being subjected to surveillance and information that a person is not being subjected to surveillance is classified information.[2] If the Committee's investigation shows that the complainant's rights have been violated, the Committee may inform the complainant that the complaint contained valid grounds for criticism.[3]

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

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 surveillance complaint cases.

3.4 Meetings and external activities

In 2023, the EOS Committee met with Minister Bjørn Arild Gram and described its oversight of the EOS services that fall within the minister's area of responsibility. The Committee also addressed issues related to the EOS Committee's international cooperation.

In connection with an inspection of the Norwegian Police Security Service (PST) Svalbard, the EOS Committee held orientation meetings with the Governor of Svalbard and the Svalbard Satellite Station (SvalSat).

The committee chair also met with the Extremism Commission. The Commission wanted to learn about the Committee's work. The consequences of an extension of the EOS services' legal basis for collecting and storing information for the Committee's oversight was discussed.

The Committee submitted the annual report for 2022 to the Storting in March 2023. In connection with the submission, the committee chair met with the President of the Storting and the Committee met with the Standing Committee on Scrutiny and Constitutional Affairs. The day after the submission, the Committee organised its annual conference, which is open to everyone. The topic for the 2023 conference was oversight of new surveillance methods. Around 150 people attended the conference. The conference was also streamed online.

Together with Swedish and Danish oversight bodies, the Committee organised the European Intelligence Oversight Conference in Oslo. Representatives from 24 organisations from 17 countries participated. The topics of the conference included the planning of oversight, the use of commercial and openly available data in the field of intelligence, and compliance with the European Court of Human Rights' decisions in *Big Brother Watch and others v. the United Kingdom* and *Centrum för Rättvisa v. Sweden*.

In connection with the conference, the Committee also hosted two meetings of the Intelligence Oversight Working Group, a collaborative project in which oversight bodies from Sweden, Denmark, the Netherlands, Belgium, Switzerland, the United Kingdom and Norway participate.

See Appendix 1 for an overview of all of the Committee's external activities.

The participants at the European Intelligence Oversight Conference in Oslo.
Photo: EOS-utvalget.

The Director of the NIS, Nils Andreas Stensønes, and the Director of PST, Beate Gangås, spoke at the EOS Committee's annual conference in 2023.
Photo: Arvid Grøtting.

European Intelligence Oversight Conference (EIOC)
The EIOC is an annual conference on the oversight of intelligence services. European oversight bodies and other public authorities whose responsibility includes the oversight of such services are invited to the conference.

4.

The Norwegian Intelligence Service (NIS)

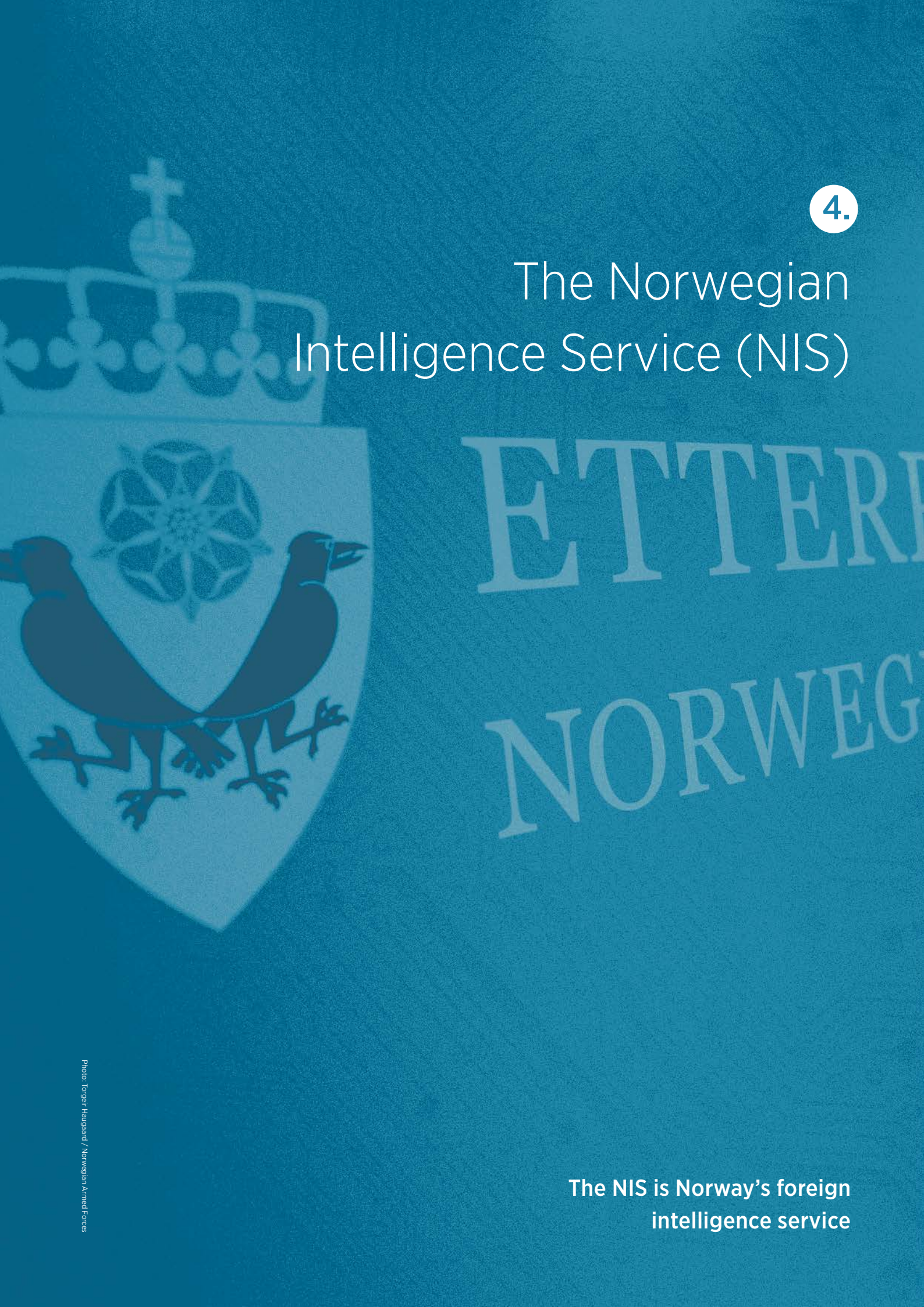


Photo: Torgeir Haugaard / Norwegian Armed Forces

The NIS is Norway's foreign intelligence service

4.1 General information about the oversight

The Committee carried out five inspections of the Norwegian Intelligence Service (NIS) headquarters in 2023, one of which concerned the service's security clearance of its own employees. The Committee has also inspected the service's station in Ringerike. Furthermore, the Committee inspected the Joint Intelligence and Counter-Terrorism Centre (FEKTS), where the NIS cooperates with PST. The Committee also inspected the Joint Cyber Coordination Centre (FCKS), which is a collaborative centre with participation from the NIS, PST, the National Security Authority (NSM) and the National Bureau of Crime Investigation (Kripos).

During its inspections of the NIS, the Committee focuses on

- the use of collection methods that could entail interference in relation to individuals
- the processing of personal data
- the exchange of information with foreign and domestic partners
- cases that have been submitted to the Ministry of Defence[4]
- internal approval cases[5]
- facilitated bulk collection of transboundary electronic communication
- whether the NIS's stations, equipment, methods and collection of information are subject to national control.

The Committee's right of inspection does not extend to the NIS's particularly sensitive information. The Committee is regularly updated on the scope of information that falls within this category. The information is made available to the Committee once it is no longer defined as being particularly sensitive.

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

On 30 January 2024, the Committee submitted a special report to the Storting on the role of the NIS in the 25 June case, cf. the Oversight Act Section 17 second paragraph.[6] After its investigation of the matter, the Committee found no grounds for criticism of the NIS.

4.3 Illegal collection of information in relation to a Norwegian person

The NIS is entitled to use intrusive collection methods. A decision on the use of such methods must be made in writing and state what or whom the collection of information concerns. The legal basis for collecting information must also be stated. This follows from the Intelligence Service Act Section 6-13.

The NIS made a decision in 2022 on the use of intrusive methods in relation to an unknown number of non-identified Norwegian persons abroad. The Committee asked about the basis for collection in relation to one of the Norwegian persons about whom information was collected.

In the decision, the NIS explained what conditions must be met in order to use intrusive methods. The Committee considered that the service had not established that the conditions were present for collecting information about this person. A sufficiently concrete proportionality assessment had not been made before the collection was initiated. Nor were the assessments sufficiently documented. The Committee criticised the NIS for breach of the regulations. The NIS disagreed with the Committee's assessments and conclusions.

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

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

6 Document 7:1 (2023–2024).

Particularly sensitive information
By 'particularly sensitive information', cf. the 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.

Intrusive methods
The NIS is entitled to use methods that could entail interference in relation to individuals. The methods include, but are not limited to, human intelligence, collection of electronic communication and information, and audio and video surveillance.

The chair of the EOS Committee, Astri Aas-Hansen, delivered the special report on the Norwegian Intelligence Service's role in the 25 June case to Masud Gharakhani, President of the Storting.

The Committee noted that the collection of information about the person illustrated that it can be problematic to make decisions about collection that concern an unknown number of non-identified persons. On a general basis, the Committee has raised the matter of whether the service sufficiently specifies what or whom the collection of information concerns. The Committee is continuing its work on this issue.

The Committee also criticised the NIS for having initiated collection of information about the person while the person was staying in Norway. The NIS is not entitled to use intrusive methods against persons in Norway. If there is doubt about where a person is staying, the service must seek to clarify the person's whereabouts. Before collection can be initiated, it must be established with a preponderance of probability that the person is abroad.[7] The service had not sought to clarify the persons whereabouts. The use of the methods constituted a breach of the territorial prohibition set out in Section 4-1 of the Intelligence Service Act.

4.4 Shortcomings in the assessment of whether a person was abroad

The Committee criticised the NIS for having used intrusive methods against a person without having established a preponderance of probability that the person was abroad.

Following questions from the Committee regarding the assessment of the person's whereabouts, the NIS referred to a report in which it was considered that the person would be staying in another country for a period of three days. Based on the information, the service assumed that the person had

7 Proposition No 80 to the Storting (Bill) (2019– 2020) p. 201.

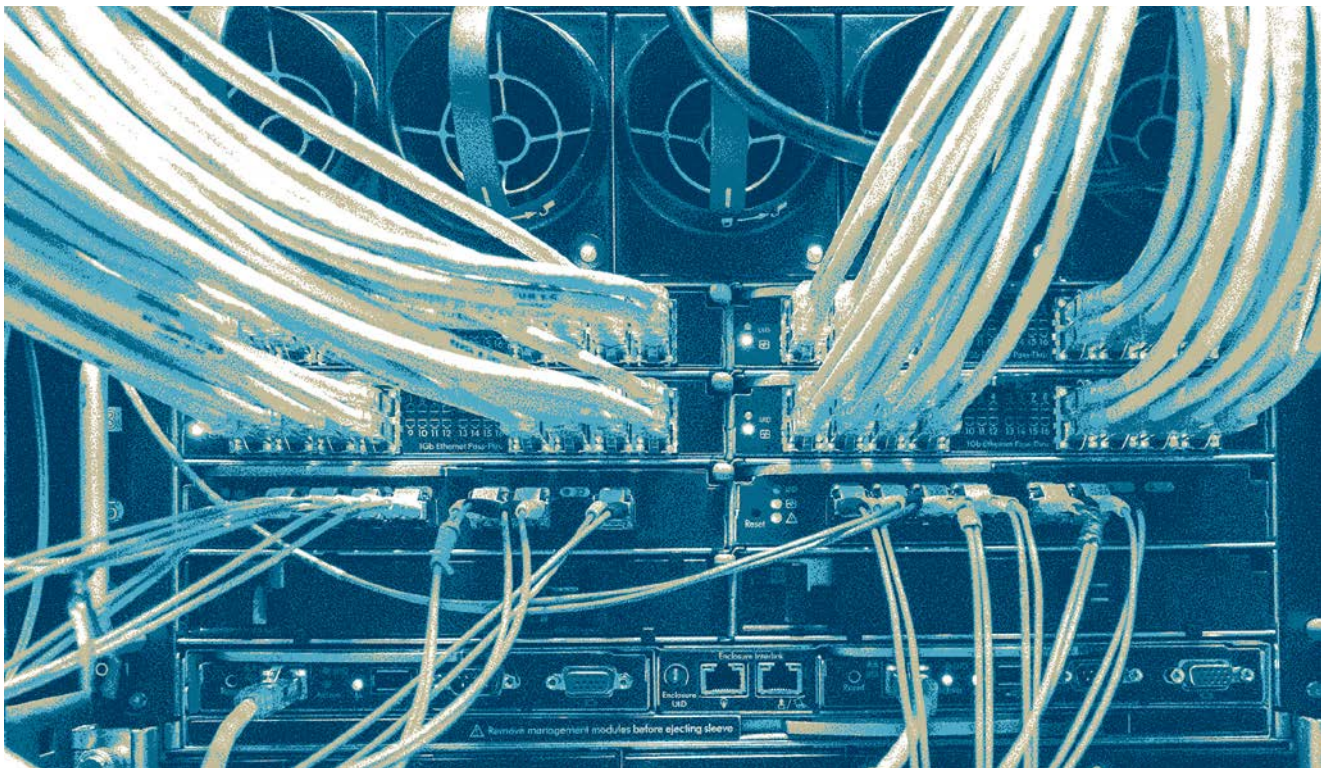
left Norway, and collection was initiated for the person's selectors. Although the same report indicated that the person in question would return three days later, this information was not emphasised and the service continued to collect information about the person. The service could not refer to any other evidence to indicate that the person remained outside Norway.

Pursuant to the Intelligence Service Act Section 5-4, a concrete proportionality assessment must be made in connection with the use of intrusive methods. The Committee concluded in this case that the proportionality assessment had not been sufficiently documented, and that it had not been substantiated *when* the assessment was made. The Committee's ability to oversee the service's use of intrusive methods rests on the decisions being sufficiently documented. The Committee criticised the service for these shortcomings.

4.5 Oversight of facilitated bulk collection

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

Amendments to the Intelligence Service Act's chapters on facilitated bulk collection entered into force on 1 October 2023. Following these amendments, the NIS is entitled to use the facilitated bulk collection method for intelligence production. The amendments also require the Director of the NIS to obtain the court's permission to issue orders to an electronic communication provider to mirror data. However, the Director of the NIS may decide to mirror data for the purpose of technical analyses that are intended to form the basis for submitting a petition to the court.



Selector
A selector is a search term associated with an intelligence target, such as a phone number or an email address, from which information is retrieved.

Facilitated bulk collection of transboundary electronic communication
Facilitated bulk collection means that the NIS can collect electronic communication transmitted across the Norwegian border.

Intelligence production
To compile and analyse information collected for intelligence purposes.

Electronic communication providers
Providers of electronic communications networks and services.

Mirroring
Mirroring involves replicating data, without changing, stopping or delaying the flow of data.

The Committee conducted oversight activities in 2023 relating to whether the NIS's testing and development of facilitated bulk collection has been carried out within the framework of the Intelligence Service Act Section 7-3. Among other things, the Committee has investigated whether the service has complied with the rules for issuing orders to electronic communication providers to make electronic communications available to the service. The Committee has also conducted oversight activities related to whether the collected data has only been used for the purposes permitted by the regulations.

The Intelligence Service Act Section 7-11 requires the NIS to facilitate the Committee's oversight of facilitated bulk collection through technical solutions. In order to carry out its oversight duties, the Committee has requested that the service develop oversight functionality in its systems. The NIS followed up this request in 2023, and the Committee is in dialogue with the service about further facilitation of oversight.

4.6 Follow-up of logging of searches of raw data in bulk

In 2022, the Committee criticised the NIS for inadequate logging of searches of raw data in bulk for oversight purposes.[8] The Committee considered that the legal requirement for logging for oversight purposes was not met. In 2023, the service developed a system that better enables the Committee to exercise oversight activities of the NIS's searches of bulk data.

4.7 Follow-up of the bulk purchase of metadata

The Committee commented in 2022 on the NIS's purchase of bulk metadata containing personal data from commercial enterprises.[9] The Committee considered that such purchases must be deemed collection of information that could entail interference in relation to individuals, and that it was thus required that the collection be warranted by the Intelligence Service Act Chapter 6. The NIS stated in 2022 that it would raise the issue with the Ministry of Defence.

The NIS stated in 2023 that the service has informed the Ministry of Defence both verbally and in writing. In the first quarter of 2024, the service will present a recommendation to the Ministry and address any need for regulatory changes. The Committee will be kept informed about the matter.

4.8 Follow-up of internal regulations on collection in cyberspace

In 2022, the Committee expressed its opinion on the NIS's internal regulations on collection in cyberspace.[10] These regulations are classified. The Committee urged the service to consider certain provisions to ensure that they complied with the Intelligence Service Act.

In connection with follow-up in 2023, the NIS reiterated that one issue would be raised with the Ministry in the course of 2024. The service also stated that a proposal will be made to adjust one provision in the internal regulations and that new internal regulations are expected to be issued in January 2024. The Committee will be kept informed about the service's follow-up of the matter.

4.9 Complaint cases

The Committee accepted six complaints against the NIS for consideration in 2023. Some of these complaints were against more than one of the EOS services. The Committee concluded 11 complaint cases against the NIS in 2023.

One of the concluded cases resulted in criticism of the NIS.

8 See Section 4.4 of the Committee's annual report for 2022.

9 See section 4.3 of the Committee's annual report for 2022.

10 See section 4.7 of the Committee's annual report for 2022.

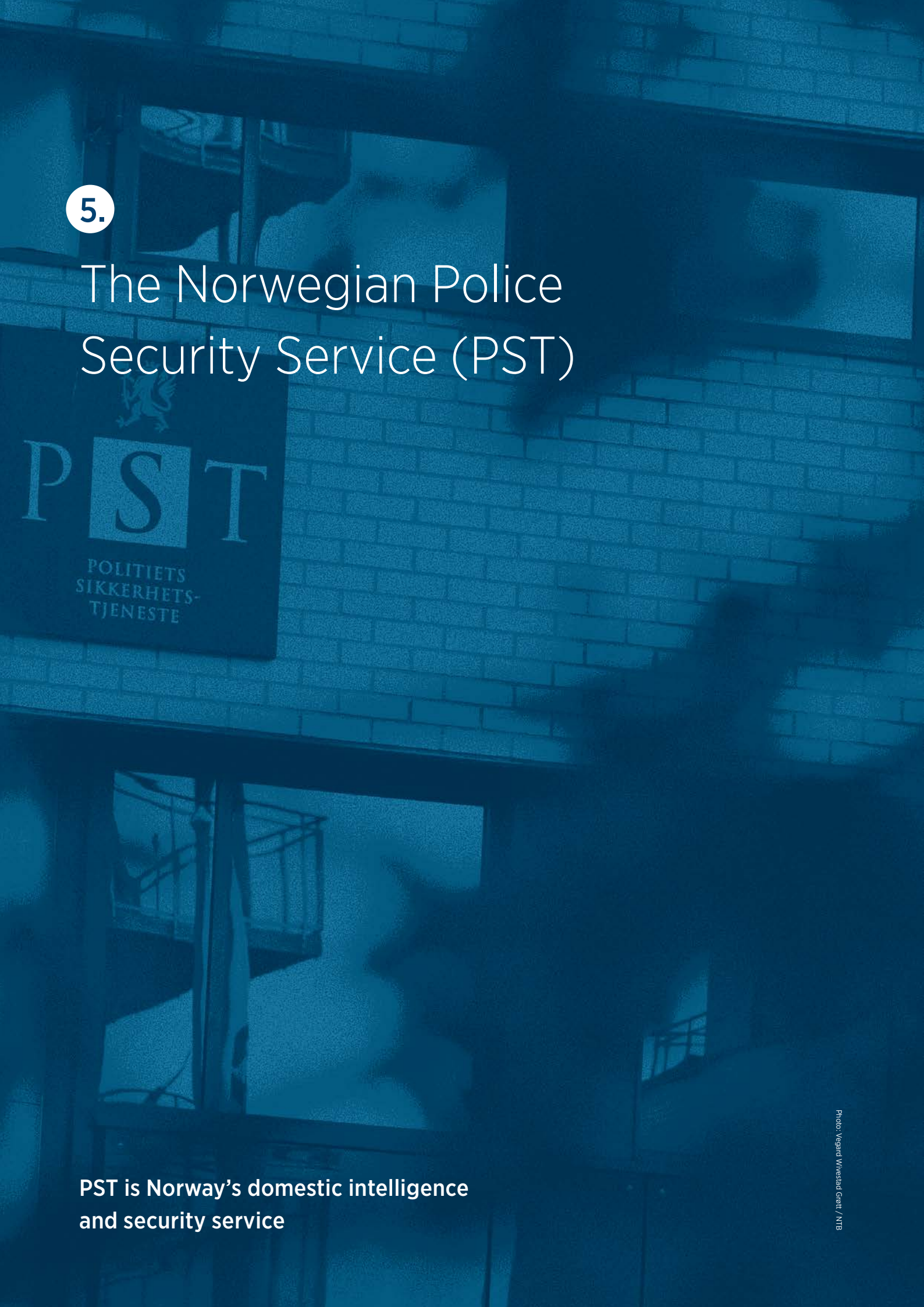
Raw data
Data that are unprocessed or automatically processed, and thus not analysed or evaluated in any way.

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

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

5.

The Norwegian Police Security Service (PST)



PST is Norway's domestic intelligence and security service

Photo: Vegard Wivestad Grøtt / NTB

5.1 General information about the oversight

In 2023, the Committee conducted five inspections of the PST Headquarters (DSE), one of which concerned the service's security clearance of its own employees. The PST units in Svalbard and in Agder, Sør-Vest and Nordland police districts were also inspected.

Furthermore, the Committee inspected the Joint Intelligence and Counter-Terrorism Centre (FEKTS) and the Joint Cyber Coordination Centre (FCKS), cf. section 4.1.

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

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

5.2 Insufficient deletion in PST's registers

A key part of the Committee's oversight of PST is to ensure that the service does not process data for longer than required for the purpose of the processing, cf. the Police Databases Act[11] Section 50 and the Police Databases Regulations Section 22-3 first paragraph. Data that are no longer necessary to process must be deleted or access to it must be restricted.

In practice, even if a person is deleted as an object, information about the person may still be present in a description of an incident that includes other objects. Information about the person will only be deleted when the registration of the incident is deleted. This is not done until all objects associated with the incident are deleted.

PST previously had a technical solution that limited the possibility of searching for information about persons who have been deleted as objects.[12] However, this technical solution was not included in the analysis and compilation tool (hereinafter referred to as the tool) that PST adopted in 2019.

The introduction of the tool entailed that information about 44,893 objects, which according to PST it was no longer necessary to process information about, became available to PST's employees. PST does not know how the stated number of objects is distributed between physical and legal persons.

The Committee considered the matter to be a serious non-conformity. In its assessment, the Committee emphasised that the introduction of the tool meant that information had been made available about a large number of people whom PST itself did not consider it necessary to process information about. In addition, the Committee emphasised that PST had not implemented measures to prevent or restrict searches for or results containing the information.

The Committee criticised PST on this basis. The Committee pointed out that since the introduction of the tool, the service had failed to implement a solution that ensured compliance with the deletion rules. This gave the service access to information that should have been deleted, and was, in the Committee's opinion, an extensive breach of the Police Databases Act Section 50 first paragraph and the Police Databases Regulations Section 22-3 first paragraph.

The Committee has asked PST how the service will ensure that information about the 44,893 objects will be processed in line with the deletion requirement in future. PST will review the objects during the first quarter of 2024 to this end. PST has informed the Committee that the service will introduce a new

11 Act No 16 of 28 May 2020 relating to the processing of data by the police and the prosecuting authority (the Police Databases Act).

12 See e.g. the EOS Committee's annual report for 2011, Document 7:1 (2011–2012) Roman numeral IV section 7.

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.

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

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

Covert coercive measures
Police methods that are regulated by law and that are used without the person who is the target of such methods being aware of their use. Examples include searches, video surveillance and equipment interference.

Deletion
Deletion means that the information is removed from registers or other systems.

Restriction of access to information
Marking of stored information for the purpose of limiting future processing of it.

Objects
An object can be a person or an organisation, or similar. The object registration contains identifiers such as personal data and a description of the object's roles.

Incident
Registered information related to one or more objects.

procedure to ensure that the rules on deletion are observed in the future. PST is working to develop technological tools to ensure that deleted objects are also deleted in documents. The Committee has requested that PST inform the Committee when the procedure has been introduced.

5.3 Non-conformities in connection with the conclusion of prevention cases

The inspection of the PST Headquarters (DSE) in November 2022 revealed that in its conclusion of prevention cases, PST did not consider whether access to the case information should be restricted or could be continued for other uses, as required by the Police Databases Regulations Section 22-3. The service initiated a project to rectify this issue. During the inspection of DSE in November 2023, the service reported that all prevention cases have been reviewed and have now been concluded in the correct manner.

5.4 Information about use of non-statutory methods in petitions to the court

In connection with information about the use of non-statutory methods, the Committee asked whether PST informs the court about all the methods it employs when the service requests permission to use statutory coercive measures. PST responded that the court should be informed of this to a greater extent, to enable it to make a more informed proportionality assessment of the use of methods seen as a whole. In November 2023, PST informed the Committee that the service is preparing guidelines for how the court should be informed about the use of non-statutory methods. Such guidelines will be included in PST's internal regulations. The Committee takes a positive view of this.

5.5 Facilitation and planning of oversight of PST's collection of information from open sources

On 28 April 2023, the Storting decided to incorporate a new provision in the Police Databases Act on PST's use of openly available information.[13] The amendment authorises PST to store information from open sources in order to prepare analyses and intelligence assessments, as well as to use the information in prevention cases and investigations. Access to the information will be restricted and may only be used for the purposes stated in the Act. It has not been decided when the provision will enter into force.

In its recommendation to the Storting, the majority of the Standing Committee on Justice stated that the technical systems to be developed must be adapted to the EOS Committee's oversight.[14] PST has begun work on preparing the possibility of processing information as specified in the new provision. It is important that the EOS Committee has a good dialogue with PST to ensure the necessary oversight functionality in the system. The Committee has been informed verbally and in writing about the service's plans and ongoing work. In a letter to PST, the Committee described the necessary functional requirements for oversight of the service's processing.

5.6 Proposal for clarification of the rules on notification of interception of communication

The Criminal Procedure Act Section 216 j regulates the right to be informed if a person has been subject to lawful interception of communication. Petitions for such notification are considered by the Communications Surveillance Control Committee, cf. the Criminal Procedure Act Section 216 h. However, it follows from the provision that the Communications Surveillance Control Committee shall not oversee matters covered by the Oversight Act. The Communications Surveillance Control Committee cannot therefore consider PST cases.

The EOS Committee handles complaints about surveillance activities in PST and conducts the investigations that are appropriate in relation to the complaint. The EOS Committee handles petitions for notification of interception of communication directed to PST in accordance with the Oversight Act Section 5 second paragraph.

In November 2023, the EOS Committee proposed to the Ministry of Justice and Public Security to clarify that petitions for notification of interception of communication carried out by PST pursuant to the Criminal Procedure Act Section 216 j sixth paragraph, are considered by the EOS Committee in accordance with the Oversight Act. This is in the interest of those who wish to petition for notification of interception of communication in PST.

5.7 Complaint cases

The Committee has accepted 16 complaints against PST for consideration in 2023. Some of these complaints were against more than one of the EOS services. The Committee concluded 20 complaint cases against PST in 2023.

The Committee expressed criticism against PST in two complaint cases in 2023. In both cases, the Committee requested to give the complainant a more detailed explanation of the grounds for its criticism. The Committee provided a detailed explanation in both cases.

In one of the complaint cases, PST was criticised for having informed another enterprise that the EOS Committee was considering a complaint from a named person. The Committee stated that complainants must be able to trust that information they provide to the Committee will be treated confidentially.

In the second complaint case, the Committee criticised PST for non-conformities in the processing of information about the complainant.

13 Proposition No 31 to the Storting (Bill) (2022–2023).

14 Recommendation 229 to the Storting (Bill) (2022–2023) p. 8.

Lawful interception of communication
A method that monitors a person's communication – for example telephone surveillance or monitoring of metadata about telephone and computer communication. PST can use this method subject to court approval.

6. The National Security Authority (NSM)

The NSM is Norway's directorate for preventive security services

Photo: Gorm Kallestad / NTB

6.1 General information about the oversight

In 2023, the Committee conducted three inspections of the National Security Authority (NSM). One inspection concerned NSM's handling of security clearance cases, one targeted NSM's technical capabilities with a focus on penetration testing, and the third concerned the Norwegian National Cyber Security Centre (NCSC). The function of NCSC is to protect fundamental national functions, the public administration and business and industry against serious cyber-attacks. Furthermore, the Committee inspected the Joint Cyber Coordination Centre (FCKS), cf. section 4.1.

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

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

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

A person who has received a justification for a clearance decision where information has been omitted pursuant to the Security Act Section 8-13 second paragraph,[15] has the right to assistance from a specially appointed lawyer, cf. the Security Act Section 8-15. The purpose of the lawyer arrangement was to ensure due process protection of the person the decision concerns.[16] However, the lawyer has a duty of confidentiality to the person applying for security clearance and may only advise the person whether to appeal the decision or not.

In 2021, the Committee pointed out to the Ministry of Justice and Public Security that the lawyer arrangement had not been used for the past ten years.[17] The Ministry assigned the Norwegian National Security Authority (NSM) the task of establishing an interim scheme for the specially appointed lawyer arrangement. Such a scheme was established in March 2023.

Following a new review in 2023, the Committee concluded that the interim lawyer arrangement is not suitable for balancing the interests of the vetted person's due process protection and the interests of national security in clearance cases.

The Committee pointed out that there is little left in the arrangement of the core tasks that would normally characterise the relationship between lawyer and client. Due to the lawyer's duty of confidentiality, the vetted person cannot receive guidance on why an appeal should be lodged or how such an appeal should be formulated. Nor can the lawyer verify that the factual basis on which the decision is based is correct.

If the vetted person refrains from using the lawyer arrangement, their appeal will be processed more quickly and a new assessment made. The Committee asked the Ministry of Justice and Public Security to consider discontinuing the scheme.

The Committee has requested feedback from the Ministry on what measures have been decided or implemented by the end of 2024, cf. the Oversight Act Section 14 last paragraph.

6.3 Complaint cases

The Committee has accepted 12 complaints against NSM for consideration in 2023. Some of these complaints were against more than one service. The complaint cases concerned surveillance and security clearance issues. The Committee concluded 15 complaint cases in 2023. Six of the cases, all of which concerned security clearance, resulted in criticism.

In one case, the Committee criticised both the Norwegian Defence Security Department (FSA) and NSM for not having elucidated the matter as well as possible, cf. the Security Act Section 8-4 third paragraph. This matter is described in more detail in section 7.2. Both FSA and NSM were also criticised for long case processing times in the case.

The other complaint cases concerned a long case processing time.

15 Cf. Act No 24 of 1 June 2018 relating to National Security (the Security Act) Section 8-13. Information may be omitted if it could reveal circumstances that are relevant to national security interests, for the protection of sources, information the person should not gain knowledge of in the interests of their health, information which concern the person's associates and of which the person should not gain knowledge.

16 Proposition No 153 to the Storting (Bill) (2016–2017), section 19.8.

17 See section 6.3 of the Committee's annual report for 2021.

Penetration testing
An undertaking can request that the National Security Authority attempt to penetrate the undertaking's critical information systems, to check whether the security measures are sufficient.

The vetted person
The person for whom security clearance is requested.

In one complaint case, NSM was criticised for having taken more than four months to process a petition for access. The Committee also criticised NSM for having taken around eleven months to have a special lawyer appointed to review a security clearance case, cf. the Security Act Section 8-15.

In two cases, the Committee criticised NSM for it having taken nine months before the appeal case was decided by NSM, and ten months without NSM having considered the appeal, respectively.

In two other cases, the Committee pointed out to NSM that the appeal cases seemed to have remained as good as unprocessed for more than one year and ten months, and more than two years and four months, respectively, from the time they were received by NSM. The cases had not been decided by NSM when the Committee concluded its consideration of the complaints. The overall case processing time in both cases was more than four years. This is considered to undermine the right to a proper and timely review of the decision. The Committee stated to NSM that this warrants strong criticism.

6.4 Case processing times in NSM's security clearance cases

Below is a table of case processing times for 2023 as provided by NSM:[18]

CASE PROCESSING TIME NSM 2023	Average case processing time overall	Average case processing time, positive decisions[19]	Average case processing time, negative decisions
Request for access	78 days (4 cases)[20]		
Request for security clearance	81 days (162 cases)[21]	85 days (151 cases)	172 days (2 cases)
First-tier appeals	360 days (3 cases)	No cases	360 days (3 cases)
Second-tier appeals	453 days (104 cases)	333 days (5 cases)	460 days (99 cases)

NSM's case processing times for both access cases and first and second tier appeals are still very long. The Committee's consideration of the case processing times is discussed in section 9.

18 The statistics are based on the date on which NSM received the security clearance or appeal.

19 Appeals where the body found partly in favour of the appellant are included in 'positive decisions'.

20 NSM also considered three appeals concerning requests for access for which the directorate made the initial decision. The case processing time was two, four and eleven weeks, respectively.

21 This figure includes dropped cases.

Negative decision in a clearance case
A decision where clearance is denied, or where clearance is granted at a lower level, for a shorter period of time than requested, or subject to certain conditions.

7.

The Norwegian Defence Security Department

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

7.1 General information about the oversight

The Committee conducted two inspections of the Norwegian Defence Security Department (FSA) in 2023. One inspection targeted FSA's processing of security clearance cases and the other concerned FSA's operational security services.

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 Complaint cases

The Committee accepted six complaints against FSA for consideration in 2023. Some of these complaints were against more than one service. Eleven complaint cases against FSA were concluded in 2023. The complaint cases concerned surveillance and security clearance issues.

Four of the cases, all of which concerned security clearance, resulted in criticism.

In one case, the complainant had withdrawn their consent to access to health information *before* the information was disclosed to the security clearance authority. The Committee was of the opinion that the security clearance authorities should have investigated the complainant's claim that the health information had been disclosed without a legal basis. Nor could the Committee see that FSA or NSM had considered the significance of the withdrawal of consent in their internal grounds. The Committee therefore criticised FSA and NSM for not having elucidated the matter as well as possible, cf. the Security Act Section 8-4 third paragraph. Furthermore, FSA was criticised for not fulfilling its activity obligation in relation to NSM as the appellate body, and both FSA and NSM were criticised for long case processing times.

The Committee also criticised FSA for long case processing times in three other cases. In one of these cases, FSA had the security clearance case under consideration for nine months, before the appellant's call-up for national service was eventually annulled as a result of unresolved security clearance. The Committee concluded that it was very unfortunate that the long processing time had led to the lapse of the need for security clearance. In the two other cases, the Committee criticised FSA for the fact that the security clearance cases had been under consideration for more than 13 months and two years, respectively, without being decided.

7.3 Case processing times in FSA's security clearance cases

Below is a table of case processing times for 2023 as provided by FSA:[22]

CASE PROCESSING TIME FSA 2023	Average case processing time overall	Average case processing time, positive decisions[23]	Average case processing time, negative decisions
Requests for access	9 days (19 cases)		
Requests for security clearance[24]	43 days (23,590 cases)	40 days (20,893 cases)	433 days (148 cases)
First-tier appeals	75 days (23[25] cases)	252 days (1 case)	67 days (21 cases)

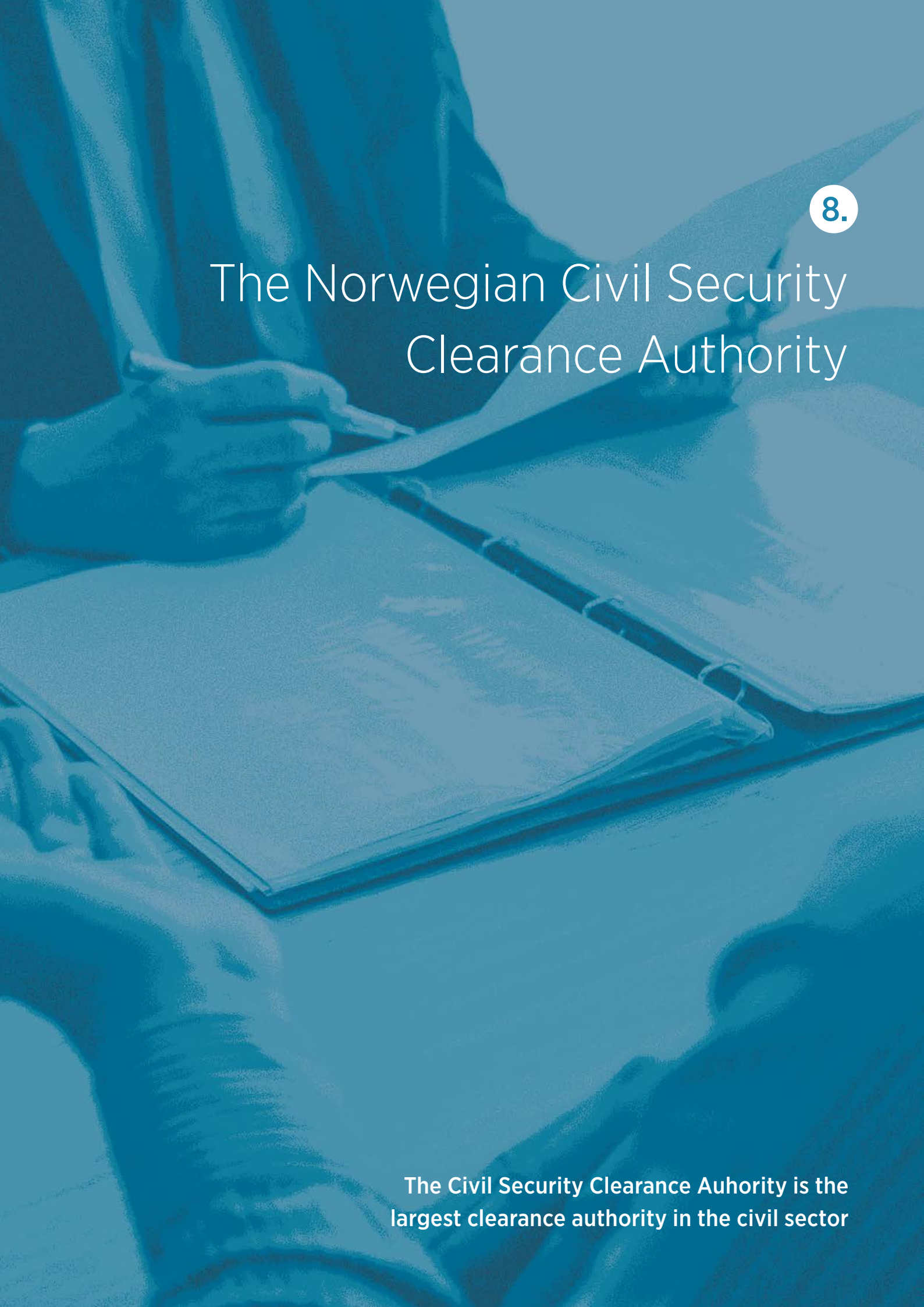
Case processing times in appeal cases where FSA makes the initial decision have decreased from 2022. Case processing times for security clearance cases with negative results have increased. The Committee's consideration of the case processing times is discussed in section 9.

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

23 Appeals where the body found partly in favour of the appellant are included in 'positive decisions'.

24 FSA has also stated that the average processing time for processing incoming information in security clearance cases in 2023 was 258 days.

25 One of the complaint cases was dropped when the complaint was withdrawn.



8.

The Norwegian Civil Security Clearance Authority

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

8.1 General information about the oversight

The Committee carried out one inspection of the Norwegian Civil Security Clearance Authority (SKM) in 2023. The focus of the inspection was case processing times in security clearance cases, as well as the specially appointed lawyer arrangement in security clearance cases set out in the Security Act.

During the inspection of SKM, the Committee reviewed security clearance cases submitted by the Office of the Prime Minister. This was because the Committee's planned inspection of the Office of the Prime Minister in 2022 was cancelled when SKM took over responsibility for the Office's security clearance cases. The inspection of SKM did not give grounds for follow-up.

8.2 Complaint cases

The Committee received three complaints against the SKM in 2023, all of which were concluded in 2023. Two of the cases resulted in criticism. Both cases concerned long case processing times.

The Committee criticised SKM for taking nine and eleven months, respectively, before the cases were concluded. One case was concluded because the need for security clearance lapsed due to the assignment in question being completed before the case had been processed.

8.3 Case processing times in SKM's security clearance cases

Below is a table of case processing times for 2023 as provided by SKM:[26]

CASE PROCESSING TIME SKM 2023	Average case processing time overall	Average case processing time, positive decisions	Average case processing time, negative decisions
Request for access[27]	8 days (33 cases)		
Request for security clearance[28]	62 days (7,594 cases)	53 days (7,333 cases)	321 days (261 cases)
Request for access clearance	40 days (1,046 cases)	29 days (1,008 cases)	337 days (38 cases)
First-tier appeals	129 days (47[29] cases)	132 days (5 cases)[30]	131 days (41 cases)

Case processing times in complaint cases where SKM makes the initial decision have decreased from 2022. Case processing times for security clearance cases with negative results have increased. The Committee's consideration of the case processing times is discussed in section 9.

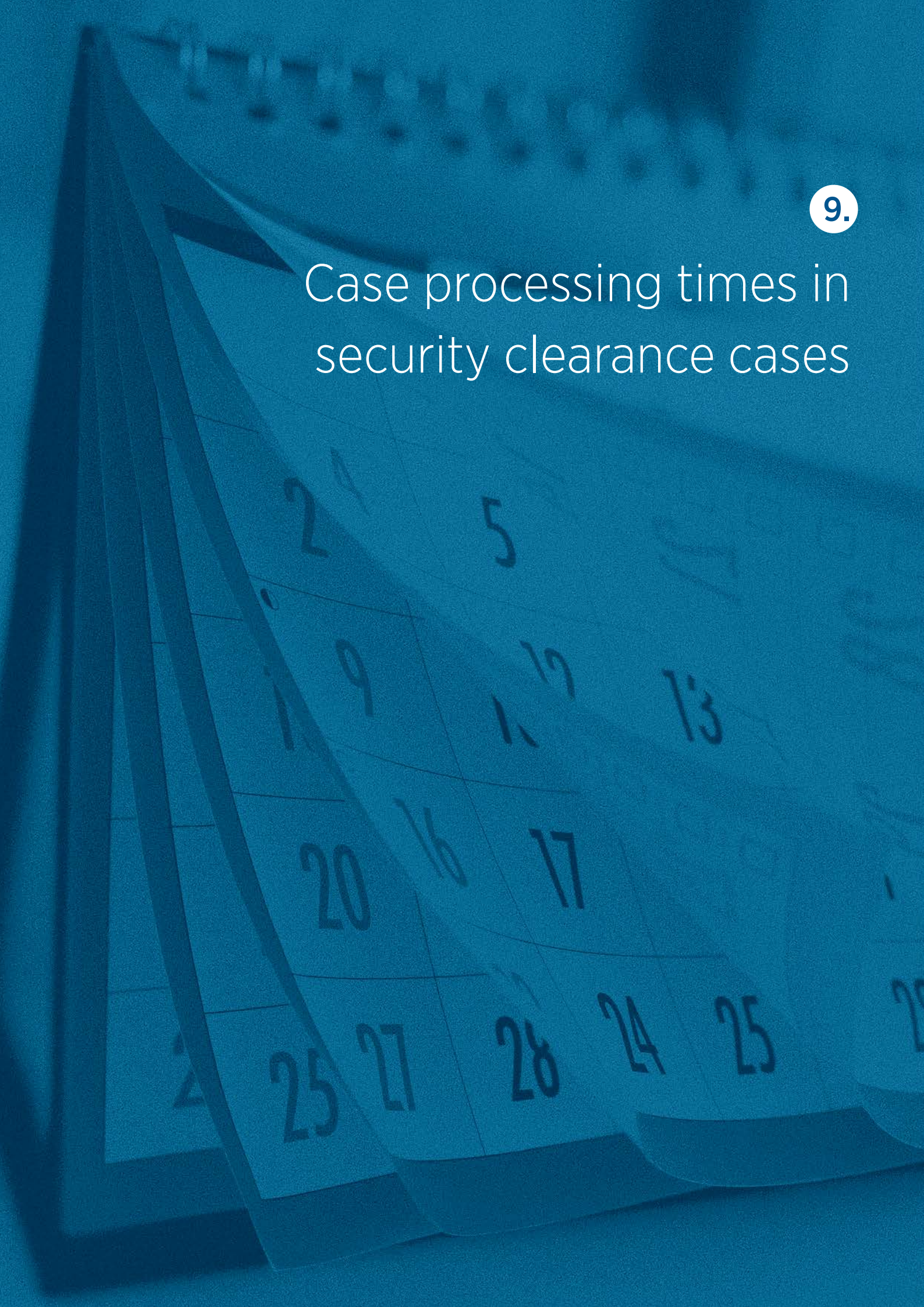
26 The statistics are based on the date on which the request was received by the security clearance authority.

27 The average case processing time for appeal cases concerning access to information was 10 days in 2023.

28 SKM has also stated that the average case processing time in 2023 for processing incoming information in security clearance cases was 127 days.

29 One of the appeal cases was dismissed because it was lodged too late. The dismissal was not appealed.

30 Appeals where the body found partly in favour of the appellant are included in 'positive decisions'.



9. Case processing times in security clearance cases

9.1 Background

The Committee reviews the processing of security clearance cases in NSM, FSA and SKM. In the Committee's opinion, case processing times in security clearance cases are often much too long, particularly in appeal cases.

In the annual report for 2022, the Committee stated that the increase in NSM's case processing times gives cause for concern. The Committee wrote to the Ministry of Justice and Public Security about the matter. On this basis, on 3 March 2023, the Ministry ordered NSM to take extraordinary measures to bring the backlog of appeal cases down to an acceptable level.

In the Standing Committee on Scrutiny and Constitutional Affairs' recommendation to the Storting on the Committee's annual report for 2022,[31] the Committee addressed several issues related to case processing times in security clearance cases.

9.2 The Standing Committee on Scrutiny and Constitutional Affairs' comments to the Committee's annual report for 2022

In its recommendation (p. 11) to the Storting, the Standing Committee asked the EOS Committee to:

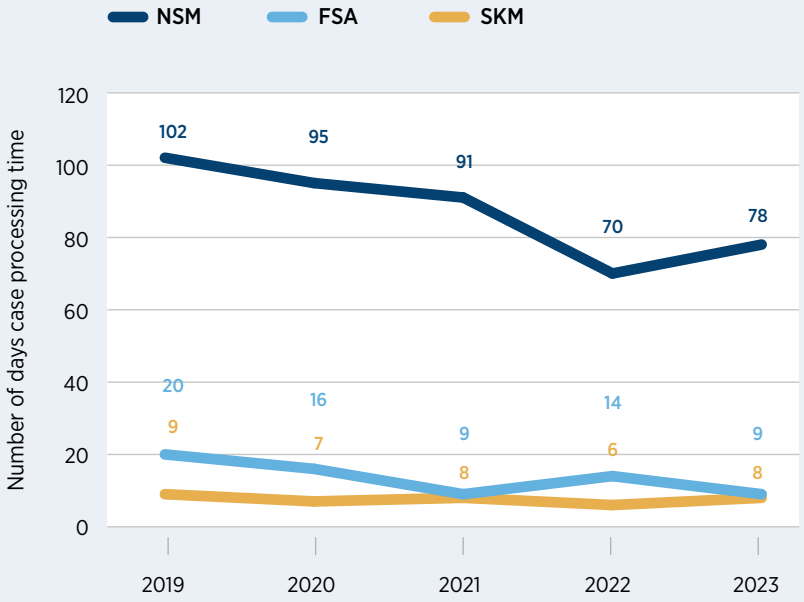
> *'[c]onsider whether the reporting of case processing times in security clearance cases can to a greater extent show the development over time and the circumstances associated with citizens' rights, such as the extent to which delays are due to circumstances on the part of the person requesting clearance or on the part of the services' case processing.'*

Diagrams 1 to 5 show the development in case processing times for different case categories from 2019 to 2023.

Case processing times for requests for access, average number of days

The case processing times for requests for access are relatively short in SKM and FSA at less than ten days on average.

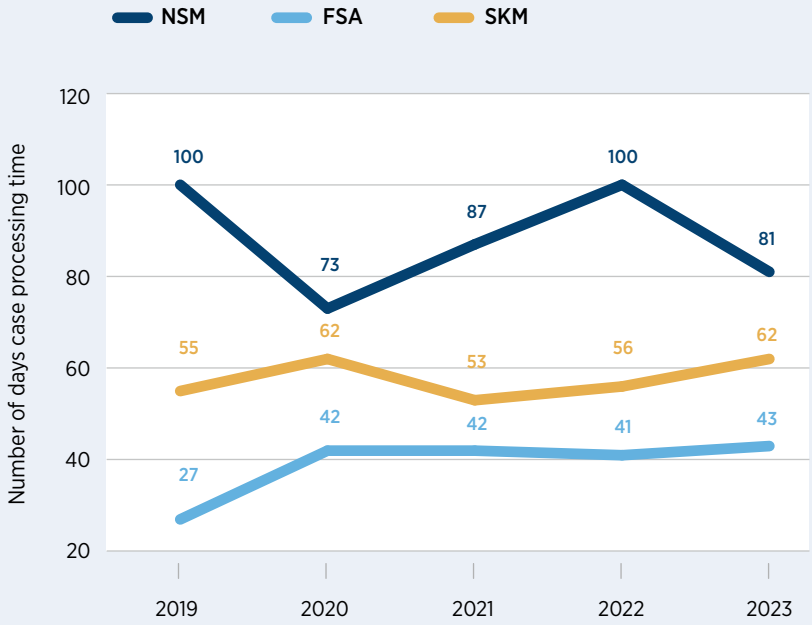
NSM's case processing times are still very long, with an average of 78 days.



31 Recommendation No 456 to the Storting (2022–2023).

Case processing times for requests for security clearance, average number of days for all cases

In 2023, SKM, FSA and NSM reached a decision on security clearance requests after an average of 62, 43 and 81 days, respectively. This includes both positive and negative decisions.

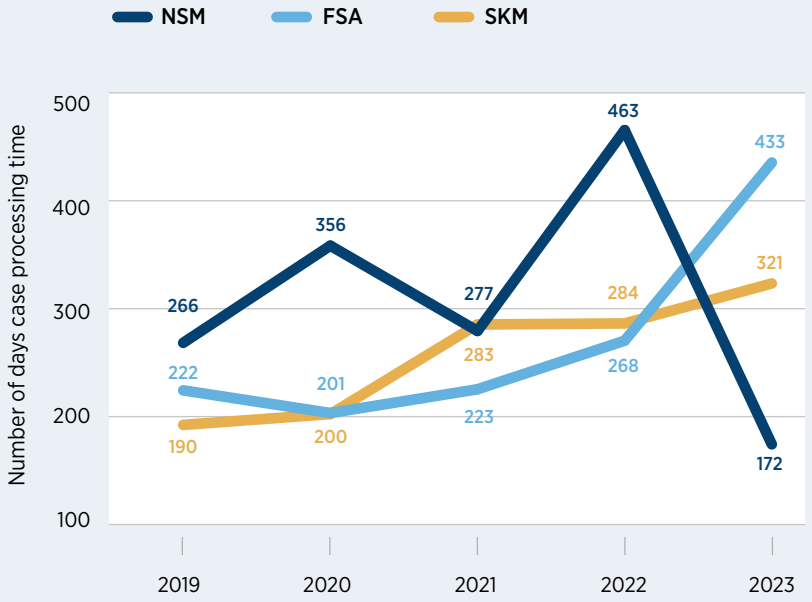


Case processing times for requests for security clearance, average number of days for all cases with a negative result

Case processing times for this category of cases have increased in FSA and SKM since 2020.

In 2023, they averaged 433 days at FSA and 337 days (access clearance) and 321 days (security clearance), respectively, at SKM.

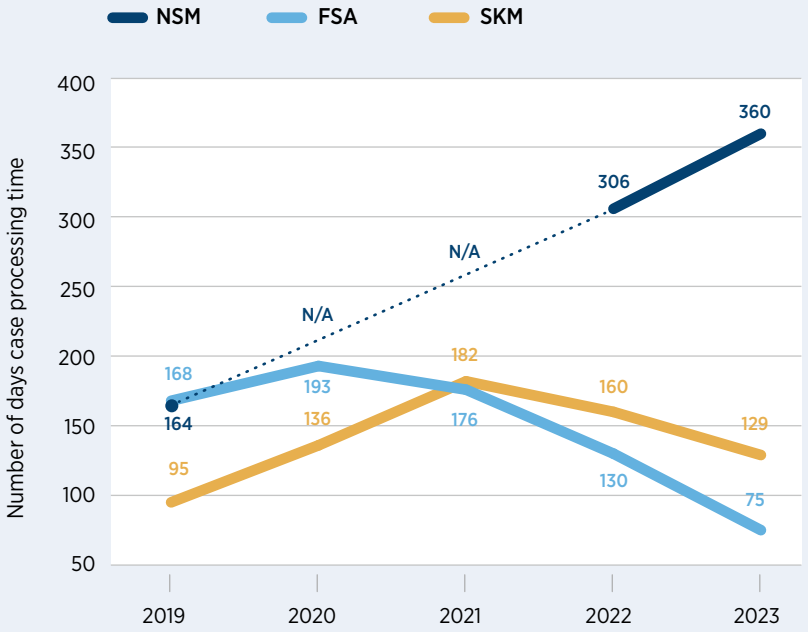
Case processing times in NSM's cases decreased in 2023 to an average of 172 days.



Case processing times for first-tier appeals, average number of days

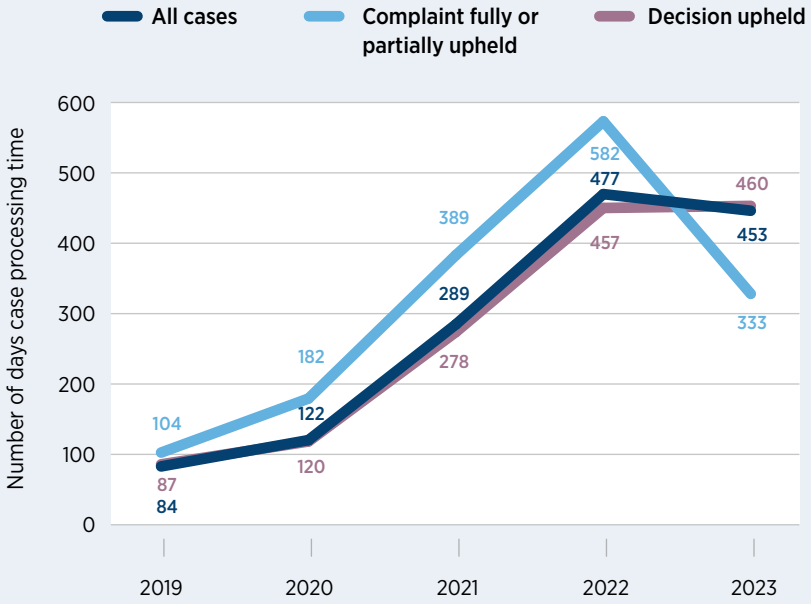
SKM's and FSA's processing of first-tier appeals took an average of 129 and 75 days, respectively, in 2023, which is a decrease from 2022.

NSM's case processing times increased to an average of 360 days (three cases).



Case processing times for second-tier appeals, average number of days

Case processing times in NSM's appeal cases decreased somewhat in 2023, but are still unacceptably long. On average, it took 453 days for an appeal to be decided.



On the basis of the Standing Committee's comments, the Committee has asked SKM, FSA and NSM whether there is or can be obtained information that shows whether the delays in the case processing are due to circumstances on the part of the person for whom security clearance is requested (the vetted person) or to circumstances on the part of the authorities. SKM, FSA and NSM all stated that they saw the need for such statistics. However, they pointed out that such statistics had to be prepared manually due to lack of functionality in their case management system.

In 2023, FSA and SKM reached a decision in 23,590 and 7,594 security clearance requests, respectively. The vast majority of the decisions were positive, and these were decided after an average of 62 and 53 days, respectively. In 2023, NSM decided 104 appeal cases with an average case processing time of 453 days. NSM has previously stated that most of the processing time can be attributed to time spent in the 'queue'. The Committee's spot checks during inspections and the processing of complaint cases reinforce the impression that circumstances on the part of the vetted person are only to a modest extent the reason for the extended case processing times. The establishment of a manual procedure for investigating the issue further would likely require such extensive resources that it would delay the case processing even further.

In the Committee's assessment, it would require a disproportionate amount of resources on the part of the security clearance authority to establish such statistics, relative to the benefits it would provide.

9.3 Case processing times in security clearance cases in 2023

The Committee's inspections in 2023 have shown that many security clearance cases are still not processed within a reasonable time frame. The case processing times in security clearance cases are described in more detail in sections 6.4 (NSM), 7.3 (FSA) and 8.3 (SKM). In 2023, the Committee has also criticised the security clearance authorities for long case processing times in a total of eleven complaint cases.[32] The cases fall under NSM, FSA, SKM and the Ministry of Justice and Public Security.

The case processing times in NSM's appeal cases and its backlog both decreased slightly in 2023. However, the effect of the implemented measures seems to have been modest so far, and case processing times are still unacceptably long. On average, it took 453 days for an appeal to be decided.

In November 2023, NSM had 81 appeals awaiting processing that it had received more than six months previously. There were thus at least 81 cases that had already been pending for longer than the 90 to 120 days that the Ministry had estimated as an acceptable level of case processing time, which NSM was to achieve by 1 July 2023.

NSM has informed the Committee that the case processing times are longer than the directorate would like, and has reported on the measures that have been implemented to reduce the backlog.

FSA and SKM had lower case processing times for requests for security clearance than NSM. However, the Committee is concerned about the case processing times for clearance requests that end in negative results.[33] The processing times for such cases at FSA and SKM have increased since 2020, and averaged 433 days at FSA in 2023. At SKM, the average was 337 and 321 days for access clearance and security clearance, respectively. From the time a decision was appealed, it took an average of 75 days (FSA) and 129 days (SKM), respectively, before the appeal was forwarded to NSM as the appellate body. This is in addition to the appellate body's case processing times. The total case processing times can thus be very long.

The security clearance system must balance important considerations between the individual's due process protection and national security. It is particularly important that the security clearance authorities manage their duties in a satisfactory manner to ensure that the right to a proper and timely review of decisions is safeguarded. Furthermore, there is an embedded guarantee of due process protection in the possibility of having the case reconsidered. The Committee has seen several cases where the quarantine period has expired before the appeal has been processed. In the Committee's opinion, the long case processing times contribute to undermining trust in the security clearance system.

In January 2024, the Committee informed the Ministry of Justice and Public Security about the unacceptably long case processing times in security clearance cases, as well as about the outcome of the complaint cases that the Committee has considered in 2023 and the criticism it has resulted in. The letter is enclosed as Appendix 2. The Committee has emphasised the need for the Ministry to keep close track of developments in this area.

32 In two of the cases, the Committee criticised both the body making the initial decision and the appellate body for long processing times in the same case.

33 This means that clearance is denied, or that clearance is granted at a lower level, for a shorter period of time than requested, or subject to certain conditions.

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 subject to a new assessment until the quarantine period has expired.

10.

Oversight of other EOS services

Photo: Fabian Helmersen / Norwegian Armed Forces

10.1 General information about the oversight

The Committee oversees EOS services regardless of which part of the public administration the services are carried out by. The oversight area encompasses all public bodies that carry out intelligence, surveillance or security services and is not limited to specific organisational entities. The oversight area also includes those who 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 two complaints against other intelligence, surveillance or security services for consideration in 2023. Three complaint cases against other intelligence, surveillance or security services were concluded in 2023. One complaint case against the Norwegian Defence University College was concluded without criticism. Two of the complaint cases resulted in criticism. These are discussed in sections 10.4 and 10.5.

10.2 The Army Intelligence Battalion

The topics addressed in the Committee's inspection of the Army Intelligence Battalion (Ebn) at Setermoen in Troms included Ebn's use of information from open sources (OSINT – open-source intelligence) and electronic warfare capabilities. The Committee was also informed about how these disciplines are used during exercises in Norway. The inspection did not give grounds for follow-up.

10.3 The Norwegian Special Operation Forces

In 2023, the Committee inspected the staff function of the Norwegian Special Operation Forces. The inspection included the Special Operation Forces' processing of personal data. The inspection did not give grounds for follow-up.

10.4 Complaint case against the Ministry of Justice and Public Security

In one case regarding security clearance, the Ministry of Justice and Public Security was criticised for having taken almost six months to process a request for access as the appellate body. The Ministry was also criticised for the fact that the lawyer arrangement required under the Security Act was not established at the conclusion of the Committee's complaint case. NSM was also criticised in the same case, see section 6.3.

10.5 Complaint case against a police unit

On the basis of a complaint against a police unit, the Committee asked about the basis for the creation of a search filter. The purpose of the search filter was to filter out the complainant's activity in an IT system and uncover any abnormal activity.

The Committee found that the measure must in part be considered to constitute the performance of security services, and considered the creation of the search filter in relation to the requirements of the Security of Undertakings Regulations Section 15 third and fourth paragraphs. The Committee did not find that the measure was disproportionately intrusive in relation to the complainant. However, the Committee pointed out that '[w]hen a security measure may interfere with the legal safeguards or right to privacy granted to individuals, the undertaking shall be able to document why such interference is necessary', cf. the Security of Undertakings Regulations Section 15 fourth paragraph. The Committee stated that it could not see that the unit had complied with the requirement for documentation of the necessity of the search filter.

Electronic warfare capabilities
Includes the collection of information from electromagnetic waves, such as radio traffic. The purpose is to provide intelligence and decision-making support, or to limit the enemy's freedom of action.

Performance of security services
Implementation and oversight of prevention measures targeting activities that pose a threat to security and the consequences of such activities.

11.

Appendices

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

- In January, the Committee met with Minister of Defence Bjørn Arild Gram (Centre Party).
- In a meeting in January, the Communications Surveillance Control Committee and the committee chair discussed interfaces between the committees' respective remits.
- In February, the committee chair gave a lecture on the EOS Committee's oversight activities to the participants of the Norwegian National Defence College's senior executive course.
- In April, the Committee held orientation meetings with the Governor of Svalbard and the Svalbard Satellite Station, respectively, in connection with its inspection of PST Svalbard.
- In April and October, the Secretariat held meetings with the Office of the Auditor General on oversights methods and possible overlapping oversight responsibilities.
- In May, the Secretariat visited the Hague in the Netherlands to meet with oversight bodies from Denmark, Sweden, Belgium, the Netherlands, the United Kingdom and Switzerland in the Intelligence Oversight Working Group (IOWG).
- In June, the Secretariat met with the Parliamentary Ombud to exchange oversight experiences.
- In September, the head of the technology unit gave a lecture for Norwegian internet service providers on oversight of the NIS's facilitated bulk collection method.
- In October, the committee chair met members of the Extremism Commission, who wanted to learn more about the Committee's work.
- In November, the EOS Committee, together with the Swedish and Danish oversight bodies, organised the European Intelligence Oversight Conference (EIOC) in Oslo.
- In connection with the EIOC, meetings were also held at the secretariat level and senior level between the oversight bodies involved in the IOWG collaborative project.
- A committee member and the head of the secretariat attended the International Intelligence Oversight Forum conference in Washington DC in the USA. This conference brings together people from all over the world who work in or are interested in the oversight of secret services. The themes of this year's conference included the Council of Europe's Convention 108+ on data protection and how to incorporate security mechanisms in intelligence services' operations.
- In November and December, the Secretariat held meetings with the Norwegian Parliamentary Ombudsman for the Norwegian Armed Forces on inspection methodology.
- In December, the Secretariat held a digital meeting with Lithuania's newly appointed intelligence ombud.

APPENDIX 2 – Letter from the Committee to the Ministry of Justice and Public Security dated 23 January 2024

Deferred public disclosure until
20 March 2024
Cf. the Oversight Act Section 16 fourth paragraph

MINISTRY OF JUSTICE AND PUBLIC SECURITY
P.O. Box 8005 Dep.
NO-0030 OSLO

Our reference
2023/101-15

Date
23 January 2024

Statement from the EOS Committee on case processing times in security clearance cases

Reference is made to the EOS Committee's letter of 2 February 2023 to the Ministry of Justice and Public Security and the Committee's annual report for 2022. In these documents, the Committee drew the Ministry's attention to the fact that developments in NSM's case processing times in security clearance cases in 2022 were considered to give cause for concern. In Recommendation No 456 to the Storting (2022–2023), the Standing Committee on Scrutiny and Constitutional Affairs supported the EOS Committee's assessment.

On this basis, on 3 March 2023,[1] the Ministry requested that NSM take extraordinary measures to bring the backlog of appeal cases down to an acceptable level[2] by 1 July 2023. During the debate in the Storting on 6 June 2023, Minister Emilie Enger Mehl added that NSM had reported that the directorate aimed to achieve the goal within the deadline.

Throughout 2023, the Committee has kept informed of case processing times in the Norwegian National Security Authority (NSM), the Norwegian Defence Security Department (FSA) and the Norwegian Civil Security Clearance Authority (SKM). The Committee's inspections and investigations have shown that many security clearance cases are still not processed within a reasonable time frame.

The case processing times in NSM's appeal cases and NSM's backlog were both slightly reduced in 2023. However, the effect of the implemented measures seems to have been modest so far, and case processing times are still unacceptably long. On average, it took 453 days to decide an appeal case.

In November 2023, NSM had 81 appeals awaiting processing that it had received more than six months previously. There were thus at least 81 cases that had already been pending for longer than the 90 to 120 days that the Ministry had estimated as an acceptable level of case processing time, which NSM was to achieve by 1 July 2023.

NSM has informed the Committee that the case processing times are longer than the directorate would like, and has reported on the measures that have been implemented to reduce the backlog.

1 The Ministry's reference 23/75.

2 Which, according to the Ministry, was a case processing time of between 90 and 120 days.

FSA and SKM had shorter case processing times for requests for security clearance than NSM. However, the Committee is concerned about the case processing times for clearance requests that end in negative results.[3] The processing times for such cases at FSA and SKM have increased since 2020, and averaged 433 days at FSA in 2023. At SKM, the average was 337 and 321 days for access clearance and security clearance, respectively. From the date on which someone appealed a negative decision, it took an average of 75 days (FSA) and 129 days (SKM), respectively, before the appeal was forwarded to NSM as the appellate body. This is in addition to the case processing times for appeal cases. The total case processing times can thus be very long.

In 2023, the Committee has criticised the security clearance authorities for long case processing times in a total of eleven complaint cases.[4] These comprise clearance cases considered by NSM, FSA, SKM and the Ministry of Justice and Public Security. The criticism concerned case processing times from nine months to more than two years and four months in the respective bodies. Five of the cases had still not been decided when the Committee issued its criticism. Two of the cases were concluded by the case being dropped, as the need for clearance had lapsed. In two other cases, the Committee criticised case processing times of four months for requests for access and case processing times of eleven months for requests for a specifically appointed lawyer pursuant to the Security Act.

The security clearance system must balance important considerations between the individual's due process protection and national security. It is particularly important that the security clearance authorities manage their duties in a satisfactory manner to ensure that the right to a proper and timely review of decisions is safeguarded. Furthermore, there is an embedded guarantee of due process protection in the possibility of having the case reconsidered. The Committee has seen several cases where the quarantine period has expired before the appeal has been processed. In the Committee's opinion, the long case processing times contribute to undermining trust in the security clearance system.

With this, the Committee wishes to inform the Ministry of Justice and Public Security of our continued concern about case processing times in security clearance cases, cf. the Oversight Act Section 14 fifth paragraph.

The Committee emphasises the need for the Ministry to keep close track of developments in this area. We ask that the Committee be kept informed of any tasks assigned by the Ministry.

Yours sincerely,

Astri Aas-Hansen
Chair of the EOS Committee

This document has been electronically approved without a signature.

Copy: Ministry of Defence
NSM
FSA
SKM

3 This means that security clearance is denied, or that clearance is granted at a lower level, for a shorter period of time than requested, or subject to certain conditions.

4 In two of the cases, the Committee criticised both the body making the initial decision and the appellate body for long processing times in the same case.

APPENDIX 3 – Act relating to Oversight of Intelligence, Surveillance and Security Services[34]

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

34 The act was last changed on 1 January 2023.

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

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

Section 6. The Committee's oversight

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

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

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

The Committee shall:

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

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

Section 7. Inspections

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

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

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

Section 8. Right of inspection, etc.

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

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

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

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

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

Section 9. Statements, obligation to appear, etc.

All persons summoned to appear before the Committee are obliged to do so.

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

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

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

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

Section 10. Ministers and ministries

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

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

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

Section 11. Duty of secrecy, etc.

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

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

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

Section 12. Procedures

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

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

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

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

Section 13. Quorum and working procedures

The Committee has a quorum when five members are present.

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

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

Section 14. On the oversight and statements in general

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

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

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

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

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

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

Section 15. Statements to complainants and the public administration

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

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

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

Section 16. Information to the public

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

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

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

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

Section 17. Relationship to the Storting

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

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

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

The annual report should include:

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

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

Section 18. Procedure regulations

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

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

Section 18 a. Relationship to the Security Act

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

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

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

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

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

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

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

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

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

Section 19. Assistance etc.

The Committee may engage assistance.

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

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

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

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

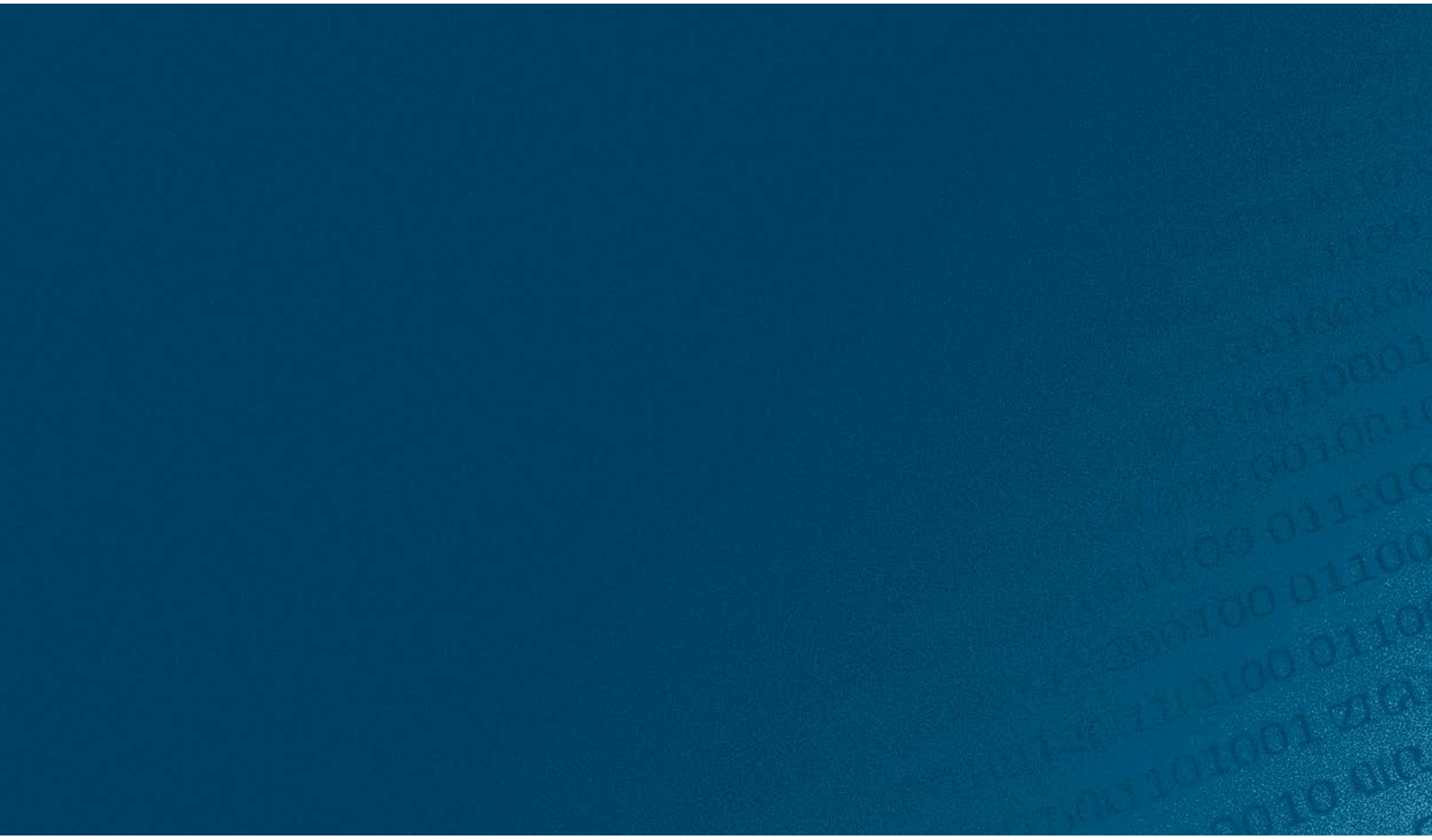
Anyone summoned before the Committee is entitled to reimbursement of any travel expenses in accordance with the State travel allowance scale. Loss of income is reimbursed in accordance with Act No 2 of 21 July 1916 on the Remuneration of Witnesses and Experts.

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

Section 21. Penalties

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

NORWEGIAN PARLIAMENTARY OVERSIGHT COMMITTEE
ON INTELLIGENCE AND SECURITY SERVICES



fdesign.no

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

www.eos-utvalget.no