



**NORWEGIAN PARLIAMENTARY  
OVERSIGHT COMMITTEE**  
ON INTELLIGENCE AND SECURITY SERVICES



# ANNUAL REPORT 2020

**DOCUMENT 7:1 (2020-2021)**





## 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 2020 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. Before the report is submitted to the Storting, the Committee sends the relevant sections of the report to each of the respective services so that they can clarify whether the report complies with this requirement. The services have been given the opportunity to check that there are no factual errors or misunderstandings.

Oslo, 24 March 2021

  
Svein Grønnern

  
Astri Aas-Hansen

  
Øyvind Vaksdal

  
Eldfrid Øfsti Øvstedal

  
Magnhild Meltveit Kleppa

  
Erling Johannes Husabø

  
Camilla Bakken Øvald

  
Henrik Magnusson



Photo: Ingar Sørensen

The EOS Committee in 2020: From left: Øyvind Vaksdal, Camilla Bakken Øvald, Magnhild Meltveit Kleppa, Svein Grønnern (chair), Astri Aas-Hansen (deputy chair), Erling Johannes Husabø and Eldfrid Øfsti Øvstedal.

# Contents

<b>1.</b>	<b>The Committee's remit and composition</b>	<b>6</b>
<b>2.</b>	<b>Overview of the Committee's activities in 2020</b>	<b>9</b>
2.1	Summary – main issues in the oversight of the services	10
2.2	Oversight activities carried out	10
2.3	About the Committee's inspections	10
2.4	The oversight model	12
2.5	More legal advisers needed in the Committee Secretariat	13
2.6	The coronavirus pandemic and the oversight activities in 2020	13
<b>3.</b>	<b>25th anniversary of the EOS Committee</b>	<b>14</b>
3.1	Facts and figures from 25 years of democratic oversight of the Norwegian secret services	15
3.2	Developments in oversight over the past 25 years	16
<b>4.</b>	<b>The Norwegian Police Security Service (PST)</b>	<b>17</b>
4.1	General information about the oversight	18
4.2	Sharing of information with states where there is a risk that human rights will not be respected	18
4.2.1	Introduction	18
4.2.2	PST's sharing of information about a Norwegian citizen with a foreign partner	18
4.2.3	PST's further cooperation with the foreign service	18
4.2.4	About PST's practice for obtaining assurances before sharing information	19
4.3	Follow-up of the special report on PST's unlawful collection and storage of information about airline passengers	20
4.4	Non-conformity reports from PST	20
4.5	Complaint cases against PST	20
<b>5.</b>	<b>The Norwegian Intelligence Service (NIS)</b>	<b>21</b>
5.1	General information about the oversight	22
5.2	National control over information that the NIS shares with foreign partners	22
5.3	Prohibition against covert information collection relating to persons in Norway	22
5.4	Issues relating to an old database of intelligence targets	23
5.5	Review of information previously defined as particularly sensitive	24
5.6	New Intelligence Service Act and oversight of facilitated bulk collection	24
5.6.1	The new Intelligence Service Act	24
5.6.2	About the method facilitated bulk collection	24
5.6.3	About oversight of facilitated bulk collection	25
5.7	Non-conformities in technical information collection	25
5.8	Complaint cases against the NIS	25

<b>6.</b>	<b>The National Security Authority (NSM)</b>	<b>26</b>
6.1	General information about the oversight	27
6.2	Complaint cases against NSM	27
6.2.1	Introduction	27
6.2.2	Complaint case 1 – NSM's right to alter a security clearance decision to the detriment of the complainant	27
6.2.3	Complaint case 2 – Unreasonably long case processing times in a security clearance case	28
6.2.4	Complaint case 3 – Concerning access to correspondence between NSM and the EOS Committee	29
6.2.5	Complaint case 4 – FSA and NSM's processing of a request for access to information about a security clearance case	29
6.3	Case processing times in security clearance cases	29
<b>7.</b>	<b>The Norwegian Defence Security Department (FSA)</b>	<b>30</b>
7.1	General information about the oversight	31
7.2	Complaint cases against FSA	31
7.2.1	Introduction	31
7.2.2	Complaint case 1 – FSA and NSM's processing of a request for access to information about a security clearance case	31
7.2.3	Complaint case 2 – Unreasonably long case processing times in a security clearance case	32
7.3	Case processing times in security clearance cases	32
<b>8.</b>	<b>Oversight of other EOS services</b>	<b>33</b>
8.1	General information about the oversight	34
8.2	Inspection of the Army Intelligence Battalion	34
8.3	Inspection of the Norwegian Special Operation Command	34
8.4	The Norwegian Civil Security Clearance Authority (SKM)	34
8.4.1	Planned inspection postponed	34
8.4.2	Case processing times in security clearance cases	34
<b>9.</b>	<b>Cooperation between the EOS services</b>	<b>35</b>
9.1	On the cooperation between PST and the Norwegian Intelligence Service	36
<b>10.</b>	<b>The investigation into the Frode Berg case</b>	<b>37</b>
<b>11.</b>	<b>Communication and external relations</b>	<b>38</b>
11.1	Communication	39
11.2	International cooperation	39
<b>12.</b>	<b>Appendices</b>	<b>40</b>
	Appendix 1 – Meetings, visits, lectures and participation in conferences etc.	41
	Appendix 2 – News from foreign oversight bodies	42
	Appendix 3 – Input to the Storting's consideration of the new Intelligence Service Act	43
	Appendix 4 – Act relating to oversight of intelligence, surveillance and security services	46



**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 services (EOS services). Only EOS services carried out by, under the control of or initiated by the public administration are subject to oversight by the EOS Committee.<sup>1</sup>

Pursuant to the Oversight Act<sup>2</sup> Section 2 first paragraph, 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 shall not seek more extensive access to classified information than warranted by its oversight purposes.<sup>3</sup> The Committee shall insofar as possible show consideration for the protection of sources and safeguarding of information received from abroad. Subsequent oversight is practised in relation to individual cases and operations, but

we are 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 consultation purposes or ‘prior approval’ of methods, operations etc. The oversight shall cause as little inconvenience as possible to the services’ operational activities, and the Committee shall show consideration for national security and relations with foreign powers in its oversight activities.<sup>4</sup>

The Committee conducts reviews of legality. This means, for example, that we do not review the services’ effectiveness or how they prioritise their resources.

The Committee has seven members. They are elected by the Storting in plenary session on the recommendation of the Storting’s Presidium for a term of up to five years.<sup>5</sup> No deputy members are appointed. The Committee is independent of both the Storting and the Government.<sup>6</sup> This means that the Government cannot issue instructions to the Committee, and members of the Storting cannot also be members of the Committee. 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.<sup>7</sup> This means security clearance and authorisation for TOP SECRET and COSMIC TOP SECRET.

- 1 References to the Oversight Act are found in the Act relating to National Security (the Security Act) Section 11-1, the Act relating to the Norwegian Intelligence Service (the Intelligence Service Act) Section 2-6, and the Act relating to the Processing of Data by the Police and the Prosecuting Authority (the Police Databases Act) Section 68.
- 2 Act No 7 of 3 February 1995 relating to the Oversight of Intelligence, Surveillance and Security Services (the Oversight Act). The Act was most recently amended in June 2020.
- 3 Cf. the Oversight Act Section 8 third paragraph. It is stated in the Oversight Act Section 8 fourth paragraph that the Committee can make binding decisions regarding right of access and the scope and extent of oversight. Any objections shall be included in the annual report, and it will be up to the Storting to express an opinion about the dispute, after the requested access has been granted (no suspensive effect). In 1999, the Storting adopted a plenary decision introducing a special procedure that would apply in connection with disputes about access to Norwegian Intelligence Service documents. The decision did not lead to any amendments being made to the Act or Directive governing the Committee’s oversight activities, see Document No 16 (1998–1999), Recommendation No 232 to the Storting (1998–1999) and minutes and decisions of the Storting from 15 June 1999. The Storting’s 1999 decision was based on the particular sensitivity associated with some of the Norwegian Intelligence Service’s sources, the identity of persons with roles in occupation preparedness and particularly sensitive information received from foreign partners. In 2013, the EOS Committee asked the Storting to clarify whether the Committee’s right of inspection as enshrined in the Act and Directive shall also apply in full in relation to the Norwegian Intelligence Service, or whether the Storting’s decision from 1999 shall be upheld. At the request of the Storting, this matter was considered in the report of the Evaluation Committee for the EOS Committee, submitted to the Storting on 29 February 2016, see Document 16 (2015–2016). When the Evaluation Committee’s report was considered in 2017, the limitations on access to ‘particularly sensitive information’ were upheld without the wording of the Act being amended.
- 4 Cf. the Oversight Act Section 2.
- 5 Cf. the Oversight Act Section 3.
- 6 ‘The Storting in plenary session may, however, order the Committee to undertake specified investigations within the oversight mandate of the Committee,’ cf. the Oversight Act Section 1 final paragraph second sentence.
- 7 Cf. the Oversight Act Section 11 second paragraph.

#### Non-statutory law

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

#### Classified information

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

#### Review of legality

Review to ensure that rules of law are complied with.

#### Security clearance

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

#### Authorisation

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

Below is a list of the committee members and their respective terms of office for 2020:

<b>Svein Grønnern</b> , Oslo, chair 13 June 1996 – 30 June 2021
<b>Astri Aas-Hansen</b> , Asker, deputy chair 1 July 2019 – 30 June 2024
<b>Øyvind Vaksdal</b> , Karmøy 1 January 2014 – 30 June 2021
<b>Eldfrid Øfsti Øvstedal</b> , Trondheim 1 July 2016 – 30 June 2021
<b>Magnhild Meltveit Kleppa</b> , Hjelmeland 1 July 2019 – 30 June 2024
<b>Erling Johannes Husabø</b> , Bergen 1 July 2019 – 30 June 2024
<b>Camilla Bakken Øvald</b> , Oslo 1 July 2019 – 30 June 2024

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

The Committee is supported by a secretariat. At year end 2020, the Secretariat consisted of sixteen full-time employees – the head of the secretariat (who has a law degree), six legal advisers, five technological advisers, one head of security, one communications adviser and two administrative advisers in charge of financial matters, HR, archive and office functions.

The Committee's expenses amounted to NOK 23,257,049 in 2020, compared with a budget of NOK 26,497,000, including transferred funds. The Committee has applied for permission to transfer NOK 1,300,000 of the unused funds of NOK 3,239,951 to its budget for 2021.

In 2019, the Committee was allocated NOK 29,000,000 for new premises. As of 31 December 2020, unused funds in the relocation project amounted to NOK 2,308,669. These funds will be transferred to 2021 to cover the remaining costs related to the project.





2.

## Overview of the Committee's activities in 2020

## 2.1 Summary – main issues in the oversight of the services

### The Norwegian Police Security Service (PST):

The Committee has criticised PST in a case concerning the exchange of information about a Norwegian citizen with a service in a country where there is a risk that human rights will not be respected. In connection with a review of PST's exchange of information with foreign services, the Committee looked into the exchange of information about a Norwegian who was imprisoned abroad. The Committee stated that PST's assessment of the risk associated with disclosing information about the person in question to PST's partner in the country in question, was inadequate.

### The Norwegian Intelligence Service (NIS):

The Committee has full right of access to all the EOS services' ongoing cases, with one exception: cases that the NIS defines as involving 'particularly sensitive information'. In 2019 and 2020, we reviewed 19 cases/operations dating back several years that were no longer defined as 'particularly sensitive information'. The Committee has found no indications that the NIS has exceeded its powers or that the rights of any person have been violated.

### The National Security Authority (NSM) and the Norwegian Defence Security Department (FSA):

- In a complaint case, the Committee has concluded that the complainant's rights were violated when NSM on incorrect grounds altered a security clearance decision from CONFIDENTIAL to no clearance.
- FSA and NSM were both criticised by the Committee for unreasonably long case processing time in connection with a complaint case. More than four years elapsed from the complainant submitted personal information as the basis for security clearance until NSM made its final decision to deny security clearance.
- Both NSM and FSA were criticised in a complaint case that concerned access to information in a security clearance case. The complainant was denied access to factual information recorded in an internal document. Moreover, a duty of secrecy under criminal liability was imposed on the complainant regarding information provided to the security clearance authority by the complainant.

## 2.2 Oversight activities carried out

In 2020, the Committee conducted 16 inspections and visited all entities required by the Act. The Police Security Service (PST) was inspected six times, the Norwegian

Intelligence Service (NIS) four times, the National Security Authority (NSM) twice and the Norwegian Defence Security Department (FSA) twice. The Army Intelligence Battalion and Norwegian Special Operation Forces were both inspected once.

The Committee raised 16 cases on its own initiative in 2020, compared with 24 in 2019. The cases raised by the Committee on its own initiative are mostly follow-up of findings made during our inspections. We concluded 10 cases raised on the Committee's own initiative in 2020, compared with 17 cases in 2019.

The Committee investigates complaints from individuals and organisations. In 2020, the Committee received 29 complaints<sup>8</sup> against the EOS services, compared with 26 complaints in 2019. Complaints that fall within the Committee's oversight area are investigated in the service or services that the complaint concerns, and we have a low threshold for considering complaints.

The EOS Committee members normally meet for several days every month, except in July. The workload of the chair of the committee corresponds to about 30% of a full-time position, while the office of committee member is equivalent to about 20% of a full-time position. In 2020, we had nine internal working meetings at the Committee's office, a digital meeting on unclassified issues in the spring and internal working meetings on site in connection with inspections. During our internal meetings, we discuss planned and completed inspections, complaint cases, cases raised on the Committee's own initiative, reports to the Storting and administrative matters.

## 2.3 About the Committee's inspections

The Committee's inspections consist of a briefing part and an inspection part. The services' briefings are a useful way of giving us insight into the services' views of their responsibilities, assessments and challenges. The topics for the briefings are mostly selected by the Committee, but the services are also asked to brief us on any matters they deem to be relevant to the Committee's oversight. During the inspections, we are briefed, among other things, about the service's ongoing activities, its national and international cooperation and issues that have triggered public debate. The Committee asks oral questions during the briefings and sends written questions afterwards. We can also summon the services' employees and other parties of relevance to the oversight for interviews or questioning.

<sup>8</sup> The Committee rejected a small number of complaints because they did not fall within the Committee's oversight area. A fair number of complaints were against more than one of the EOS services

## Inspections by the Committee in 2020



During the inspection part, we conduct searches directly in the services' electronic systems. The services are not informed about what we search for. This means that the inspections include considerable unannounced elements. The Secretariat makes thorough preparations, which enable us to conduct targeted inspections.

## 2.4 The oversight model

The EOS Committee was evaluated by the Solbakken Committee in 2016.<sup>9</sup> Some changes were made following the evaluation, but the general model whereby the Committee oversees all the EOS services and comprises seven members from a broad range of backgrounds, was retained.

The introduction of the new Intelligence Service Act, and possible implementation of facilitated bulk collection of transboundary communication<sup>10</sup>, will entail many new responsibilities for the Committee. The Committee will receive funding to increase the number of positions in the Secretariat, but it will also have a bearing on the work of the Committee itself.

The Storting's Standing Committee on Foreign Affairs and Defence wrote the following in its recommendation<sup>11</sup> concerning the new Intelligence Service Act:

'The Committee has noted the input from the EOS Committee in which it is pointed out that such a new oversight responsibility will necessitate a review of its oversight activities and priorities, and that the EOS Committee will get back to the Storting if necessary after gaining experience of the new oversight responsibility.'

The input that the Standing Committee refers to is a letter it received from the EOS Committee in connection with the Storting's consideration of the new Intelligence Service Act.<sup>12</sup> Copies of the letter were sent to the Standing Committee on Scrutiny and Constitutional Affairs and the Storting's Presidium.

In the letter, we expressed our expectations that continuous oversight of facilitated bulk collection will 'necessitate a review of the Committee's oversight activities and priorities'.

In autumn 2020, the Committee began to consider how the oversight model can be developed within the applicable framework conditions for the committee members.



Because of the pandemic, the chair of the EOS Committee, Svein Grønnern, delivered the annual report for 2019 to Tone Wilhelmsen Trøen, President of the Storting, in a digital meeting. Photo: Stortinget



Among other things, we are looking into whether it is possible to expand the Committee's inspection capacity by splitting the Committee and developing new ways of conducting inspections. Access to the services' systems from the Committee's premises could also help to increase capacity. The Committee is also in the process of implementing increased use of risk assessments to determine where to conduct inspections and what topics to focus on during inspections. The Committee will revisit the matter of any needs for legislative amendments and budgetary consequences of the continued work on the oversight model.

## 2.5 More legal advisers needed in the Committee Secretariat

In recent years, several new statutory provisions have granted PST wider surveillance powers. The service has also been given extended rights to use existing legal bases for averting and preventive purposes. In a statement<sup>13</sup> on the Norwegian government's website, Minister of Defence Frank Bakke-Jensen and Minister of Justice and Public Security Monica Mæland write: 'Work on examining and updating PST's legal authority is currently under way. We agree that PST cannot be an analogue service in a digital age, and we are also looking at how the service's role as a domestic intelligence service should be strengthened.'

The new Intelligence Service Act (2020) and Security Act (2018), as well as the increasingly close and organised collaboration between the different EOS services, will also make greater demands of the Committee's oversight work. Together, these developments mean that the Committee will have more and more complex legal issues to consider. It is a significant burden on the Committee that oversight mechanisms are increasingly viewed as preconditions for the provisions providing legal authority for lawful surveillance.

The Secretariat's current legal adviser capacity is not sufficient to enable the Committee to fulfil these requirements in a satisfactory manner, and the Committee considers it necessary to further strengthen the Secretariat towards 2025.

The Committee is regularly assigned comprehensive and particularly time-consuming cases to look into. In connection

with work on such cases, it is imperative that the Committee has enough legal advisers to allow it to deal with day-to-day oversight work as well as conduct such special investigations. That is not the situation at present. The Secretariat's legal adviser capacity is currently not sufficient to investigate cases in the EOS services to the extent that the Committee would like.

In connection with its work on the budget for 2022, the Committee will present an overview of the expected budgetary needs for the period until 2025.

## 2.6 The coronavirus pandemic and the oversight activities in 2020

The oversight activities in 2020 were less extensive than planned due to infection control measures resulting from the coronavirus pandemic. In the period from March to May 2020, the Committee held an unclassified digital meeting and conducted two inspections with fewer committee members present than would usually have been the case. Since June 2020, it has been more or less business as usual, except for somewhat limited participation in inspections due to infection control considerations.

There has been a good dialogue between the Committee and the EOS services on the facilitation of inspections and the Secretariat's preparations in light of official recommendations, measures and instructions. As shown in Chapter 2, the EOS Committee has met the minimum requirement for inspection activities in 2020.

The Secretariat's case processing capacity was substantially reduced during the period from March to May 2020. Most of the staff have worked at the office in autumn 2020, as most of them cannot do their work from home. All employees have their own cell offices, and steps have been taken to help secretariat employees to travel to and from work without having to use public transport.

The pandemic has resulted in longer case processing times for complaint cases and cases raised by the Committee on its own initiative. We have also raised fewer cases on our own initiative than we would have done in a normal year.

9 Document 16 (2015–2016) – Report to the Storting from the Evaluation Committee for the Norwegian Parliamentary Intelligence Oversight Committee (EOS Committee).

10 Read more in section 5.6.2.

11 Recommendation 357L to the Storting (2019-2020).

12 Appendix 3 to this annual report.

13 [Regjeringen.no/no/aktuelt/eostjenestene/id2834667/](https://regjeringen.no/no/aktuelt/eostjenestene/id2834667/)

3.

25th anniversary of  
the EOS Committee

### 3.1 Facts and figures from 25 years of democratic oversight of the Norwegian secret services

The submission of this annual report to the Storting in March 2021 takes place almost exactly 25 years after the first meeting of the EOS Committee. Since then, the Committee has held hundreds of meetings and submitted 25 annual reports and 11 special reports:

- *On classified information in the Frode Berg case* (2021)
- *On PST's unlawful collection and storage of information about airline passengers* (2019)
- *On differing practices in the security clearance of persons with connections to other states* (2019)
- *The legal basis for the Norwegian Intelligence Service's surveillance activities* (2016)
- *The Committee's duty of secrecy vis-a-vis the Evaluation Committee* (2014)
- *Investigation into allegations of politically motivated surveillance and PST's use of Christian Høibø as a source* (2014)
- *Investigation into information about Norwegian sources etc. in the Norwegian Intelligence Service* (2013)
- *PST's registration of persons affiliated to two Muslim groups* (2013)

- *Surveillance of Norwegian citizens in Norway carried out by SDU* (2011)
- *Investigation into the methods used by the Norwegian Police Surveillance Service (POT) in the Treholt case* (2011)
- *Investigation into the Surveillance Service's collection of information from the former DDR* (1996)

If we add up activities from April 1996, when the Committee had its first meeting, up to and including December 2020, we arrive at the following statistics:

The Committee has received 627 complaints, raised 474 cases on its own initiative, carried out 591 inspections and held 458 meetings.

The EOS Committee's first chair was Per N. Hagen (1996–1997). Rikard Olsvik replaced him in 1997 and chaired the Committee until 1999. Leif Mevik was chair of the Committee from 1999 to 2006, followed by Helga Hernes from 2006 to 2011. Eldbjørg Løwer was the Committee's longest-serving chair to date (2011 to 2019). Current chair Svein Grønnern will retire as chair of the Committee in summer 2021 after having been a member of the EOS Committee for 25 years.



Per N. Hagen (right) was the first chair of the EOS Committee. This picture from 1997 shows him together with the politician Berge Furre who was central to the first special report that the EOS Committee issued to the Storting in 1996. Photo: Gunnar Lier/NTB

To mark the anniversary, the Committee will publish an anniversary booklet (in Norwegian only) containing contributions from present and former members, as well as from external persons who have followed the Committee over several years.

### 3.2 Developments in oversight over the past 25 years

Both the services and the Committee's oversight have changed a great deal from the mid-90s until the present day. The services' budgets have substantially increased, and the number of secretariat employees is many times what it was.

In the 1990s and early 2000s, the inspections were dominated by paper files and frequent visits to the services' archives. Today, the EOS Committee, supported by the technological advisers in the Secretariat, has access to the same digital tools as the services use. As a result of this development, conditions are much more favourable for effective oversight today than in 1996, despite the vast increase in the amount of information held by the services.

Technology has progressed by leaps and bounds, but that is not the only development that the world, the services and the Committee have experienced. Events in Norway and abroad have led to changes in the services' priorities as well as amendments of the legislation governing the services. PST, in particular, has been authorised to use many more

methods, including in prevention cases. And the new Act relating to the Norwegian Intelligence Service entered into force on 1 January 2021.<sup>14</sup> The Committee with the support of the Secretariat are charged with overseeing all of this. In the 1990s, the seven committee members had only a few people to support them. In 2021, the Secretariat will have more than 20 employees. Nearly one-third of them will be technological advisers, which means that the Committee's ability to oversee the services' complicated computer systems and large quantities of data is quite different from what it was only a few years ago.

However, there is one important thing that has not changed over the past 25 years – the EOS Committee's remit. Our main task is still to ascertain whether the rights of any person are violated and to prevent such violations, ensure that the EOS services' activities do not unduly harm the interests of society, and that our secret services keep their activities within the legislative and regulatory bounds that apply.

Although the core of the Committee's remit remains the same, there has been a constant development in oversight methods. The Oversight Act in particular has proven to be effective when faced with services that have not always been obliging in relation to the Committee's requests for access to information. The right of inspection and access to information has been a vital prerequisite for the oversight – and for confidence in it. In light of regulatory changes as well as changes in what is technically possible, it is a continuous task for the Committee to make sure that the EOS services facilitate our oversight.



The EOS Committee in 2010: From left: deputy chair Svein Grønnern, member Trygve Harvold, member Wenche Elizabeth Arntzen, member Theo Koritzinsky, member Knut Hanselmann, head of the secretariat Henrik Magnusson and chair Helga Hernes. The committee member Gunhild Øyungen was not present when the picture was taken.

Photo: Erik Johansen / NTB

<sup>14</sup> Read more in section 5.6 of this annual report.





4.

## The Norwegian Police Security Service (PST)

## 4.1 General information about the oversight

In 2020, the Committee conducted four inspections of the PST headquarters (DSE). The Committee also inspected the PST entities in Troms and Western police districts.

In our inspections, we focus on the following:

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

## 4.2 Sharing of information with states where there is a risk that human rights will not be respected

### 4.2.1 Introduction

The Committee checks whether the conditions for PST's disclosure of information to foreign services are met.<sup>15</sup>

In a statement to PST, the Committee commented on the service's exchange of information about a Norwegian citizen with a service in a country where there is a risk that human rights will not be respected. In the same case, the Committee expressed its view on PST's cooperation with the foreign service and PST's practice as regards obtaining assurances before information is shared.

### 4.2.2 PST's sharing of information about a Norwegian citizen with a foreign partner

The Committee reviewed PST's exchange of information about a Norwegian person imprisoned abroad with a foreign service. PST had an investigation case concerning the person in question.

PST was asked to explain its cooperation with the foreign service and whether the exchange of information about the Norwegian citizen was necessary and proportional.

The service referred to the fact that it had completed an internal risk assessment form before it first shared information about the Norwegian with the foreign service.

PST considered there to be a 'low probability' that the sharing of information would have negative consequences for the person in question, considering that the person was already in prison at the time when the information was shared.

The Committee took a somewhat different view of the matter. We failed to see that the completed form was sufficient to substantiate that PST had conducted an overall assessment of whether the disclosure was proportional. The Committee expressed the opinion that precisely the fact that the person was imprisoned necessitated a particularly thorough assessment of whether the conditions for information sharing were met. In our opinion, PST's assessment of the risk associated with disclosing information about the person in question was inadequate.

PST's *subsequent* decision to share information from its own investigation case was thorough and carefully considered. The Committee nevertheless believes that PST should also have considered more risk-reduction measures. PST could have obtained assurances from the foreign service in question about its ability and willingness to respect human rights before sharing information about the Norwegian citizen who was imprisoned at the time.

### 4.2.3 PST's further cooperation with the foreign service

After PST had shared the above-mentioned information, the service learned of indications that the foreign service had allegedly used information from PST in a manner that was in breach of the conditions that the PST had stipulated for its use. PST informed the Committee that there was no evidence to suggest that the disclosed information was used against the Norwegian citizen, neither in a criminal case nor in that the Norwegian suffered cruel, inhuman or degrading treatment.

As a consequence of these indications, PST considered discontinuing information sharing with the foreign service. PST was not able to fully clarify whether information it had shared had been used in breach of the conditions set. Nevertheless, PST chose to continue to share information and cooperate with the foreign service.

The fact that shared information may have been used in a manner that was in breach of the conditions set by PST illustrates the core of the problem of sharing personal data with states where there is a risk that human rights will not be respected. The Committee stated that it is problematic that PST has continued to share information with the

#### Personal data processing

Any form of electronic or manual processing of personal data – including storage.

#### Prevention case

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

#### Averting investigation case

Case opened for the purpose of averting a criminal offence that falls within PST's area of responsibility.

foreign service in question without fully clarifying whether the foreign partner may have misused information previously shared by PST.

#### 4.2.4 About PST's practice for obtaining assurances before sharing information

PST has a procedure in place describing what the service should do before each instance of disclosing information to countries where there is a risk of human rights violations. When the disclosure of personal data could entail a risk of human rights violations, PST should consider whether to obtain assurances concerning the recipient's ability and willingness to respect human rights.

In the above case, no such assurance had been obtained from the foreign service. PST was of the opinion that such assurances are of 'very limited, if any, value', as it is the internal assessments and investigations carried out by the service itself before sharing information that can prevent cruel, inhuman or degrading treatment. PST also stated that conditions stipulated by the service in connection with previous instances of information sharing contain conditions/provisions that 'the information is shared as intelligence information only and cannot be shared with other authorities

or used for prosecution purposes or other judicial processes without the consent of PST'.

Before PST concludes in a concrete case that it will disclose personal data to countries where there is a risk of human rights violations, the Committee assumed that the service considers whether obtaining assurances is a relevant way of clarifying whether the recipient is willing and able to respect human rights.

The Committee has noted that PST has decided that all new communications from PST to partners in which personal data are shared, will contain new and comprehensive restrictions on access that specify the established practice of avoiding cruel, inhuman or degrading treatment as a result of the information being disclosed. The Committee takes a positive view of this.

We expect PST to keep informed about any changes in the human rights situation in relevant countries, including how foreign partners respect human rights. We also expect that Norwegian services must exercise caution when exchanging information about individuals with states where there is a risk that human rights will not be respected.



15 The Police Databases Act Section 22 allows PST to disclose information to foreign authorities for such purposes as mentioned in Section 26 of the Act, as well as in order to avert or prevent criminal offences or if disclosure is necessary in order to verify the data. This relates to PST's duty to cooperate with the police authorities and security and intelligence services of other countries, see the Police Act Section 17c.

#### Investigation case

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

#### Equipment interference

A method that allows for continuous collection of information from a mobile phone/computer. PST can use this method subject to court approval.

### 4.3 Follow-up of the special report on PST's unlawful collection and storage of information about airline passengers

On 5 December 2019, the Committee submitted a special report to the Storting 'On PST's unlawful collection and storage of information about airline passengers'.<sup>16</sup> In this report, the Committee strongly criticised PST for having unlawfully collected and stored information about airline passengers.

The EOS Committee has asked PST what steps the service has taken to follow up the special report. PST replied that a number of internal measures have been implemented to obtain an overview of the information and process it in accordance with the Committee's comments and within the bounds of the law. This extensive material was collected over a period of several years.

In the special report, the Committee also criticised the fact that PST lacked sufficient internal control and documentation of its own collection activities. PST is now in the process of establishing a new entity that will take responsibility for internal control and risk management in the service.

The Committee is pleased with the service's follow-up so far and will continue to follow up the matter.

### 4.4 Non-conformity reports from PST

PST has in recent years informed the Committee about non-conformities on its own initiative. The Committee takes a positive view of the fact that PST reports non-conformities that the service itself has identified. This year, the service has informed the Committee of three matters.

One of the non-conformities was related to the use of fake base stations. The case concerned a police district that requested assistance from PST in locating a mobile phone in a serious case. The request for assistance was not submitted in writing, as it should normally be. It turned out

that, although the police district had obtained court approval for lawful interception of communication in the case, the court decision did not cover the use of a fake base station. PST has reported the matter to the Director of Public Prosecutions and tightened its procedures for dealing with requests for assistance it receives from the ordinary police.

The second non-conformity arose in connection with the new Penal Code. When the new Penal Code came into force, the legal authority for some of the service's tasks became unclear. This may have resulted in information being registered in error in PST's register. The service has appointed a group to review the registrations in question. PST is also working to clarify the legal authority.

Finally, PST has informed the Committee about a possible non-conformity in connection with the transfer of personal data from a register to the intelligence register Smart. The service has informed the Committee that it will review its entire internal control system.

### 4.5 Complaint cases against PST

The Committee received 19 complaints against PST in 2020, compared with 13 complaints in 2019. Some of these complaints also concerned other EOS services.

The Committee's statements to complainants shall be unclassified. Information about whether a person has been under surveillance or not, is classified unless otherwise specified. This means that, in principle, a complainant cannot be told whether he or she is under surveillance by PST. The Oversight Act dictates that statements in response to complaints against the services concerning surveillance activities shall only state whether or not the complaint contained valid grounds for criticism.

The Committee concluded 13 complaint cases against PST in 2020. None of these cases resulted in criticism of the service.

<sup>16</sup> Document 7:2 (2019–2020).

#### Fake base station

A fake base station poses as a legitimate one. It can function as an intermediary between a mobile phone and the network provider's legitimate base station. It can be used to identify the mobile phones that contact the fake base station, and can potentially intercept mobile phone communication, listen to calls, read text messages and see mobile data traffic.



5.

# The Norwegian Intelligence Service (NIS)

## 5.1 General information about the oversight

The Committee conducted three inspections of the NIS headquarters in 2020, in addition to inspections of the Norwegian Intelligence Service station at Eggemoen, Ringerike, which collects information from selected satellites.

During our inspections of the NIS, we focus on the following:

- that the service does not violate the statutory prohibition against performing surveillance or in any other covert manner procuring information concerning persons on Norwegian territory<sup>17</sup>
- the NIS's technical information collection
- the service's processing of information in its computer systems
- the service's exchange of information with domestic and foreign services
- national control of the NIS's stations, equipment, methods and information sharing
- matters of particular importance or that raise questions of principle that have been submitted to the Ministry of Defence<sup>18</sup> and internal approval cases<sup>19</sup>

The Committee's full right of access to information in the services has one exception – access to information defined as particularly sensitive information by the NIS. The Committee is regularly informed about the scope of information that falls within this category.

## 5.2 National control over information that the NIS shares with foreign partners

In the annual report for 2019, we described our oversight of how the NIS ensures national control over what intelligence information is disclosed to foreign partners. In 2020, we have reviewed the NIS's most important cooperation agreements. The Committee has focused on checking whether the agreements are capable of ensuring that national control over what information is disclosed to foreign partners is adequately addressed.

The NIS has provided satisfactory answers to the Committee's questions, and we have emphasised the importance of national control in this area.

We have also referred to the fact that part of the purpose of the requirement for national control is to facilitate *subsequent oversight*, which is also stated in the proposition to the Storting concerning the new Act relating to the Norwegian Intelligence Service.<sup>20</sup>

We are aware that, in some cooperation areas, it will be challenging for the NIS to reconstruct all information for subsequent oversight. However, we have assumed that the Committee's subsequent oversight will be facilitated insofar

as this is possible in relation to shared information that *may* contain information about Norwegian citizens. This applies to both existing and new cooperation platforms.

The EOS Committee has followed the media coverage of developments in what is known as 'the FE scandal' in Denmark. The background to this scandal is a special report on the Danish Defence Intelligence Service (FE) from the Danish oversight body, the Danish Intelligence Oversight Board, and the Danish media's claims of inadequate national control over the sharing of intelligence information with a foreign partner.<sup>21</sup>

National control has been an important oversight area for many years and will continue to be so in future. In 2020, the Committee inspected, among other things, the NIS's station at Ringerike where information from satellites is collected.

## 5.3 Prohibition against covert information collection relating to persons in Norway

The Intelligence Service Act Section 4 first paragraph contains a prohibition against the NIS performing surveillance or, in any other covert manner, procuring information concerning Norwegian persons on Norwegian territory.

We have concluded two cases in 2020 that involved issues relating to this prohibition. What the cases have in common is that the activities of the NIS, which should target matters of relevance to foreign intelligence activities, indirectly concern Norwegian persons in Norway, i.e. that Norwegians abroad who are under surveillance by the NIS are in contact with Norwegians in Norway. None of these cases resulted in criticism of the NIS.

In one of the cases, the Committee considered whether the NIS had tried to obtain information about a Norwegian in Norway via a target abroad.

In response to the Committee's questions, the NIS stated that the purpose of the collection of information about the target abroad was not to obtain 'domestic Norwegian communication in breach of the Intelligence Service Act Section 4' or any 'active attempt to collect surplus information from the Norwegian connection'. The service acknowledged that the wording of parts of the underlying written material was unclear and 'could leave room for doubt as to the true purpose of the collection'.

On the basis of the documents in the case and the replies received from the NIS, the Committee concluded that the NIS had not acted in violation of the Intelligence Service Act Section 4 first paragraph.

The Committee nevertheless advised the NIS to word its

grounds for initiating covert collection targeting persons abroad in such cases more clearly in future. We also requested the NIS to make it clearer in the underlying written material that no collection activities will be initiated targeting Norwegians in Norway via a person abroad.

#### 5.4 Issues relating to an old database of intelligence targets

In a case concerning the NIS's personal data processing in an old database of intelligence targets, the Committee questioned the processing of personal data about some Norwegians in the database, as the reason for registration was unclear in some cases. The Committee also asked why some Norwegians were registered as '*non-Norwegian*' in the target database.

The NIS replied that the service's technical systems have 'historically not facilitated deletion to any great extent'. The NIS admitted that not all the information in the target database is of current intelligence relevance, but that some of the registered information is now of a more 'historical nature'.

In our concluding letter, we noted that the service stated that several of the persons would be deleted from the target database. We referred to the fact that the principle of necessity is a fundamental data protection principle that governs how long personal data can be processed for. This means that data must be deleted once the purpose for which they were collected has been achieved or no longer applies.

The Committee stated that the duty to delete personal data that are no longer necessary for the purpose for which they were collected, also applies to personal data processed in the target database. In the Committee's opinion, the NIS's old target database was not suited to ensuring the deletion of personal data that it was no longer necessary to store. The Committee stated that this is unfortunate, even though there are historical reasons why the system has not facilitated deletion. This is a problem that the NIS must solve.

In connection with this case, the Committee pointed out that, from an oversight perspective, it creates a demanding situation when Norwegians in the database are not registered as Norwegian. We therefore expect systems and procedures to be implemented to ensure that correct information about nationality is registered.



The Norwegian Intelligence Service's headquarters in Oslo. Photo: The Norwegian Armed Forces

17 Cf. the Intelligence Service Act Section 4 first paragraph. Exemptions are regulated in the Instructions for the Norwegian Intelligence Service Section 5 third paragraph. The new Intelligence Act enters into force on January 1 2021.

18 Cf. Instructions for the Norwegian Intelligence Service Section 13 letter d.

19 Internal approval cases can concern permission to share information about Norwegian persons with foreign partners or for the surveillance of Norwegian persons' communication when the persons are abroad. As the Committee has previously pointed out, the NIS is not required to obtain court approval for surveillance of Norwegian persons' communication abroad. PST, on the other hand, needs a court ruling to carry out lawful interception of communication in relation to persons in Norway.

20 Proposition No 80 to the Storting (Bill) page 229 - *Til § 10-3*.

21 Read more in Appendix 2 to this annual report.



Finally, the Committee stated that:

*'In the Committee's opinion, the NIS must implement comprehensive procedures and systems that ensure that personal data stored by the service are deleted once they are no longer necessary for the purpose for which they were registered. This applies regardless of whether the EOS Committee asks the service to account for their necessity. It is the NIS's responsibility to ensure that personal data are not processed in breach of the necessity requirement. The Committee's task is not to ensure, but to oversee, that the NIS complies with the law. If necessary, the service is encouraged to engage in a dialogue with the Ministry on possible technical solutions.'*

From 2021, the Committee will check the NIS's processing of personal data against the requirements of the new Intelligence Service Act.

## 5.5 Review of information previously defined as particularly sensitive

Information that the NIS defines as 'particularly sensitive information' is exempt from the Committee's right of access. This is the only exemption that the Storting has stipulated from the EOS Committee's right of inspection.<sup>22</sup>

According to the NIS's definition, 'particularly sensitive information' is information that discloses:

- '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<sup>23</sup> which, were they to be compromised,
  - a) could seriously damage relations 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.'

In connection with the Committee's inspections of the NIS, we request regular updates on the scope and development of cases and operations that the service defines as 'particularly sensitive information'. The NIS provides an overview of the current number and types of such cases. The information is made available to the Committee once it is no longer defined as being particularly sensitive.

In 2019 and 2020, we reviewed 19 cases/operations dating back several years that were no longer defined as 'particularly sensitive information'. The Committee has found no

indications that the NIS has exceeded its powers or that the rights of any person have been violated.

## 5.6 New Intelligence Service Act and oversight of facilitated bulk collection

### 5.6.1 The new Intelligence Service Act

The year 2020 was the final year the EOS Committee oversaw the NIS pursuant to the act of 1998. On 1 January 2021, the new act adopted by the Storting in 2020 enters into force. The new act was partly a result of the special report concerning the legal basis for the NIS's surveillance activities that the Committee submitted to the Storting in 2016. In the special report, the Committee asked the Storting to examine in more detail whether the NIS should be given a clearer legal basis for the methods it uses based on actual, technological and legal developments.

The EOS Committee has no opinion about what methods the NIS should use in the performance of its duties, but is satisfied to note that the new act is more detailed and up to date. Hopefully, the Committee's oversight of the NIS will become easier than has been the case so far.

The Committee submitted input to the Storting's consideration of the draft act in May 2020, and the act was adopted in June 2020. The letter is enclosed with the annual report as Appendix 3.

### 5.6.2 About the method facilitated bulk collection

Facilitated bulk collection of transboundary electronic communication is one of several methods authorised by the new Intelligence Service Act. A lot of attention is devoted to this completely new method, both in the Act itself and in the preparatory works<sup>24</sup> to the Act. The method gives the NIS access to a copy of electronic communication transmitted across the Norwegian border via cables.

Searches in metadata and the collection of content data are subject to independent advance oversight by Oslo District Court. The EOS Committee will carry out continuous oversight of such collection in addition to its ordinary subsequent oversight of the NIS. The EOS Committee is also tasked with overseeing that the NIS does not exceed the powers granted to the service through Oslo District Court's orders.

The implementation of the chapters of the new Intelligence Service Act that deal with this method (chapters 7 and 8) has been delayed because further legal clarification is needed in relation to EU law and human rights. The service's preparations for the introduction of facilitated bulk collection are already under way. The EOS Committee must also continue its preparations to monitor what the service is developing and put in place the necessary oversight functions well before the method's possible introduction.



### 5.6.3 About oversight of facilitated bulk collection

The EOS Committee's oversight of facilitated bulk collection will take place in several phases. The first step comprises competence-building, both in the Committee and in the Secretariat. This phase has already started. Work is under way to supplement the Secretariat with more people with new expertise. The Committee will then need to obtain more detailed information from the NIS about the service's plans and work in relation to the new method. A dialogue with the NIS is important in order to have oversight functions incorporated into the facilitated bulk collection system. Work is also under way to define the oversight methodology and strike a reasonable balance between inspections, reports, statistics, spot checks and other oversight methods. The division of tasks between the Committee and the Secretariat must be clarified in more detail.

The Storting has allocated extra funding to enable the EOS Committee to perform its new duties, and new legal and technological advisers, as well as an office manager, will be appointed in 2021.

## 5.7 Non-conformities in technical information collection

In late 2019, the Committee identified a non-conformity in the service's technical information collection. The NIS should have discontinued surveillance once there was no longer any connection between the means of communication

under surveillance and the user.

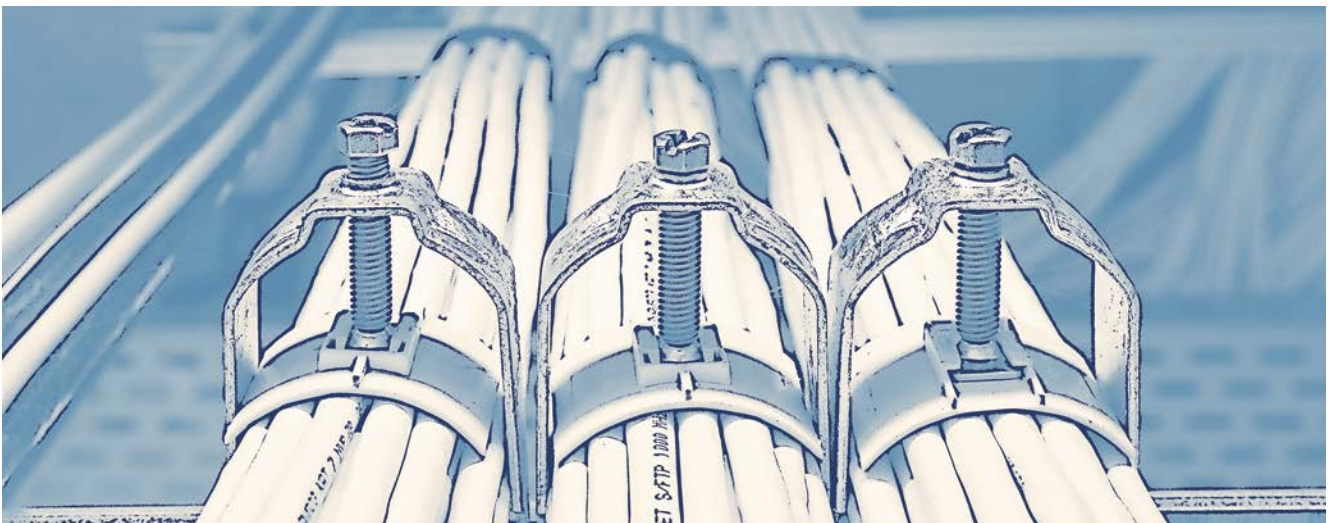
In early 2020, the service admitted to the Committee that this error constituted a non-conformity, although no information/data had been collected as a result of the error. The Committee has raised the case on its own initiative. We will return to the outcome of our investigations in the annual report for 2021.

## 5.8 Complaint cases against the NIS

The Committee received eight complaints against the NIS in 2020, compared with three complaints in 2019. All eight complaints also concerned other EOS services.

The Committee's statements to complainants shall be unclassified. Information about whether a person has been under surveillance or not is classified unless otherwise specified. This means that, in principle, a complainant cannot be told whether he or she is under surveillance by the NIS. The Oversight Act dictates that statements in response to complaints against the services concerning surveillance activities shall only state whether or not the complaint contained valid grounds for criticism.

The Committee concluded six complaint cases against the NIS in 2020. None of these cases resulted in criticism of the service.



22 The head of the NIS can grant the Committee access following a special assessment.

23 By 'intelligence operations abroad' is meant operations targeting foreign parties (foreign states, organisations or individuals), including activities relating to such operations that are prepared and carried out on Norwegian territory.

24 Proposition No 80 to the Storting (2019-2020).

A person is seen from behind, sitting at a desk and working on a laptop. The laptop screen displays a grid of data or code. In the background, there are several large monitors on a wall, showing various graphical interfaces, including a world map and data visualizations. The entire scene is overlaid with a dark blue tint.

6.

## The National Security Authority (NSM)

## 6.1 General information about the oversight

In 2020, the Committee conducted two inspections of NSM. One of these inspections focused on security clearance cases. The Committee's other inspection was of the Norwegian National Cyber Security Centre (NCSC)<sup>25</sup>.

NSM is a directorate and overall responsibility for protective security services pursuant to the Security Act. NSM is the security clearance authority for its own personnel in addition to being the appellate body for clearance decisions made by other security clearance authorities.

In our inspections of the service, we focus on the following:

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

The function of the security clearance authorities are to assess whether a person is reliable, loyal and has sound judgment, and to determine whether he or she is fit to process classified information.<sup>26</sup> A security clearance decision can be decisive for a person's career. It is therefore essential that these cases are considered by the security clearance authorities in a fair manner based on due process protection. The Committee therefore has a strong focus on such cases – and also because the processing of security clearance cases is a more closed process than other administrative decisions.

## 6.2 Complaint cases against NSM

### 6.2.1 Introduction

The Committee received 12 complaints against NSM in 2020, compared with 9 complaints in 2019. The cases concerned both surveillance and security clearance issues, including access to information about security clearance cases.

In cases where the Committee criticises NSM, the complainant is given grounds for the Committee's decision.

We concluded 16 complaint cases against NSM in 2019. The Committee criticised NSM in six cases. Four of these cases are described below. In the last two cases, the Committee criticised NSM for its long case processing time.

### 6.2.2 Complaint case 1 – NSM's right to alter a security clearance decision to the detriment of the complainant<sup>27</sup>

The complainant was granted a conditional security clearance for the level CONFIDENTIAL by the body that made the initial decision. The person appealed the decision to NSM, and the outcome of the consideration of the appeal was that the decision was altered and the person was denied security clearance.

Pursuant to the Public Administration Act Sections 34 and 35, certain conditions must be fulfilled before a decision can be reversed to the detriment of the person to whom the administrative decision is directed. Among other things, a three-month deadline applies to the reversal of a decision to the detriment of a party to a complaint case. In this case, more than a year elapsed from the complaint was submitted until the appellate body made its decision to the detriment of the complainant.

<sup>25</sup> NCSC is the national response function for serious cyber attacks and runs the national warning system for digital infrastructure (VDI). The former NSM NorCERT has now been incorporated into NCSC.

<sup>26</sup> Cf. the Security Act 2018 Section 8-4.

<sup>27</sup> Another part of the case concerned the complainant being given inadequate grounds for the decision. This part of the case was discussed in the EOS Committee's annual report for 2019, section 8.4.3.

#### Protective security services

Planning, facilitating, implementing and overseeing protective security measures that aim to eliminate or reduce risks resulting from activity that poses a threat to security.

#### Conditional security clearance

A security clearance authority may grant a person security clearance subject to specific conditions, for example that the clearance is limited to a specific position or a shorter period than usual.

#### To the detriment of

When a decision is altered to the detriment of someone in a security clearance case, that means that the security clearance status of the person in question is changed to a lower security classification or to no clearance.

On the basis of the complaint, the Committee asked questions of NSM, and later the Ministry of Justice and Public Security. We asked about NSM's right to alter a security clearance decision to the detriment of the principal person in cases where more than three months have elapsed since the principal person appealed the decision.

In its reply to the Committee, the Ministry of Justice stated that deadlines stipulated in Sections 34 and 35 of the Public Administration Act for a reversal to the detriment of the principal person also apply in security clearance cases. At the same time, the Ministry was of the opinion that a decision may be altered to the detriment of the principal person when national security interests outweigh consideration for a person for whom security clearance has been requested.

The Committee concluded that NSM's assessment of its own competence to alter the decision to the detriment of the principal person in the complaint case was inadequate, and we found that NSM did not have the right to alter the decision to the detriment of the principal person in the complaint case. We stated that, when NSM has exceeded the deadline for reversal to the detriment of a person stipulated in the Public Administration Act Section 34 third paragraph, it is important for the complainant that the decision clearly states the legal authority and grounds for the reversal.

At the same time, we assumed that NSM might have authority to amend the decision to the detriment of the principal

person pursuant to the Public Administration Act Section 35 fifth paragraph. However, such a decision must be deemed to constitute an independent decision that the principal person has a right to appeal.

The Committee concluded that the complainant's rights have been violated, and we expect NSM to grant the complainant the right to appeal NSM's decision in the case.

### 6.2.3 Complaint case 2 – Unreasonably long case processing times in a security clearance case

More than four years elapsed from the complainant signed the personal data form until NSM made its final decision to deny security clearance. Nearly three years elapsed from the complainant appealed FSA's initial decision until NSM made the no clearance decision.

We found reason to criticise NSM and FSA for unreasonably long case processing time in the concrete case in question. Such long case processing times in security clearance cases could weaken confidence in the security clearance system. The Committee noted that both FSA and NSM had apologised to the complainant for the long case processing time.

There are clear guidelines laid down by NSM, as the superior security authority, for satisfactory case processing times in security clearance cases for all security clearance authorities, including FSA. This includes clear procedures for forwarding complaint cases from the body that made the



The Norwegian National Cyber Security Centre has its office in downtown Oslo. Photo: Lillian Tveit / Shutterstock.com.

#### Principal person

The person for whom security clearance is requested.



initial decision to the appellate body. It is the Committee's impression that FSA and NSM are both striving to achieve shorter case processing times and to improve the quality of their case processing. We have been informed that the procedures for the forwarding of cases to the appellate body have been changed and that quality assurance has improved. This is a positive development.

#### 6.2.4 Complaint case 3 – Concerning access to correspondence between NSM and the EOS Committee

This case concerns an appeal case concerning security clearance that was concluded in 2019 without criticism of NSM. In connection with the consideration of this case, we asked NSM to consider whether some of the correspondence between the Committee and NSM could be communicated to the complainant.<sup>28</sup> NSM replied that a lot of the information was classified and would have to be redacted before the complainant could be given access.

The Committee has previously expressed agreement with NSM that, on a general basis, collation of detailed security assessments and methods could harm national security interests if they become known to unauthorised parties.<sup>29</sup> In this specific case, the Committee found it difficult to see what the grounds were for not granting access to all the redacted information. Among other things, we pointed out that most of the information that NSM had redacted was already known to the complainant. The Committee again asked NSM to consider the grounds for the correspondence between the Committee and NSM being classified.

NSM reported back to the Committee that it had considered the matter again and granted the complainant access to large parts of the correspondence in question between NSM and the Committee. It is positive that NSM reconsidered the matter and that this resulted in the complainant

being granted extended access.

#### 6.2.5 Complaint case 4 – FSA and NSM's processing of a request for access to information about a security clearance case

See section 7.2.2 of the chapter on FSA for details.

### 6.3 Case processing times in security clearance cases

The Committee has for several years been concerned about the security clearance authorities' case processing times. The statistics are based on the date on which the application was received by the security clearance authority. Below is a table of case processing times for 2020 based on information provided by NSM.

The Committee notes that the case processing time has been significantly reduced for security clearance cases where NSM made the initial decision. For cases considered by NSM as the appellate body, the case processing time has increased markedly.

NSM points to the pandemic and an increase in number of complaint cases as two of the reasons for long case processing times in some areas. The Committee understands the difficulties of this situation, but nevertheless believes that the case processing times should be shorter, particularly in cases concerning requests for access to information (an average of 95 days). By comparison, both the Norwegian Civil Security Clearance Authority (7 days) and the Norwegian Defence Security Department (16 days) have a considerably shorter case processing time for requests for access to information.

CASE PROCESSING TIMES NSM 2020	Average case processing time overall	Average case processing time, positive decisions <sup>30</sup>	Average case processing time, negative decisions
Requests for access to information	95 days <sup>31</sup> (6 cases)		
Requests for security clearance	73 days	68 days (115 cases)	356 days (2 cases)
First-tier appeals	No cases		
Second-tier appeals	122 days	182 days (2 cases)	120 days (673 cases)

28 The EOS Committee cannot decide whether information from a service can be declassified, cf. Section 11 of the Oversight Act.

29 See the annual report for 2018 section 6.3.3 page 28.

30 In the statistics for SKM and NSM, figures for appeals granted in part are included under 'positive decisions', while for FSA, such appeals are included under 'negative decisions'.

31 NSM also considered appeals concerning requests for access received by NSM itself and cases in which it was the appellate body. The case processing times for these cases averaged 177 and 135 days, respectively.



7.

## The Norwegian Defence Security Department (FSA)

## 7.1 General information about the oversight

The Committee conducted two inspections of the FSA in 2020.

In our inspections of the department, we focus on the following:

- FSA's processing of cases where security clearance has been denied, limited or suspended by the security clearance authority. FSA is Norway's largest security clearance authority by far.
- FSA's [operational security services](#)
- FSA's processing of personal data as part of its protective security services
- FSA's cooperation with other EOS services

## 7.2 Complaint cases against FSA

### 7.2.1 Introduction

The Committee received six complaints against FSA in 2020 compared with none in 2019. We concluded five complaint cases against the FSA in 2020. In two complaint cases, the Committee criticised both FSA and NSM.

### 7.2.2 Complaint case 1 – FSA and NSM's processing of a request for access to information about a security clearance case

Based on a complaint concerning partial denial of access to information about a security clearance case, the Committee gave its opinion on several matters and concluded that the complainant's rights have been violated.

#### Access to factual information in internal documents

The complainant was denied access to factual information contained in an internal document. We referred to the Security Act Section 8-14 second paragraph:

'The person is not entitled to disclosure of all or parts of documents which contain information as specified in section 8-13, second paragraph. Nor is the person entitled

to disclosure of documents prepared as part of the internal case preparations of the clearance authority or the body of appeal. **The exception in the second paragraph does not apply to factual information or summaries or other processed forms of factual information.'** (the Committee's boldface)

The following is stated about the above sentence in bold in the preparatory works to the act: 'Access to factual information cannot be denied, cf. second paragraph third sentence'.<sup>32</sup>

In our opinion, there is no legal authority for denying access to 'factual information or summaries or other processed forms of factual information' contained in an internal document. On the contrary, the Security Act stipulates that access to such information *shall* be granted.

Only such factual information in an internal document as listed in the Security Act Section 8-13 second paragraph letters a)–e)<sup>33</sup> can be exempted from access. These exemptions did not apply in the complainant's case.

We informed FSA and NSM that we expected the complainant to be granted access in accordance with the applicable regulatory framework. In the future, the Committee expects the security clearance authorities to grant access to factual information in internal documents in accordance with the Security Act.

Following our concluding statement, NSM has notified the Ministry of Justice and Public Security that it disagrees with our interpretation of the regulations, and it has requested that the Ministry clarify the prevailing law.

#### Duty of secrecy in a security clearance case concerning information presented by the complainant

Both FSA and NSM imposed a duty of secrecy under criminal liability on the complainant concerning information provided to the security clearance authority by the complainant. The Public Administration Act Section 13b was cited as the legal basis. Information about the complainant as well as a statement from the spouse was provided to the security

32 Proposition No 153 to the Storting (Bill) (2016–2017) Chapter 19.8 Comments on Section 8 8.

33 'The statement of reasons shall not include information which may reveal circumstances a) which are relevant to national security interests b) which are relevant for the protection of sources c) of which the person should not gain knowledge in the interests of their health d) which concern the person's closely associated and of which the person should not gain knowledge e) which concern technical installations, production methods, business analyses and calculations, and business secrets otherwise, provided that these are such that third parties could exploit them in a commercial context.'

#### Operational security services

By operational security services is meant identifying and counteracting activity that poses a threat to security targeting Norwegian or foreign military activities, objects or personnel that are not normally covered by the Norwegian Intelligence Service's or military units' intelligence activities or force protection measures.

clearance body by the complainant. We therefore assumed that the spouse had consented to the complainant seeing the statement in question. The provision cited by the security clearance authority as grounds for imposing a duty of secrecy under criminal liability on the complainant applies when a party is granted access to information about another person's personal circumstances without the other person's consent.

In our view, the Public Administration Act Section 13b second paragraph does not authorise either FSA or NSM to impose such a duty of secrecy on the complainant.

### Long case processing time

The Committee pointed out to both FSA and NSM that the case processing time for the request for access was too long. We referred to the following statement by the Parliamentary Ombudsman about the processing of cases concerning access to information:

'Quick and expedient processing of requests for access requires internal procedures that make it practicable to consider cases concerning access to information as they are received. For example, the internal organisation should not be so vulnerable that case processing times grow long if certain individuals are absent or have other pressing duties to attend to. It is first and foremost circumstances relating to the access case or the documents to which access is requested that can give grounds for extended case processing times, not limited resources.'<sup>34</sup>

NSM informed the Committee that its objective is to significantly reduce its processing times in access cases. We take a positive view of this and expect this objective to be followed up.

### 7.2.3 Complaint case 2 – Unreasonably long case processing times in a security clearance case

See section 6.2.3 of the chapter on NSM for details.

## 7.3 Case processing times in security clearance cases

The Committee has for several years been concerned about the security clearance authorities' case processing times. The statistics are based on the date on which the application was received by the security clearance authority. Below is a table of case processing times for 2020 based on information provided by FSA.

The Committee is somewhat concerned to note that the case processing time has increased for security clearance cases where FSA makes the initial decision, as well as when the department considers complaint cases. It is positive that the long case processing times for negative initial decisions pointed out by the Committee last year have decreased slightly, however. FSA points out that, in 2020, it has processed more cases than in 2019 without increasing its staff.

CASE PROCESSING TIMES FSA 2020	Average case processing time overall	Average case processing time, positive decisions	Average case processing time, negative decisions <sup>35</sup>
Requests for access for information	16 days (55 cases)		
Requests for security clearance <sup>36</sup>	42 days	39 days (21,772 cases)	201 days (470 cases)
First-tier appeals	193 days	270 days (19 cases)	175 days (82 cases)

<sup>34</sup> Statement from the Parliamentary Ombudsman – 4.3.2018 – *Krav til saksbehandlingstid for innsynsbejæringer i straffesaksdokumenter*.

<sup>35</sup> In the statistics for SKM and NSM, figures for appeals granted in part are included under 'positive decisions', while for FSA such appeals are included under 'negative decisions'.

<sup>36</sup> FSA has also provided information about the average case processing time for incoming information in security clearance cases. In 2020, it averaged 191 days.





8.

## Oversight of other EOS services

## 8.1 General information about the oversight

The Committee oversees EOS services regardless of which part of the public administration carries out the services.<sup>37</sup> The oversight area is defined by function rather than being limited to certain organisations.

The Committee shall carry out one inspection per year of the Army Intelligence Battalion and one inspection per year of the Norwegian Special Operation Forces, cf. the Oversight Act Section 7.

The Committee received 3 complaints against other intelligence, surveillance or security services in 2020. One of the complaints also concerned the Norwegian Intelligence Service. The complaints in question were against the Ministry of Defence and different branches of the Norwegian Armed Forces. The Committee has not concluded any complaint cases against other intelligence, surveillance or security services in 2020.

## 8.2 Inspection of the Army Intelligence Battalion

During the Committee's inspection of the Army Intelligence Battalion (Ebn) at Setermoen in Troms, we were briefed, among other things, about the battalion's ongoing activities since the previous inspection in 2019. The briefing included an updated operational concept, Ebn's production of intelligence reports, changes in information systems, training activities and the use of volunteers for training purposes. We also requested a briefing about the processing of personal data in the battalion's information systems. As usual, the Committee conducted its own searches in Ebn's computer system.

We asked some follow-up questions after the inspection, and the follow-up has not been concluded.

## 8.3 Inspection of the Norwegian Special Operation Command

During the Committee's inspection of the Norwegian Special Operation Command (NORSOCOM) in Oslo, we were informed, among other things, about personal data processing, procedures for collecting information, important activities and exercises in the Norwegian Special Operation Forces and cooperation with other intelligence, surveillance or security services. The Committee also carried out an inspection of NORSOCOM's physical archive.

The inspection did not give grounds for follow-up.

## 8.4 The Norwegian Civil Security Clearance Authority (SKM)

### 8.4.1 Planned inspection postponed

The Committee had plans to inspect SKM in 2020, but the coronavirus pandemic situation forced us to prioritise the services that we are legally required to oversee. The Committee plans to inspect SKM in early 2021.

### 8.4.2 Case processing times in security clearance cases

The Committee has for several years been concerned about the security clearance authorities' case processing times. The statistics are based on the date on which the application was received by the security clearance authority. Below is a table of case processing times for 2020 based on information provided by SKM.

The Committee is pleased to note that the case processing time for access cases decreased in 2020 from an already fairly low level in 2019. SKM points to challenges relating to the coronavirus situation as the reason why the case processing times in security clearance cases and complaints concerning such cases have both increased. The Committee understands this. Nevertheless, the Committee considers it unfortunate that the average case processing time for negative decisions in security clearance cases, which was already long, increased further in 2020.

CASE PROCESSING TIMES SKM 2020	Average case processing time overall	Average case processing time, positive decisions <sup>38</sup>	Average case processing time, negative decisions
Requests for access for information	7 days <sup>39</sup> (46 cases)		
Requests for security clearance <sup>40</sup>	62 days	56 days (5,378 cases)	200 days (265 cases)
First-tier appeals	136 days	165 days (14 cases)	126 days (40 cases)

<sup>37</sup> Cf. the Oversight Act Section 1 first paragraph.

<sup>38</sup> In the statistics for SKM and NSM, figures for appeals granted in part are included under 'positive decisions', while for FSA, such appeals are included under 'negative decisions'.

<sup>39</sup> SKM also considered appeals concerning requests for access to information. The case processing times for these cases averaged 29 days.

<sup>40</sup> SKM also provided information about the average case processing time for incoming information in security clearance cases. In 2020, it averaged 85 days.

## Cooperation between the EOS services



## 9.1 On the cooperation between PST and the Norwegian Intelligence Service

The Committee discussed the cooperation between the Norwegian Intelligence Service and PST in its annual report for 2013.<sup>41</sup> The Committee's general comments from 2013 remain highly relevant in 2021:

'The basis for this cooperation is the fact that PST's area of responsibility covers what goes on within Norway's borders, while the NIS's area of responsibility is outside the country. The services are required to cooperate in order to safeguard and protect the nation's interests. Cooperation must take place within the limitations imposed by the services' respective powers and areas of responsibility, and otherwise be kept within the bounds set out in Instructions No 1151 of 13 October 2006 for the Collaboration between the Norwegian Intelligence Service and the Norwegian Police Security Service. The purpose of the Instructions is, among other things, to ensure that the services, through their overall resources, exchange of information, cooperation and division of tasks, shall be able to deal with relevant threats and security challenges in an effective manner. The Instructions also set out clear guidelines for the establishment of close and trusting cooperation between the services, at the general level and as well as in concrete cases. It is the Committee's impression that the services cooperate to an increasing extent and maintain a close dialogue.'

Since 2013, the Committee has been particularly concerned about the following issues concerning cooperation between the EOS services:

- The activities of the Joint Counter Terrorism Centre (FKTS) founded in 2013. Here, the Committee has focused in particular on the fact that each of the two services can only collect information under its own legal authority.
- The cyber security work of the Joint Cyber Coordination Centre (FCKS), a collaboration between NSM, the NIS, PST and the National Bureau of Crime Investigation (Kripes).

The Committee has found that more joint analyses and threat assessments are prepared than before.

The Collaboration Instructions<sup>42</sup> express a clear expectation that the services will cooperate on counter-terrorism and cyber security. A similar expectation is expressed with regard to counterintelligence work. Both services have for several years produced analyses that identify the intelligence threat posed by foreign powers as one of the most serious threats to Norway and one that is given top priority by the Norwegian authorities.

Over the past two years, we have paid particular attention to how the counterintelligence collaboration has developed in practice. The Committee has noted that several new collaborative projects between the NIS and PST in the field of counter-intelligence have been launched in 2019 and 2020. The most important ones appear to be the plans to establish a coordination centre and a concrete ongoing counterintelligence collaboration.

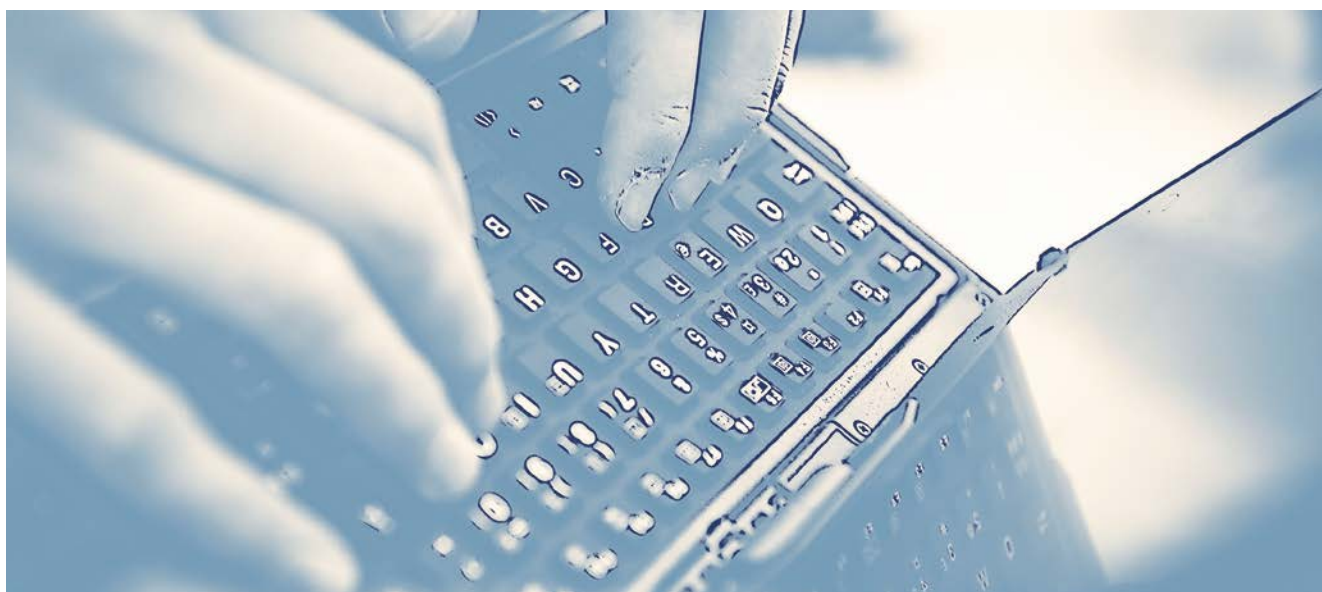


Photo: Norwegian Armed Forces

<sup>41</sup> Chapter VII section 4 in the Committee's annual report for 2013.

<sup>42</sup> Instructions for the Collaboration between the Norwegian Intelligence Service and the Norwegian Police Security Service.



# The investigation into the Frode Berg case

In the annual report for 2019, the Committee reported that we had initiated an investigation into the Frode Berg case. The investigation was initiated on the Committee's own initiative based on information that had come to public attention.

On 14 December 2020, the Committee submitted a concluding statement to the public administration about its investigation.

The Committee then asked the public administration several times whether information in the statement could be declassified or given a lower classification. However, the administration decided that all the information was classified – including the conclusions and whether or not the Committee has expressed criticism. The Committee is bound by the decision of the public administration.

On 25 February 2021, the Committee submitted a special report on classified information in the Frode Berg case to the Storting. In this special report, the Committee wrote that the Storting should familiarise itself with the Committee's assessments and conclusions as set out in the Committee's classified final report.

On the following day, 26 February 2021, the Storting asked the Committee to send it the classified final report. The Committee then sent its final report to the Storting.



**11.**

## Communication and external relations

### 11.1 Communication

The EOS Committee wishes to draw attention to and encourage debate about the democratic oversight of the secret services. The purpose of this is both to spread knowledge about the Committee to the general public and to strengthen confidence in the democratic oversight. Furthermore, the Committee wants to learn from others, both in Norway and abroad, in order to improve its oversight of the EOS services.

In 2020, the coronavirus pandemic has affected both the oversight (see section 2.6) and how we have been able to communicate. A study trip to London and the 2020 annual conference sadly had to be cancelled. We have nonetheless done our best to communicate our oversight message in the best way possible.

Provided that the Committee is able to and not prevented by our duty of secrecy, we make ourselves available to the media, researchers and other interested parties. The committee chair gave a talk on the Norwegian oversight model to students at the Norwegian Defence University College. Meetings have also taken place with the Ombudsman for the Armed Forces and the Parliamentary Ombudsman, among others, and we managed to attend some conferences in early 2020 before the pandemic hit Europe.

In connection with the EOS Committee's 25th anniversary (see Chapter 3 for details), we will publish an anniversary booklet this year based on the Committee's history.

The Committee publishes media summaries about relevant news stories and reports, both on its website [eos-utvalget.no](https://eos-utvalget.no) and via its Twitter account. External parties can receive these summaries via email. About 50 external

parties receive media summaries by email, and the EOS Committee has just under 800 followers on Twitter.

An overview of meetings, visits and conferences that the Committee and the Secretariat have attended in 2020 is provided in Appendix 1.

### 11.2 International cooperation

In the Committee's opinion, international oversight cooperation is important, both to learn from oversight colleagues in other countries, but also because of the extensive cooperation between the Norwegian intelligence and security services and foreign services. This includes sharing of sensitive personal data about Norwegian nationals.

We have cooperated with oversight colleagues abroad for many years. In recent years, a cooperation has been formalised in the Intelligence Oversight Working Group (IOWG). The oversight bodies of Belgium, the Netherlands, Switzerland, Denmark, the UK and Norway are members of the group, where methods and experience are discussed at an unclassified level. In January 2020, a meeting was held in Oslo that was also attended by representatives of the two Swedish oversight bodies. The topic of the meeting was system-based oversight and the development of oversight methodology.

PST has confirmed to the Committee that Norway's membership of the collaborative forum Counter Terrorism Group (CTG) is publicly available information.<sup>43</sup> This makes it easier for us to take part in discussions about oversight of multi-lateral cooperation in Europe.

43 See the EOS Committee's annual report for 2017, section 5.10, for details.

#### Sensitive personal data

The Personal Data Act defines certain information (referred to as 'special categories' in the Act) as sensitive. This applies to information about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of identifying a person, health data, and information about a person's sexual orientation or sex life.



**12.**

## Appendices



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

### Conference presentation

Committee member Øvstedal gave a presentation on the EOS Committee at the Security Divas conference at Gjøvik in January. The conference, which is hosted by the Norwegian Center for Information Security (NorSIS), targets women who study or work in the field of information security.

### Meeting of the international oversight cooperation group IOWG

In January, the EOS Committee welcomed oversight colleagues from Switzerland, Belgium, the Netherlands, Denmark, the UK and Sweden to a meeting in Oslo in connection with the Intelligence Oversight Working Group. See section 11.2 for details.

### 5G conference in Belgium

The head of the Secretariat's technology unit attended the European 5G Conference in Brussels in January.

### Police congress in Germany

In February, the head of the Secretariat's technology unit attended the European Police Congress in Berlin.

### Meeting with a delegation from Kyrgyzstan

In February, the committee chair and two secretariat employees met with representatives of the Norwegian Helsinki Committee and human rights activists representing Kyrgyzstan's civil society who were visiting Oslo. They were interested in hearing about how the Norwegian model for

oversight of the intelligence and security services works, since work is under way to endeavour to establish oversight of such services in the former Soviet republic.

### Meeting with the Parliamentary Ombudsman

Three secretariat employees attended a meeting with the Parliamentary Ombudsman in September to discuss issues of relevance to the Storting's external oversight bodies.

### Meeting with the Ombudsman for the Armed Forces

The committee chair and representatives of the Secretariat met with the Ombudsman for the Armed Forces in September. The topic was where to draw the line between the EOS Committee's and the Ombudsman's scope of activity and issues relating to security clearance. The meeting was followed up with a meeting at secretariat level in October.

### Lecture at the Norwegian Defence University College

In November, the committee chair gave a talk on the Norwegian oversight model to students on the course on politics, society and intelligence.

### Webinar on oversight of military intelligence services

In December, one committee member and three secretariat employees took part in an online seminar organised by the NATO Parliamentary Assembly and DCAF – Geneva Centre for Security Sector Governance on oversight of military intelligence services.



## APPENDIX 2 – News from foreign oversight bodies

### Denmark

The Danish Intelligence Oversight Board's (TET) special report on the Danish Defence Intelligence Service (FE) attracted a great deal of attention in Danish media last year. Both the head of FE and other senior personnel were put on leave of absence in connection with this.

In a nutshell, the case concerned information that the Oversight Board received from one or more whistle-blowers, and which resulted in the Oversight Board reporting the following, among other things, to the Danish authorities:

- that FE has withheld important information and given the Oversight Board incorrect information
- that an 'unfortunate legality culture' prevailed in FE's management and parts of the services
- possible unlawful surveillance of Danish nationals
- that an evaluation should be carried out to assess whether the Oversight Board has a wide enough remit and sufficient resources to effectively review legality in relation to FE
- that an external whistle-blower system should be established

The case has given rise to debate about the Danish oversight system. TET has a narrower remit than the EOS Committee. Questions have also been raised regarding the Danish Parliament's Intelligence Services Committee, which practises complete secrecy on all matters.

In the wake of TET's special report, Danish media have reported claims that the NSA is spying on Denmark, Norway and other countries through a system for collecting information from internet cables.

TET has also criticised the Danish Security and Intelligence Service (PET) for taking a very long time to respond to the Oversight Board. PET also received criticism because they had unlawfully processed information about 30 people solely based on lawful political activity in the form of participation in a demonstration.

In its oversight of the Centre for Cyber Security, TET has found both unlawful processing of personal data and failure to delete sensor data.

### The UK

In its annual report for 2019, the UK oversight body, the Investigatory Powers Commissioner's Office (IPCO), writes about shortcomings in source management when the SIS<sup>44</sup> engages in HUMINT. The oversight body also writes about the oversight of the SIGINT service GCHQ's work to find weaknesses in technology and the process that GCHQ has in place for determining whether to make weaknesses publicly known or exploit them.

### Belgium

The annual report for 2019 from the Belgian oversight body shows that there has been a sharp increase in the Belgian security services' use of covert coercive measures.

### France

The French parliament has so far not granted the French oversight body CNCTR's wish to be given the possibility of overseeing information that French intelligence services share with their partners. Several other independent oversight bodies in Europe, including the EOS Committee, have such a right.

### Germany

There is debate in Germany about what form the oversight of the German intelligence services should take. Among other things, a new oversight body has been proposed to exercise stricter oversight of the foreign intelligence service BND.

### Sweden

Unlike the EOS Committee, the Swedish oversight body – the Swedish Commission on Security and Integrity Protection (SIN) – can oversee the higher prosecuting authorities. SIN also oversees both the ordinary police and the Swedish Security Service (which corresponds to PST in Norway). In one of its 2020 statements, SIN wrote about its oversight of how the Swedish Prosecution Authority deals with surplus information from covert coercive measures.

44 Also known as the MI6.

#### HUMINT

Abbreviation for Human Intelligence. An intelligence discipline that collects intelligence using human sources.

#### SIGINT

Abbreviation for Signal Intelligence. An intelligence method whereby signals sent from one place to another are intercepted.

## APPENDIX 3 – Input to the Storting's consideration of the new Intelligence Service Act



The Standing Committee on Foreign Affairs and Defence  
Stortinget  
NO-0026 OSLO

Copy: The Presidium of the Storting  
The Standing Committee on Scrutiny and Constitutional Affairs  
12 May 2020

### Input to the Storting's consideration of Proposition No 80 to the Storting (Bill) (2019–2020)

#### 1. Draft bill for a new Act relating to the Norwegian Intelligence Service and the EOS Committee's oversight

On 22 April 2020, the Ministry of Defence proposed a new Act relating to the Norwegian Intelligence Service, which will replace the 1998 Intelligence Service Act. The draft bill is based on the Ministry's consultation paper of 12 November 2018. The EOS Committee submitted a consultation statement on 12 February 2019.

The proposed Section 2-6 of the draft bill confirms that the Norwegian Intelligence Service is subject to oversight by the EOS Committee pursuant to the Oversight Act. The Ministry writes as follows:

'The new Intelligence Service Act will not change the framework for the Committee's oversight. However, it will establish continuous oversight of the service's compliance with the provisions of Chapter 7 on facilitated bulk collection, cf. first paragraph second sentence, **which will come in addition to general subsequent oversight pursuant to the Oversight Act.**' (Committee's boldface)

A key part of the proposition concerns the assessment of whether facilitated bulk collection of transboundary electronic interception should be recommended and on what conditions. The proposition consistently emphasises the importance of the EOS Committee's oversight. We note the confidence placed in the Committee.

#### 2. Review of the EOS oversight model

If the bill is adopted by the Storting, the Committee expects that the new oversight task (continuous oversight of facilitated bulk collection) will necessitate a review of the Committee's oversight activities and priorities. In the Committee's consultation statement, we referred to the Standing Committee on Scrutiny and Constitutional Affairs' comments in Recommendation No 146 to the Storting (2016–2017)<sup>1</sup>:

'The rapidly accelerating technological development, increased globalisation and an increasingly complex threat situation change the conditions for surveillance and thus for the EOS Committee's oversight of

<sup>1</sup> The Standing Committee on Scrutiny and Constitutional Affairs' recommendation concerning the Report from the Evaluation Committee for the Norwegian Parliamentary Intelligence Oversight Committee (EOS Committee) on the evaluation of the EOS Committee.

the methods. The Committee has noted that the Evaluation Committee points to the probability of the oversight tasks increasing in complexity and scope, among other things with reference to potential consequences of “digital border defence” that the Ministry of Defence has announced will be reviewed. The Committee notes that the Evaluation Committee finds that it would be **difficult to expand the scope of parliamentary oversight of the secret services without an overall review of the oversight model.**

The Committee also notes that the Evaluation Committee has not conducted such a review, but limited itself to pointing out the need for fresh thinking. In light of the trends described by the Evaluation Committee, **the Committee is of the opinion that the oversight model should have been included in the Evaluation Committee’s work, but takes note of the fact that the Storting will have to return to this matter at a later time** (Committee’s boldface)

In its consultation submission, the EOS Committee also referred to the proposal to introduce facilitated bulk collection and raised the question of whether the oversight model has been examined to the extent that the Storting appears to assume. Section 11.15 of the proposition discusses the need to strengthen the Committee Secretariat. *If new and demanding tasks are assigned to the EOS Committee, however, that will also challenge the framework for the work of the Committee itself and its involvement in the different aspects of oversight.*

*Regardless of whether the EOS oversight model is reviewed or not, the EOS Committee will get back to the Storting if necessary after gaining experience of the new oversight task.*

### 3. Where should the EOS Committee’s continuous oversight of facilitated bulk collection take place?

In the proposed bill, the Ministry gave grounds for its view that the ‘continuous oversight’ should be carried out by the EOS Committee.

It is assumed in section 11.10.4 of the proposition that the ‘continuous oversight’ of facilitated bulk collection will primarily take place on the Norwegian Intelligence Service premises:

‘The EOS Committee is of the opinion that as much as possible of the continuous oversight should be performed from the Committee’s own premises [in the consultation submission]. The Ministry agrees that consideration for the Committee’s independent position could indicate that as much as possible of the oversight should be performed from the Committee’s own premises, in the same way as the court of law’s advance oversight will be carried out on the court’s own premises. On the other hand, continuous oversight differs in nature from advance oversight, and weighty information security considerations indicate that the continuous oversight should be carried out from the Norwegian Intelligence Service premises. Moreover, there are key oversight elements that it will not be practically possible to carry out from the Committee’s premises. The Ministry therefore concludes that continuous control will primarily have to be performed from the service’s premises. The Ministry presumes that the Norwegian Intelligence Service and the Committee will be aware of the importance of safeguarding the Committee’s independent position in the practical performance of continuous oversight activities.’



In the EOS Committee's opinion, considerations of independence and confidence in the oversight should result in the Committee's oversight of facilitated bulk collection being performed from our own premises insofar as this is possible.

The Committee points out that the question of where the oversight of the EOS services is performed, is part of a dynamic process. We are currently engaged in discussions with all the EOS services about how more of the oversight activities can be performed in a secure manner from the Committee's premises. The discussions cover both the issue of digital communication and remote access to parts of the services' information systems. In the long term, the outcome of these discussions will have a bearing on where and how oversight activities are performed.

\*\*\*

*The EOS Committee will naturally be at the committee's disposal to answer any further questions you may have.*

## APPENDIX 4 – Act relating to oversight of intelligence, surveillance and security services<sup>45</sup>

### 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 can issue instructions concerning the activities of the Committee within the framework of this Act and lay down provisions concerning its composition, period of office and secretariat.

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 five years. A member may be re-appointed once and hold office for a maximum of ten 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 head of the Committee's secretariat shall be appointed by the Presidium of the Storting on the basis of a recommendation from the Committee. Appointment of the other secretariat members shall be made by the Committee. More detailed rules on the appointment procedure and the right to delegate the Committee's authority will be stipulated in personnel regulations approved by the Presidium of the Storting.

### Section 5. The responsibilities of the Committee

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

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

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

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

The oversight activities do not include activities which concern persons or organisations not domiciled in Norway, or foreigners whose stay in Norway is in the service of a foreign state. The Committee can, however, exercise oversight in cases as mentioned in the first sentence when special reasons so indicate.

<sup>45</sup> The law was last changed in June 2020.

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 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 stipulates its own financial management directive. The directive shall be approved by the Presidium of the Storting.

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.

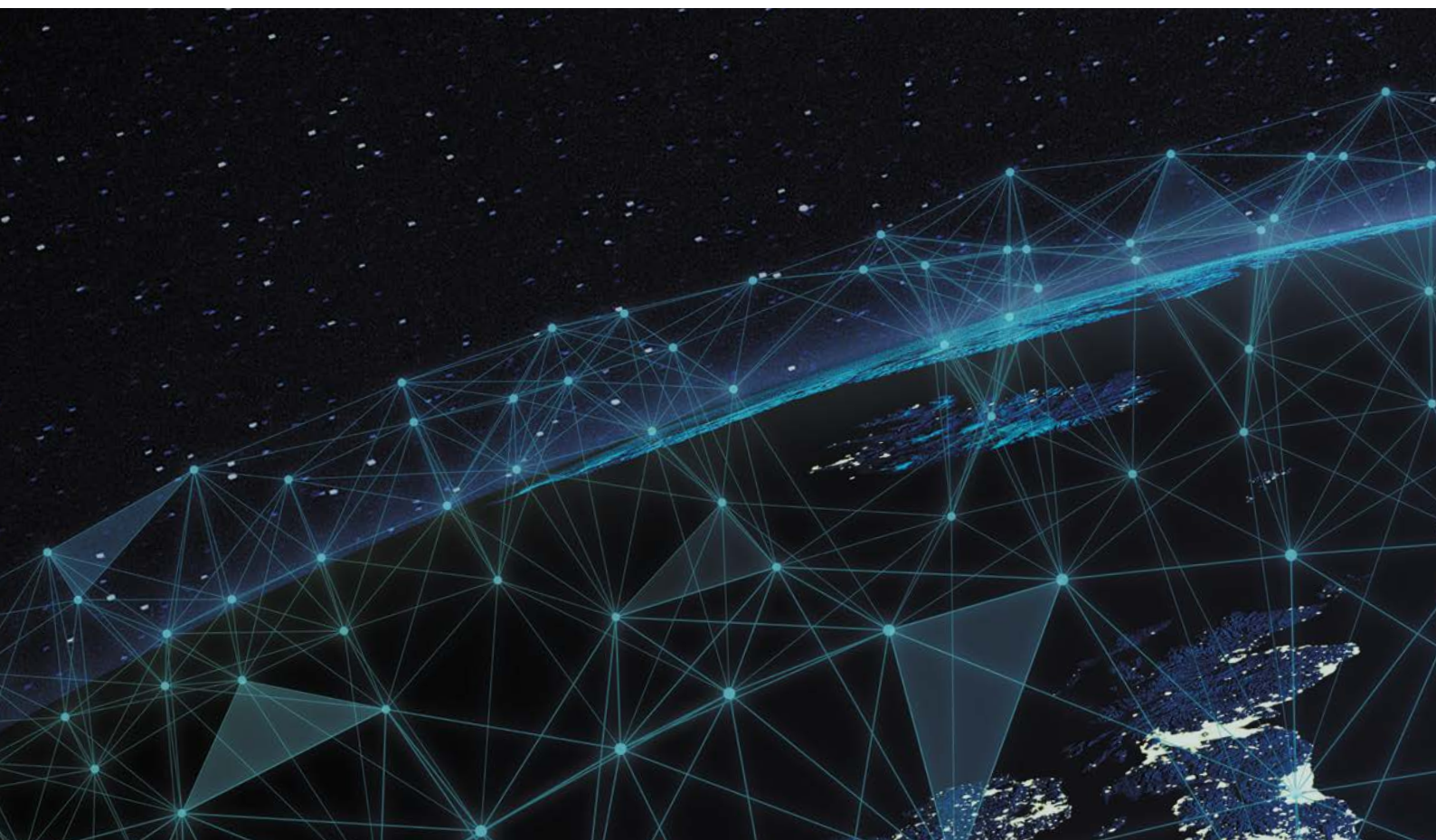
### Section 21. Penalties

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



tdesign.no

**Contact information**

Telephone: +47 21 62 39 30

Email: [post@eos-utvalget.no](mailto:post@eos-utvalget.no)

[www.eos-utvalget.no](http://www.eos-utvalget.no)